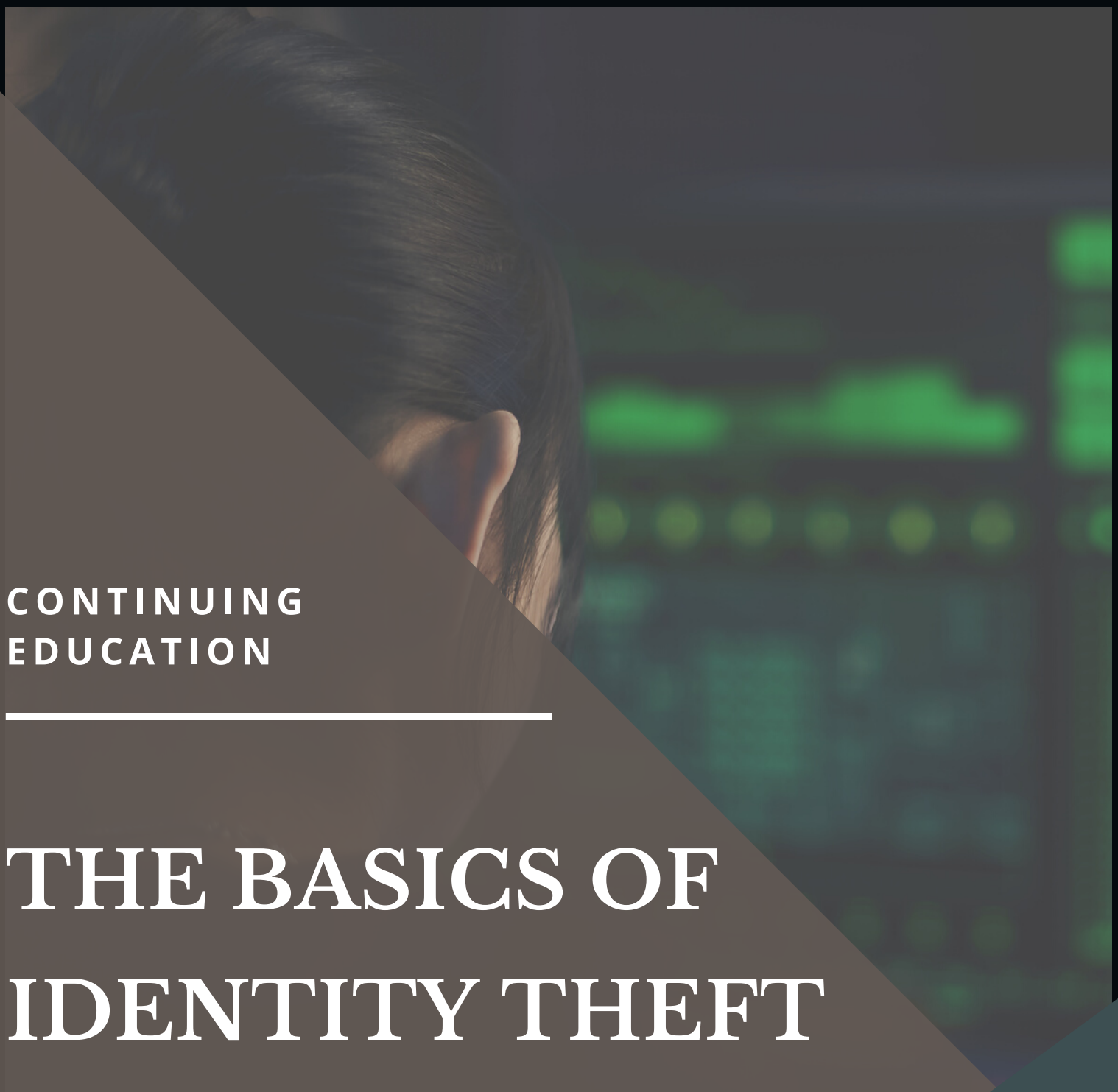

CONTINUING EDUCATION

# THE BASICS OF IDENTITY THEFT

8 CPE Hours

Course 7050

Self-Study Online
Sequoia CPE

# THE BASICS OF IDENTITY THEFT (COURSE #7050D)

## COURSE DESCRIPTION

More than ever before, the information explosion has led to the expansion of a crime in the form of identity theft. This course provides an overview of the problems of identity theft, types of identity theft, and remedies available for its victims. In addition, it will look at suggestions for businesses to use to reduce the risk of such crimes. Lastly, the course focuses on several rules mandating practices for financial firms to safeguard client information.

## LEARNING ASSIGNMENTS AND OBJECTIVES

*As a result of studying each assignment, you should be able to meet the objectives listed below each individual assignment.*

**ASSIGNMENT 1:** **SUBJECT**

**Introduction to Identity Theft**

**Common Schemes in Identity Theft**

**Victims of Identity Theft**

Study the course materials from pages 1 to 60

Complete the review questions at the end of each chapter

Answer the exam questions 1 to 11

**Objectives:**

- To identify the most common reasons for identity theft
- To recognize the requirement of consumer reporting agencies to provide individuals with credit reports
- To identify common schemes used in perpetrating identity theft
- To recall the impacts of using fraud alerts
- To recall an individual's limited responsibility for unauthorized credit card charges

**ASSIGNMENT 2:** **SUBJECT**

**Other Forms of Identity Theft**

**How to Protect Yourself When Using Technology**

**Social Security Numbers**

**Identity Theft and Business**

Study the course materials from pages 61 to 130

Complete the review questions at the end of each chapter

Answer the exam questions 12 to 26

**Objectives:**

- To identify common sources for child identity theft
- To recognize the impact on a victim of criminal identity theft
- To recognize the security measures that should be taken due to advances in wireless technology
- To identify the control recommendations for protecting the security of social security numbers
- To recognize ways businesses can help prevent identity theft

**ASSIGNMENT 3:** **SUBJECT**

**The Financial Privacy Requirements of the Gramm-Leach-Bliley Act**

**Financial Institutions and Customer Data: Complying with the Safeguards Rule**

**The Disposal Rule and the Red Flags Rule**

Study the course materials from pages 131 to 186

Complete the review questions at the end of each chapter

Answer the exam questions 27 to 40

**Objectives:**

- To recall the requirements of the Gramm-Leach-Bliley Act
- To identify what is governed by the Financial Privacy Rule
- To recognize who is impacted by the Safeguards Rule
- To recognize the impact of the federal Disposal Rule
- To recall who must comply with the Red Flags Rule

**ASSIGNMENT 4:**

**Complete the Online Exam**

**NOTICE**

This course is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional advice and assumes no liability whatsoever in connection with its use. Since laws are constantly changing, and are subject to differing interpretations, we urge you to do additional research and consult appropriate experts before relying on the information contained in this course to render professional advice.



Program publication date **08/24/22**

## EXAM OUTLINE

- **TEST FORMAT:** The final exam for this course consists of 40 multiple-choice questions and is based specifically on the information covered in the course materials.

- **ACCESS FINAL EXAM:** Log in to your account and click Take Exam. A copy of the final exam is provided at the end of these course materials for your convenience, however you must submit your answers online to receive credit for the course.

- **LICENSE RENEWAL INFORMATION:** This course (#7050D) qualifies for **8** CPE hours.

- **PROCESSING:** You will receive the score for your final exam immediately after it is submitted. A score of 70% or better is required to pass.

- **CERTIFICATE OF COMPLETION:** Will be available in your account to view online or print. If you do not pass an exam, it can be retaken free of charge.

ENJOY YOUR COURSE

# TABLE OF CONTENTS

# CHAPTER 1: INTRODUCTION TO IDENTITY THEFT

## Chapter Objectives

**After completing this chapter, you should be able to:**

- Identify the most common reasons for identity theft.
- Recognize the requirement of consumer reporting agencies to provide individuals with credit reports.

*Jane Sprayberry handed over her driver's license to an American Express customer service representative who had asked for it in order to replace Jane's lost credit card. True to the Amex promise, she received the replacement card without delay. The only trouble was that the recipient was not the real Jane Sprayberry. The driver's license had her name on it, but the photograph was not of her. In no time, the imposter ran up a big bill on high-priced jewelry, clothing, and appliances. Just a week before, Jane's husband's bank account had been emptied and his credit card cloned. A coincidence? Not at all. A ring of fraudsters in Detroit had gotten jobs at large businesses and had collected reams of personal information: personnel records, credit records, old rental-car agreements. Those offenders who were eventually caught had bags and books full of such records – records they had used over several years. They had run up an average of $18,000 in credit card charges per victim. And they had sold identities on the street for around $25 each. It took the real Jane Sprayberry and her husband more than six months to clean up the mess.*

## I. OVERVIEW

More than ever, the information explosion – aided by an era of easy credit – has led to the expansion of a crime that feeds on the inability of consumers to control who has access to sensitive information and how it is safeguarded. That crime is identity theft. Identity theft remains the number one concern among consumers contacting the Federal Trade Commission (FTC).

Their fears are real, as the following facts illustrate:

- Of the more than 3.2 million fraud cases reported to the Federal Trade Commission (FTC) in 2019, identity theft accounted for 20.33% of cases and was the most-common type of fraud.
- 2019 was the worst year in history for identity theft reports by a wide margin.
- There were 650,572 cases of identity theft in 2019.
- Those aged 30 to 39 reported the most cases of identity theft last year.

- Georgia, Nevada, and California were the top three states for identity theft by population.
- With over 270,000 reports, credit card fraud was the most common type of identity theft last year and more than doubled from 2017 to 2019.
- Almost 165 million records containing personal data were exposed through data breaches in 2019.
- The Capital One cyber incident was the biggest data breach of 2019, as it exposed the personal data of approximately 100 million consumers in the United States.
- Unauthorized access is on the rise and is the leading cause of exposed records with personal information in data breaches.
- 2019 was the worst year in history for identity theft reports by a wide margin. It had more than 160,000 identity theft reports than 2015, which previously had been the year to hold this dubious record.
- 2019 marked the second year in a row that identity theft reports increased significantly.
- From 2017 to 2018, the number of reports increased by 19.8%. From 2018 to 2019, there was a staggering 46.4% increase.
- Somewhere between seven and 10% of Americans are the victims of some sort of identity theft annually.

Experts believe that data breaches are playing a major role in the large increase in incidents of identity theft. The Equifax data breach that lasted from May to July 2017 exposed the sensitive personal information of approximately 147 million U.S. consumers, making it one of the largest data breaches in history. And the 2019 Capital One data breach affected approximately 100 million U.S. consumers.

These kinds of data breaches contribute to both identity theft and credit card fraud. While identity theft can happen to anyone, those in the 30 to 39 age range reported it the most. Their 170,255 cases made up 30.2% of all identity theft reports in 2019, and their number of reports shot up by 58.6% from 2018 to 2019. However, it is certainly not isolated to that group. The three groups from ages 20 to 49 all recorded more than 110,000 cases and increases of over 44% within a year.

This data indicates that identity theft is becoming more concentrated among consumers between the ages of 20 and 49 and, to a lesser extent, those from 50 to 59. The question is why. Experian has reported that “When it comes to scams, children and seniors are at the biggest risk,” but it appears the opposite is true.

A potential explanation is that consumers in those high-risk age ranges have more credit cards and purchase more. The study “Who Are the Victims of Identity Theft? The Effect of Demographics” points out that more accounts and transactions increase the risk of identity theft. Older consumers and teenagers have fewer credit cards and make fewer purchases, two factors that lower their risk.

Credit card fraud is by far the most common type of identity theft, occurring in 41.8% of all identity theft reports. Although credit card fraud is more prevalent among certain age ranges than others, it is the most common identity theft in almost every age group, with one notable exception. The 19 and under group had 1,680 cases of credit card fraud, occurring in 11.8% of their total identity theft reports. Employment or tax-related fraud was most prevalent among this group, with 7,072 cases making up 49.7% of their identity theft reports. Among the other age groups, employment or tax-related fraud occurred in only 7.0% of their identity theft reports.

Here are the states with the most identity theft reports in 2019:

- California: 101,639
- Texas: 73,553
- Florida: 64,842
- Georgia: 44,888
- New York: 36,337

Going forward, the Identity Theft Resource Center (ITRC) predicts identity theft protection services will primarily focus on data breaches, data abuse, and data privacy. ITRC also predicts that consumers will become more knowledgeable about how data breaches work and expect companies to provide more information about the specific types of data breached and demand more transparency in general in data breach reports.

According to a 2019 *Internet Security Threat Report* by Symantec, cybercriminals are diversifying their targets and using stealthier methods to commit identity theft and fraud. Cybercrime groups like Mealybug, Gallmaker, and Necurs are opting for off-the-shelf tools and operating system features such as PowerShell to attack targets. PowerShell is a command-line shell and scripting language designed by Microsoft. In recent years, malicious PowerShell scripts have increased by 1,000%.

This affects so many of us because Microsoft Office files make up 48% of malicious email attachments.

Identity theft affects both businesses and consumers. Not only do businesses suffer direct loss due to this crime, but inadequate security and poor business practices may open a company up to liability suits, fines and loss of clients. Perhaps no professional handles more sensitive financial information than CPAs and Enrolled Agents (EAs). From bank account numbers to social security numbers, CPAs and EAs receive and maintain the most sensitive of information. It is therefore incumbent that accounting professionals have a solid understanding of the problem of identity theft, its ramifications on victims and some of the many new state and federal laws that directly impact the practice of accounting and other financial-related industries.

While no one can totally prevent identity theft due to the human element of this crime, there are steps that a company can take to minimize risk factors for all of us. Safe information handling practices are the key to keeping identifying information out of the hands of thieves. These are some of the questions that must be asked:

- Information acquisition: *Do you have a good reason for requesting the information that you gather? Are you acquiring it in a safe manner so that it cannot be overheard or seen by others?*
- Storage: *What computer security measures have been placed around the systems storing personal data? Is the data considered highly classified and not common access?*
- Access: *Is personal identifying information available only to limited staff? Is database access audited or password controlled?*
- Disposal: *What is in your dumpster? Is it a treasure chest for thieves? Are electronic/paper documents and databases containing personal information rendered unreadable prior to disposal?*
- Distribution: *Are personnel trained in the proper procedures regarding information disclosure? Do you publicly display, use or exchange personal information (especially social security numbers) in your workplace? This includes employee or membership cards, timecards, work schedules, licenses or permits and computer access codes.*
- Personnel: *Do you conduct regular background checks on ALL employees with access to identifying information? That might also include mailroom staff, cleaning crews, temp workers and computer or hotline service techs.*

## Identity Theft Trends

**Formjacking is up 117%**

Formjacking is a form of digital information theft that attacks commercial websites involved in banking, e-commerce, and other activities that collect customers' personal information. Symantec describes it as software that does in the virtual world what card skimmers do in the real world. It came to light in late 2018 when Symantec reported that hackers attempted more than 3.7 million formjacking attacks that year alone. Cybercriminals continue to take in millions each month by hijacking credit card data from online payment forms to the tune of roughly 4,800 sites being infected each month.

**Ransomware activity is down 20%**

Ransomware attacks decreased last year for the first time since 2013. Identity theft experts suspect this is because ransomware attacks target Windows-based applications, and more people are storing and sharing data using the cloud. Ransomware threats remain a risk for businesses, as enterprise ransomware has increased by 12%.

**New account fraud is up 13%**

In 2018, new account fraud accounted for $3.4 billion in losses, up from $3 billion in 2017, according to Javelin Strategy. The most common targets for new account fraud are mortgages, student loans, car loans, and credit cards.

## Identity Theft Trends (continued)

**Account takeovers are up 79%**

The number of account takeovers (when a fraudster gets access to another individual's account) also increased, rising from 380,000 in 2017 to 679,000 in 2018. Both individuals and enterprises are at risk for account takeovers.

**Increased effort to solve the year 2038 problem**

Similar to the Y2K problem, the 2038 problem is a bug that will affect the way computers store time-stamps. Computer logic defines time-stamps with the current date and time, minus the number of seconds that have passed since January 1, 1970, when computers originated. In 2038, the number of elapsed seconds will exceed the information that can be stored in a four-byte data type, meaning most computers will need an extra byte to preserve their timing systems. The 2038 problem will be a logistical nightmare to solve and could affect databases and make private information public. Without a resolution, hackers will likely search for ways to exploit this bug.

Congressional hearings on identity theft in the 1990s revealed that police generally did not regard those whose identities had been stolen as the true victims, since the credit card companies took the financial loss. In addition, the companies typically did not report their losses to local police (or to anyone else, for that matter). Studies also showed that victims rarely reported the loss or theft of a card to the police, since they believed that the card company would cover the loss. However, because the repeated use of a victim's identity caused serious disruption and emotional damage, more victims began to report the offense.

Credit-reporting agencies now require that victims file a police report as part of the "identity theft affidavit." Victims previously had a hard time getting such reports from the police. However, in response to growing media coverage and congressional testimony concerning identity theft, the International Association of Chiefs of Police (IACP) adopted a resolution in 2000 urging all police departments to provide incident reports and other assistance to identity theft victims.

## Common Methods of Obtaining Personal Information

- People carry personal information on them, which offenders may obtain via pick-pocketing, mugging, or, if it is lost, simply finding it. People also leave personal information in cars or other places where experienced thieves know to look;
- Burglars can get information from victims' homes, and "Internet burglars," or hackers, can obtain personal identifying data when people shop online;
- People's trash cans serve as another source of information. People often throw away credit card statements, bank statements, and other documents containing personal information. Offenders may go through people's trash looking for such information;

## Common Methods of Obtaining Personal Information (continued)

- People routinely give out personal information during business transactions, such as in shops and restaurants; and
- If a smartphone falls into the hands of an unscrupulous person, the thief can often access email accounts, bank account balances, social networking profiles, and calendars.

There is an enormous amount of personal information available, and it is incredibly easy to obtain. Government agencies and businesses keep computerized records of their clients. They may sell or freely provide that information to other organizations. Often, all that is needed is one form of identification, such as a driver's license, and an offender can obtain the victim's mother's maiden name, social security number, etc. Many identity theft crimes are committed by employees of organizations that maintain client databases. For example, a widely publicized Detroit case involved an identity theft ring in which employees of a major credit card company stole customer information. Procedures for authenticating individual identities are often inadequate. Establishing a given person's "true identity" is a complex task. It requires the careful assessment of:

- The person's biological identity (physical features, DNA, fingerprints, etc.);
- The person's historical identity (date of birth, marriage, etc.); and
- The link between those identities.

Many agencies and businesses make only a cursory attempt – if any – to assess these.

Classifying identity theft into types is difficult, as it involves a wide variety of crimes and related problems. However, the acknowledged motives for identity theft can be used to construct a simple typology. Research indicates that the two dominant motives for identity theft are financial gain and concealment (either of true identity or of a crime). These motives are mediated by the offenders' level of commitment to the task and the extent to which offenders are simply opportunists taking advantage of the moment.

Professionals who seek out targets and create their own opportunities – usually in gangs – have a high level of commitment. A lot of planning and organization is involved. Some lone offenders also display considerable commitment and planning, especially in regard to concealing personal history. Offenders with low commitment take advantage of opportunities in which ID theft appears to solve an immediate problem; thus their identity thefts are "opportunistic."

Research has shown, for example, that organized criminal gangs in Southeast Asia manufacture plastic cards using stolen identities. These are then marketed on the street in large U.S. and European cities. Street fraudsters tend to specialize in particular types of card fraud. They use highly sophisticated techniques to avoid detection either when using the card in a retail store or when converting purchased goods into cash. They tend to work in small gangs, deal in high volume, and operate in high-population areas, usually 50 miles or more away from where they live.

Terrorism is one of the most recently cited instance of organized groups' stealing identities to conceal illegal activities, and to make tracking their true identities much more difficult after they've committed

crimes. Authorities claim that all 19 of the September 11 terrorists were involved in identity theft in some way. This resulted in the mistaken arrest of people whose identities had been stolen.

Other types of identity theft are less organized and more opportunistic. Examples include the following:

- A college student uses his or her roommate's personal information to apply for a pre-approved credit card, which comes in the mail to which they both have access; or
- A restaurant worker processes a customer's credit card payment and notices that the complete card number is printed out on the receipt, along with the expiration date. The worker copies the information and later makes several large purchases over the Internet, where he or she does not need to show the card or verify his or her identity.

The most common type of opportunistic identity theft for concealment occurs when an offender gives the name of an acquaintance, friend, or family member when stopped, questioned, or arrested by police.

Examples include the following:

### Example 1

Jefferey Williams was jailed for 10 days without bail on a warrant for drug possession and resisting arrest. The Orange County (Fla.) Sheriff's Department had issued the warrant in Orlando. Williams insisted that he was not the person the police were looking for. The trouble was that Florida authorities were seeking a relative of Williams who had passed himself off as Jefferey, giving Jefferey's name, birth date, and old home address.

### Example 2

Lisa Sims (alias Elisa McNabney) assumed the name of her cellmate from a prior prison term to cover up her extensive criminal past and avoid arrest on suspicion of murdering her husband. Investigation revealed that she had multiple social security numbers and other forms of identity.

Using a variety of methods, criminals steal social security numbers, driver's licenses, credit card numbers, ATM cards, and other pieces of individuals' identities such as date of birth. They use this information to impersonate their victims, spending as much money as they can in as short a time as possible before moving on to someone else's name and identifying information.

There are two types of financial identity theft:

- "Account takeover," also known as "account compromise," occurs when a thief acquires your existing credit account information and purchases products and services using either the actual credit card or simply the account number and expiration date.

- "Application fraud" is what some experts call "true name fraud." The thief uses your social security number (SSN) and other identifying information to open new accounts in your name. Victims are not likely to learn of application fraud for some time, because the monthly account statements are mailed to an address used by the imposter. In contrast, victims learn of account takeover when they receive their monthly account statement.

Covering up past crimes is a major reason for individuals to steal or assume another identity. Kathleen Soliah, wanted for various bombings and attempted murder in relation to her activities in the Symbionese Liberation Front in the late 1960s, assumed the identity of Sara Jones Olson (a common Scandinavian surname in Minnesota). She evaded capture for 23 years, and in the meantime became a doctor's wife, mother of three, community volunteer, veteran of charity work in Africa, and practicing Methodist living in an upscale neighborhood in St. Paul, Minnesota.

In response to public attention on this growing and serious problem, there are now many resources available to help individuals and businesses prevent and react to identity theft, including the Federal Trade Commission, which is the federal agency charged with tracking identity crime, and the Privacy Rights Clearinghouse.

State and federal laws such as the Gramm-Leach-Bliley Act, discussed in detail in this course, Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Fair and Accurate Credit Transactions Act (FACTA) require certain businesses or institutions to protect information better.

This course will provide an overview of the problem of identity theft and remedies available for its victims. It will then look at suggestions for businesses to use to reduce the risk for such crimes. Finally, the course focuses on several rules mandating practices for financial firms, like accounting, to safeguard client information. It is essential that any business or firm that collects private information understand the magnitude of the problem and its obligations in preventing it from occurring.

## II. WHAT IS IDENTITY THEFT?

The short answer is that identity theft is a crime. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another individual's personal data in some way that involves fraud or deception, typically for economic gain.

In the course of a busy day, an individual may write a check at the grocery store, charge tickets to a ball game, rent a car, mail his or her tax returns, change cell phone service providers, or apply for a credit card. In each transaction, individuals reveal bits of personal information, like their bank and credit card account numbers; their income; their social security number; or even just name, address, and phone numbers – a goldmine of information for an identity thief. Once a thief has that information, it can be used without the individual's knowledge to commit fraud or theft. Identity theft is a serious crime. People whose identities have been stolen can spend time and money cleaning up the mess the thieves made of their good name and credit record. They may lose out on job opportunities, and loans for education, housing, or cars. They may even get arrested for crimes they did not commit.

Identity theft is a growing crime, facilitated through established, underlying crimes such as forgery, counterfeiting, check and credit card fraud, computer fraud, impersonation, pick-pocketing, and even terrorism. It became a federal crime in the United States in 1998, with the passage of the Identity Theft and Assumption Deterrence Act.

A significant feature of identity theft is the offender's repeated victimization of a single person. This may include repeatedly using a stolen credit card, taking over a card account, or using stolen personal information to open new accounts.

Here are some examples of relevant cases:

- Central District of California. A woman pleaded guilty to federal charges of using a stolen social security number to obtain thousands of dollars in credit and then filing for bankruptcy in the name of her victim. More recently, a man was indicted, pleaded guilty to federal charges and was sentenced to 27 months imprisonment for obtaining private bank account information about an insurance company's policyholders and using that information to deposit $764,000 in counterfeit checks into a bank account he established.
- Middle District of Florida. A defendant has been indicted on bank fraud charges for obtaining names, addresses, and social security numbers from a Web site and using the data to apply for a series of car loans over the Internet.
- District of Kansas. A defendant pleaded guilty to conspiracy, odometer fraud, and mail fraud for operating an odometer "rollback" scheme on used cars. The defendant used false and assumed identities, including the identities of deceased persons, to obtain false identification documents and fraudulent car titles.

Identity theft may go undetected for months and even years. Victims of identity theft may not realize that someone has stolen their identity until they are denied credit or until a creditor attempts to collect an unpaid bill. One caller to the Federal Trade Commission's identity theft hotline reported that his wallet was stolen in 1992. This consumer was unaware that he was the victim of identity theft until seven years later, when, in the summer of 1999, he was arrested on an outstanding warrant for an offense committed by the identity thief in 1993. The consumer spent several nights in jail and was forced to post $15,000 bond. He was also shocked and dismayed to discover multiple outstanding criminal charges against him in several states as a result of the identity thief's activities. This example, while unusual, is not unique. The FTC has received numerous reports from consumers who were not aware that they had been victimized by an identity thief until four or more years after the first fraudulent transaction.

For victims of identity theft, the costs can be significant and long-lasting. Where the identity thief has committed a crime in the victim's name, the harm is especially pernicious. In the worst cases, the negative consequences are never completely eradicated. For example, one consumer who called the FTC identity theft hotline reported that her income tax refund was withheld due to past child support she was believed to have owed. She found out that a child was born to a person using her name and social security number in a state she had never even visited. Another consumer reported that he was unable to renew his driver's license or register to vote because, due to crimes committed in his name by another

person, he was considered to be on probation for federal law violations including possession of drugs with intent to distribute and fraud.

Many victims have been denied employment when a background check or security clearance showed criminal records relating to an offense committed by someone using their names and social security numbers. Another consumer lost his job when, as part of his promotion review, a background check indicated that he had a criminal record. Although the consumer went to court and obtained a declaration that he did not have a criminal record, he lost his job because the company that performed the background check said that it could not clear his record.

Identity thieves can run up debts in the tens of thousands of dollars under their victims' names. Even where the individual consumer is not legally liable for these debts, the consequences to the consumer are often considerable. A consumer's credit history is frequently scarred and he or she typically must spend numerous hours over the course of months or even years contesting bills and correcting credit-reporting errors. Creditors for the fraudulent accounts often continue to harass the consumer. In the interim, the consumer victim may be denied loans, mortgages and employment; a bad credit report may even prevent him or her from something as simple as opening up a new bank account at a time when other accounts are tainted and a new account is essential. Moreover, even after the initial fraudulent bills are resolved, new fraudulent charges may continue to appear, requiring ongoing vigilance and effort by the victimized consumer.

The Identity Theft Data Clearinghouse, maintained by the FTC, provides law enforcement with the first opportunity to collect and consolidate identity theft complaints on a nationwide basis. The fruits of this effort were readily evident. The basic complaint data showed that the most common forms of identity theft reported during the first ten months of operation were:

- Credit Card Fraud - Approximately 55% of consumers reported credit card fraud -- *i.e.*, a credit card account opened in their name or a "takeover" of their existing credit card account;
- Communications Services - Approximately 28% reported that the identity thief opened up a telephone, cellular, or other utility service in their name;
- Bank Fraud - Approximately 18% reported that a checking or savings account had been opened in their name, and/or that fraudulent checks had been written; and
- Fraudulent Loans - Approximately 11% reported that the identity thief obtained a loan, such as a car loan, in their name.

Of consumer identity theft complaints related to credit cards, 72% involved the establishment of a new credit card account in the victim's name and 24% involved the takeover of an existing account. Among reports of identity theft related to a checking or savings account, 44% involved the use of unauthorized checks, 28% involved the establishment of a new checking account in the victim's name and 19% involved unauthorized electronic funds transfers.

About 55% of victims calling the identity theft hotline report their age. Of these, 40% fall between 30 and 44 years of age. Approximately 27% are between age 45 and 64 and another 22% are between age 19 and 29. About 8% of those reporting their ages are 65 and over; and over 3% are age 18 and under.

Consumers also report the harm to their reputation or daily life. The most common non-monetary harm reported by consumers is damage to their credit report through derogatory, inaccurate information. The negative credit information leads to the other problems most commonly reported by victims, including loan denials, bounced checks and rejection of credit cards. Identity theft victims also report repeated contacts by debt collectors for the bad debt incurred by the identity thief. Many consumers report that they have to spend significant amounts of time resolving these problems.

Consumers also report problems with the banks and other institutions that provided the credit, goods or services to the identity thief in the consumer's name. These institutions often attempt to collect the bad debt from the victim, or report the bad debt to a consumer-reporting agency, even after the victim believes that he or she has demonstrated the fraud. Of consumers lodging identity theft-related complaints with the Clearinghouse, 29% reported complaints about a bank credit card issuer, 25% reported complaints about a bank creditor and 22% reported complaints about a depository institution.

The majority of consumer complaints related to bank credit card issuers, bank creditors and depository institutions fall into three categories:

- The institution refused to correct information or close the disputed account;
- Customer service personnel were not helpful; and
- The institution's security procedures were inadequate.

# III. SUMMARY OF FEDERAL LAWS

## A. IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT

The Identity Theft and Assumption Deterrence Act, enacted by Congress in October 1998 (and codified, in part, at 18 U.S.C. §1028) makes identity theft a federal crime. Under federal criminal law, identity theft takes place when someone *"knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."* The unauthorized use of another individual's name, social security number, or date of birth to apply for a credit card is punishable by fine or imprisonment under this Act. The Act also mandated that the FTC establish a central complaint system to receive and refer identity theft complaints to appropriate entities, including law enforcement agencies and national credit bureaus.

Violations of the federal crime are investigated by federal law enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and the social security Administration's Office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice.

Violation of the Act, in most circumstances, carries a maximum term of 15 years imprisonment, a fine, and criminal forfeiture of any personal property used or intended to be used to commit the offense.

## B. GRAMM-LEACH-BLILEY ACT

The Gramm-Leach-Bliley Act, which was enacted in 1999, prohibits the making of false or fraudulent statements or representations to an officer, employee or agent of a financial institution, or to a customer of a financial institution, in order to obtain consumer information. The Act also prohibits anyone from requesting a person to obtain customer information of a financial institution, knowing that the person will use fraudulent methods to obtain information from the institution. The Act also imposes criminal sanctions for knowing and intentional violations of these provisions.

While this statute is generally aimed at persons who victimize banks and their customers by attempting to obtain customer information through "pretexting," banks could themselves be in violation of this statute if they use the services of any person who obtains customer information in violation of the statute. Although the statute requires that the institution must "know" that the person will use artifice to obtain customer information, safe and sound banking practices dictate that a bank exercise reasonable diligence in selecting a third party to gather customer information.

This law also places numerous requirements on tax preparers and other financial institutions to provide notice to customers and clients about how the business maintains records to ensure privacy and mandates the safeguarding of customer records.

## C. FREE CREDIT REPORT

An important way for everybody to keep a watchful eye on their credit is through a periodic review of their credit report. An amendment to the federal Fair Credit Reporting Act requires each of the major nationwide consumer reporting companies to provide individuals with a free copy of their credit report, upon request, once every 12 months. Beginning September 1, 2005, free reports are available to all Americans, regardless of where they live.

A free annual report can be obtained from one or all the national consumer reporting companies. Interested persons can visit: *www.annualcreditreport.com*; call toll-free: 877-322-8228; or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Under federal law, individuals are also entitled to a free report if a company takes adverse action against them, such as denying an application for credit, insurance or employment. Such persons may request their report within 60 days of receiving notice of the action. The notice will provide the individual the name, address, and phone number of the consumer reporting company that supplied the information about them. Such individuals are also entitled to one free report a year if they are unemployed and plan to look for a job within 60 days; if they are on welfare; or if their report is inaccurate because of fraud. Otherwise, a consumer reporting company may charge individuals up to $12.00 for additional copies of their report. Under state law, consumers in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont already have free access to their credit reports. If requested, only the last four digits of the individual's social security number will appear on their credit reports.

## D. OTHER FEDERAL STATUTES

Schemes to commit identity theft or fraud may also involve violations of other statutes such as identification fraud (18 U.S.C. § 1028), credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), or financial institution fraud (18 U.S.C. § 1344). Each of these federal offenses are felonies that carry substantial penalties in some cases, as high as 30 years' imprisonment, fines, and criminal forfeiture. Another federal law, enacted in 2004, creates the crime of aggravated identity theft when someone uses another person's identity in the perpetration of a crime.

## E. STATE LAWS

Most, if not all, states have passed laws making identity theft a crime or providing help in recovery from identity theft; others are considering such legislation. States also now govern related issues such as the destruction of personal customer information. Businesses must be aware of laws in their jurisdiction as well as professional codes that might govern records maintenance.

## CHAPTER 1: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

| | |
|---|---|
| **1.** | **In 2019, which age range was most often the victim of identity theft:**<br><br>**A.** 20 to 29<br><br>**B.** 30 to 39<br><br>**C.** 50 to 59<br><br>**D.** 70 to 79 |
| **2.** | **Which of the following statements about the Gramm-Leach-Bliley Act is <u>not</u> correct:**<br><br>**A.** it requires major credit reporting agencies to provide consumers with a free copy of their credit report annually<br><br>**B.** it is aimed at stopping persons who victimize banks and its customers<br><br>**C.** it requires tax preparers to provide notice to consumers about how they maintain records<br><br>**D.** it prohibits the making of false statements to financial institutions |

## CHAPTER 1: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

| | |
|---|---|
| **1.** | **A.** Incorrect. While this youngest group does report being victimized by identity theft, other young people report being victimized more.<br><br>**B.** **CORRECT**. While it might seem logical for older people to be more commonly victimized, this group was indeed victimized more than any other in 2019.<br><br>**C.** Incorrect. This age group is not the group reporting the most cases of identity theft.<br><br>**D.** Incorrect. While older Americans are indeed victims of identity theft, it is people 30 to 39 who reported being victimized the most in 2019.<br><br>*(See page 2 of the course material.)* |
| **2.** | **A.** **CORRECT**. This is a requirement of the Fair Credit Reporting Act, not the Gramm-Leach-Bliley Act.<br><br>**B.** Incorrect. The Act does prohibit false or fraudulent statements to bank officers or employees.<br><br>**C.** Incorrect. Other businesses are also required to provide notices to consumers about how their records are maintained.<br><br>**D.** Incorrect. This is one of the centerpieces of the Act.<br><br>*(See page 12 of the course material.)* |

# CHAPTER 2: COMMON SCHEMES OF IDENTITY THEFT

## Chapter Objective

**After completing this chapter, you should be able to:**

- Identify common schemes used in perpetrating identity theft.

The term "Internet fraud" refers generally to any type of fraud scheme that uses one or more components of the Internet – such as chat rooms, e-mail, message boards, or websites – to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

Some Internet fraud schemes also involve identity theft – the wrongful obtaining and using of someone else's personal data in some way that involves fraud or deception, typically for economic gain. In one federal prosecution, the defendants allegedly obtained the names and social security numbers of U.S. military officers from a website, and then used more than 100 of those names and numbers to apply, via the Internet, for credit cards with a Delaware bank. In another federal prosecution, the defendant allegedly obtained personal data from a federal agency's website, and then used the personal data to submit 14 car loan applications online to a Florida bank.

Anyone who uses the Internet with any frequency will see that people and things online tend to move, as the saying goes, on "Internet time." For most people, that phrase simply means that things seem to happen more quickly on the Internet – business decisions, information-searching, personal interactions, to name a few – and to happen before, during, or after ordinary "bricks-and-mortar" business hours. Unfortunately, people who engage in fraud often operate in "Internet time" as well. They seek to take advantage of the Internet's unique capabilities – for example, by sending e-mail messages worldwide in seconds, or posting website information that is readily accessible from anywhere in the world – to carry out various types of fraudulent schemes more quickly than was possible with many fraud schemes in the past.

With the rise in credit card monitoring and more sophisticated policing by credit card companies, identity thieves are increasingly targeting users of smartphones and social media, where consumers have a tendency to be less cautious. Unlike traditional computers, they're always with you, and messages that arrive on them are more trusted than traditional email and landline phone calls. Studies indicate that smartphone owners are three times more likely to fall for identity-stealing "phishing" scams than those sent to a PC or Mac.

## I. PRETEXTING

When an individual thinks of their personal assets, it is likely that things like their home, car, savings accounts and investments come to mind. But what about the individual's social security number, telephone

records or bank and credit card account numbers? To people known as "pretexters," that information is also a personal asset. Pretexting is the practice of getting an individual's personal information under false pretenses. Pretexters typically sell this information to people who may use it to obtain credit under the victim's name, steal the victim's assets, or even sue the victim. Pretexting is a violation of federal law.

### A. HOW PRETEXTING WORKS

Pretexters use a variety of tactics to obtain an individual's personal information. For example, a pretexter may call, claim he or she is from a survey firm and ask a few questions. When the pretexter has the information he or she wants, he uses it to call the victim's financial institution. He pretends to be the victim or someone with authorized access to the victim's account. He might claim that he has forgotten his checkbook and needs information about his account. In such a way, the pretexter may be able to obtain personal information about the victim such as their social security number, bank and credit card account numbers, information in the victim's credit report, and the existence and size of the victim's savings and investment portfolios. Keep in mind that some information about everyone is a matter of public record, i.e., whether an individual owns their home or other real property or whether the individual has ever filed for bankruptcy protection. It is not pretexting for another person to collect this type of information.

### B. THE LAW

Under the federal law (Gramm-Leach-Bliley (GLB) Act), it is illegal for anyone to:

- Use false, fictitious, or fraudulent statements or documents to obtain customer information from a financial institution or directly from a customer of a financial institution;
- Use forged, counterfeit, lost or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution;
- Ask another person to get someone else's customer information using false, fictitious or fraudulent statements, or using false, fictitious or fraudulent documents or forged, counterfeit, lost or stolen documents.

The Federal Trade Commission Act also generally prohibits pretexting for sensitive consumer information.

## II. PHISHING

"Phishing" is a general term for criminals' creation and use of e-mails and websites – designed to look like e-mails and websites of well-known legitimate businesses, financial institutions, and government agencies – in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords. The "phishers" then take that information and use it for criminal purposes, such as identity theft and fraud.

A growing number of phishing schemes are using for illegal purposes the names and logos of legitimate financial institutions, businesses, and government agencies in North America, Europe, and the Asia-Pacific region.

## A. RISKS OF RESPONDING TO PHISHING E-MAILS

At first glance, phishing e-mails, and the websites associated with such e-mails, may appear completely legitimate. One past phishing attempt falsely used the names of the Federal Deposit Insurance Corporation (FDIC) and two of its officials, as well as the Department of Homeland Security. What Internet users may not realize is that criminals can easily copy logos and other information from legitimate businesses' websites and place them into phishing e-mails and websites.

In addition, if the e-mail recipient clicks on the link in the e-mail, even the window of the Internet browser he or she is using may contain what looks like the true Uniform Resource Locator (URL) of a legitimate business or financial institution. Unfortunately, some phishing schemes have exploited vulnerability in the Internet Explorer browser. This vulnerability allows phishers to set up a fake website at one place on the Internet, but make it look like the Internet user is accessing a legitimate website at another place on the Internet. Most phishing e-mails include false statements intended to create the impression that there is an immediate threat or risk to the bank, credit-card, or financial account of the person who receives that e-mail.

In the case of the false FDIC e-mails mentioned above, the text of the e-mails falsely claimed that the Secretary of Homeland Security had advised the FDIC to suspend all federal deposit insurance on the recipients' bank accounts. Other recent phishing e-mails have falsely claimed that the recipients' Visa credit card was being used by another person, or that a recent credit card transaction had been declined.

In some cases, phishing e-mails have promised the recipients a "prize" or other special benefit. Although the message sounds attractive rather than threatening, the object is the same: to trick recipients into disclosing their financial and personal data.

People who receive phishing e-mails also may not realize that the senders may have used "spamming" (mass e-mailing) techniques to send the e-mail to thousands and thousands of people. This means that many of the people who receive that spammed e-mail do not have accounts or customer relationships with the legitimate business or financial services company that the e-mails purport to come from. The people who create phishing e-mails count on the fact that some recipients of those e-mails will have an account or customer relationship with that legitimate business or company, and may be more likely to believe that the e-mail has come from a trusted source.

Ultimately, people who respond to phishing e-mails, and input the requested financial or personal information into e-mails, websites, or pop-up windows, may be putting their accounts and financial status at risk in three significant ways:

- First, phishers can use the data to access existing accounts of those Internet users, and withdraw money or buy expensive merchandise or services;

- Second, phishers can use the data to open new bank or credit card accounts in the victims' names, and use the new accounts to cash bogus checks or buy merchandise. Internet users may not realize that they have become victims of identity theft until they are contacted by creditors or they check their credit reports; and
- Third, some recent phishing schemes have involved the use of computer viruses and worms to disseminate the phishing e-mails to still more people.

## B. APPLICATION OF FEDERAL CRIMINAL LAWS

Because they use false and fraudulent statements to deceive people into disclosing valuable personal data, phishing schemes may violate a variety of federal criminal statutes. In many phishing schemes, the participants in the scheme may be committing identity theft (18 U.S.C. § 1028(a)(7)), wire fraud (18 U.S.C. § 1343), credit card (or "access-device") fraud (18 U.S.C. § 1029), bank fraud (18 U.S.C. § 1344), computer fraud (18 U.S.C. § 1030(a)(4)), and the enacted criminal offenses in the CAN-SPAM Act (18 U.S.C. § 1037).

When a phishing scheme also uses computer viruses or worms, participants in the scheme may also violate other provisions of the computer fraud and abuse statute relating to damage to computer systems and files (18 U.S.C. § 1028(a)(5)). Finally, phishing schemes may violate various state statutes on fraud and identity theft.

Each of the federal criminal offenses mentioned above carries substantial penalties. Sentences can range from as high as 30 years imprisonment under the wire fraud and bank fraud statutes, to 15 years imprisonment for identity theft and credit card fraud, and 5 years imprisonment under the CAN-SPAM Act. In addition, federal judges can impose substantial fines, which can be as high as $250,000 for an individual, and require forfeiture of a defendant's property. The Department of Justice has already successfully prosecuted a number of criminal cases involving phishing.

## C. SUGGESTIONS

Federal authorities recommend that Internet users follow three simple rules when they see e-mails or websites that may be part of a phishing scheme: ***Stop***, ***Look***, and ***Call***.

1. Stop

Phishers typically include upsetting or exciting (but false) statements in their e-mails with one purpose in mind. They want people to react immediately to that false information, by clicking on the link and inputting the requested data before they take time to think through what they are doing. Internet users, however, need to resist that impulse to click immediately. No matter how upsetting or exciting the statements in the e-mail may be, there is always enough time to check out the information more closely.

2. Look

Internet users should look more closely at the claims made in the e-mail, think about whether those claims make sense, and be highly suspicious if the e-mail asks for numerous items of their personal information such as account numbers, usernames, or passwords. For example:

- If the e-mail indicates that it comes from a bank or other financial institution where the individual has a bank or credit card account, but tells them that they have to enter their account information again, that makes no sense. Legitimate banks and financial institutions already have their customers' account numbers in their records. Even if the e-mail says a customer's account is being terminated, the real bank or financial institution will still have that customer's account number and identifying information; and
- If the e-mail says that the recipient has won a prize or is entitled to receive some special "deal," but asks for financial or personal data, there is good reason to be highly suspicious. Legitimate companies that want to give a real prize do not ask the recipient for extensive amounts of personal and financial information before they are entitled to receive it.

3. Call

If the e-mail or website purports to be from a legitimate company or financial institution, Internet users should call or e-mail that company directly and ask whether the e-mail or website is really from that company. To be sure that they are contacting the real company or institution where they have accounts, credit card accountholders can call the toll-free customer numbers on the backs of their cards, and bank customers can call the telephone numbers on their bank statements.

A number of legitimate companies and financial institutions that have been targeted by phishing schemes have published contact information for reporting possible phishing e-mails, as well as online notices about how their customers can recognize and protect themselves from phishing. This list will be periodically updated as appropriate.

## III. SMISHING AND VISHING

You receive a text message or an automated phone call on your cell phone saying there's a problem with your bank account. You're given a phone number to call or a website to log into and asked to provide personal identifiable information – like a bank account number, PIN, or credit card number – to fix the problem.

But beware: It could be a "smishing" or "vishing" scam…and criminals on the other end of the phone or website could be attempting to collect your personal information in order to help themselves to your money. While most cyber scams target your computer, smishing and vishing scams target your mobile phone, and they have become a growing threat as a growing number of Americans own mobile phones. Vishing scams also target land line phones.

"Smishing" (a combination of SMS texting and phishing) and "Vishing" (voice and phishing) are two of the scams the FBI's Internet Crime Complaint Center (IC3) is warning consumers about. These scams are also a reminder that cybercrimes aren't just for computers anymore.

### A. HOW IT WORKS

Here's how smishing and vishing scams work: criminals set up an automated dialing system or text or call people in a particular region or area code (or sometimes they use stolen customer phone numbers

from banks or credit unions). The victims receive messages like: “There’s a problem with your account,” or “Your ATM card needs to be reactivated,” and are directed to a phone number or website asking for personal information. Armed with that information, criminals can steal from victims’ bank accounts, charge purchases on their credit cards, create a phony ATM card, etc.

Sometimes, if a victim logs onto one of the phony websites with a smartphone, they could also end up downloading malicious software that could give criminals access to anything on the phone. With the growth of mobile banking and the ability to conduct financial transactions online, smishing and vishing attacks may become even more attractive and lucrative for cyber criminals.

1. Text Messaging Spam Is a Triple Threat

- It often uses the promise of free gifts, like computers or gift cards, or product offers, like cheap mortgages, credit cards, or debt relief services to get you to reveal personal information. If you want to claim your gift or pursue an offer, you may need to share personal information, like how much money you make, how much you owe, or your bank account information, credit card number, or social security number. Clicking on a link in the message can install malware that collects information from your phone. Once the spammer has your information, it is sold to marketers or, worse, identity thieves.
- It can lead to unwanted charges on your cell phone bill. Your wireless carrier may charge you simply for receiving a text message, regardless of whether you requested it.
- It can slow cell phone performance by taking up space on your phone’s memory.

## B. RELEVANT CASES

- Account holders at one particular credit union, after receiving a text about an account problem, called the phone number in the text, gave out their personal information, and had money withdrawn from their bank accounts within 10 minutes of their calls.
- Customers at a bank received a text saying they needed to reactivate their ATM card. Some called the phone number in the text and were prompted to provide their ATM card number, PIN, and expiration date. Thousands of fraudulent withdrawals followed.

## C. TEXT MESSAGE SPAM IS ILLEGAL

It’s illegal to send unsolicited commercial email messages to wireless devices, including cell phones and pagers, unless the sender gets your permission first. It’s also illegal to send unsolicited text messages from an auto-dialer – equipment that stores and dials phone numbers using a random or sequential number generator.

Exceptions to the law:

- Transactional or relationship types of messages. If a company has a relationship with you, it can send you things like statements or warranty information.

- Non-commercial messages. This includes political surveys or fundraising messages.

### D. CAN THE SPAM

Here are a few steps to can text message spam:

- Delete text messages that ask you to confirm or provide personal information: Legitimate companies don't ask for information like your account numbers or passwords by email or text.
- Don't reply, and don't click on links provided in the message: Links can install malware on your computer and take you to spoof sites that look real but whose purpose is to steal your information.
- Treat your personal information like cash: Your social security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. Don't give them out in response to a text.
- Place your cell phone number on the National Do Not Call Registry.
- If you are an AT&T, T-Mobile, Verizon, Sprint or Bell subscriber, you can report spam texts to your carrier by copying the original message and forwarding it to the number 7726 (SPAM), free of charge.
- Review your cell phone bill for unauthorized charges, and report them to your carrier.
- If you receive unwanted commercial text messages, file a complaint with the FTC. The Federal Communications Commission (FCC) also accepts complaints about unwanted text messages.

## IV. SKIMMING

Be wary when you use automated teller machines (ATMs) and other payment processing machines. Thieves may be using high-tech tools in scams to capture your account information to steal your money.

These scams, known as "card skimming," involve attaching devices to money machines that read the information on your debit and credit cards when you swipe them. When combined with a nearby concealed camera to record your personal identification number (PIN), the thieves can get everything they need to drain your account or to make unauthorized purchases. In addition to using the information directly, thieves may sell your information to others.

ATMs and automated payment machines in airports, convenience stores, hotel lobbies, and other well-traveled, public places may be most vulnerable to thieves who may think these machines are not regularly inspected by the machine owners. However, card skimming may take place at any ATM or card processing machine, including those on bank premises. As technology makes these devices smaller and more powerful, the risk of card skimming grows.

## A. HOW HIGH-TECH THIEVES OPERATE

Thieves have many ways to steal your account information. They may attach a card skimmer that looks and acts like a genuine part of the ATM or other type of money machine. The device may be a simple, curved plastic sheath over the card slot. The skimmer reads the magnetic strip or computer chip on your card and transmits your account information to the thieves or saves the information until the skimmer is retrieved.

Thieves may also use a wireless camera concealed nearby in a box holding brochures or in a light fixture. The camera photographs or videotapes your fingers as they enter your PIN on a keypad or screen. Like a card skimmer, the camera can transmit images instantly or save them until the thieves retrieve the camera later. A camera and card skimmer can be used together.

## B. SAFEGUARDING YOUR PERSONAL BANK ACCOUNT INFORMATION

To help protect you, banks and retailers take measures to minimize the risk of fraudulent use of your debit or credit card, particularly when those purchases are made by telephone or online.

Before approving telephone purchases, retailers typically confirm your identity by asking for personal information. They may ask for your address, the last four digits of your social security number, or answers to security questions you created when you set up your account. Retailers also may ask for the three-digit security code printed on the front or back of your debit or credit card. To protect your online transaction from electronic fraud, many commercial Web sites require you to unscramble a word or a number displayed as a fuzzy or distorted image that is difficult for software to read.

Ultimately, you must protect yourself against thieves and the tools they use to access your accounts to steal from you. To protect yourself, follow these common-sense precautions.

- Walk away from an ATM if you notice someone watching you or if you sense something wrong with the machine; immediately report your suspicions to the company operating the machine or a nearby law enforcement officer.
- Before using an ATM, examine nearby objects that might conceal a camera; check the card slot for a plastic sheath before inserting your card.
- Never keep a written copy of your PIN in your wallet or purse as it could be stolen; instead memorize your PIN and keep a paper record hidden at home.
- Beware of strangers offering to help you with an ATM that appears disabled and notify someone responsible for the security of the machine.
- Regularly review your account statements, either online or on paper, and check for unauthorized withdrawals and purchases. If you find one, immediately contact your bank or credit card provider, as this will limit your financial liability for fraudulent charges.

# V. FEDERAL ENFORCEMENT

The FTC uses a variety of tools to protect consumers' privacy and personal information. The FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take steps to remediate the unlawful behavior. This has included, when appropriate, implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and providing robust transparency and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, the Telemarketing Sales Rule, the Fair Debt Collection Practices Act, and the CAN-SPAM Act.

Using its existing authority, the Commission has brought hundreds of privacy and data security cases to date. To better equip the Commission to meet its statutory mission to protect consumers, the FTC has also called on Congress to enact comprehensive privacy and data security legislation, enforceable by the FTC. The requested legislation would expand the agency's civil penalty authority, provide the agency with targeted rulemaking authority, and extend the agency's commercial sector jurisdiction to non-profits and common carriers as well.

The FTC, building on decades of experience in consumer privacy enforcement, continued in 2019 to conduct investigations and bring cases addressing practices offline, online, and in the mobile environment, as described below. The FTC's cases generally focus on protecting American consumers, but in some cases also protect foreign consumers from unfair or deceptive practices by businesses subject to the FTC's jurisdiction.

The FTC has brought enforcement actions addressing a wide range of privacy issues in a variety of industries, including social media, ad tech, and the mobile app ecosystem. These matters include more than 130 spam and spyware cases and 80 general privacy lawsuits. In 2019, the FTC announced the following privacy cases:

## A. FACEBOOK

On July 24, 2019, the Commission and the U.S. Department of Justice announced a settlement with Facebook. The complaint alleged that Facebook violated the Commission's 2012 order against the company by misrepresenting the control users had over their personal information, and failing to institute and maintain a reasonable program to ensure consumers' privacy. It also alleged that Facebook deceptively failed to disclose that it would use phone numbers provided by users for two-factor authentication for targeted advertisements to those users. The Facebook order imposed a $5 billion penalty, as well as a host of modifications to the Commission's order designed to change Facebook's overall approach to privacy. The $5 billion penalty against Facebook is the largest ever imposed on any company for violating consumers' privacy.

## B. CAMBRIDGE ANALYTICA

In a related, but separate case, the FTC also filed a law enforcement action against the data analytics company Cambridge Analytica, as well as its former Chief Executive Officer, Alexander Nix, and app developer, Aleksandr Kogan. The FTC's complaint alleged that Cambridge Analytica, Nix, and Kogan used false and deceptive tactics to harvest personal information from millions of Facebook users for voter profiling and targeting. The complaint alleged that app users were falsely told the app would not collect users' names or other identifiable information.

Contrary to this claim, the complaint alleged, the app collected users' Facebook User ID, which connects individuals to their Facebook profiles. Kogan and Nix agreed to settlements with the FTC that restrict how they conduct any business in the future, and the Commission entered a default judgment against Cambridge Analytica. The Commission's opinion holds that Cambridge Analytica violated the FTC Act through the deceptive conduct and reaffirms the proposition that, like any other claim, a company's privacy promises are viewed through the lens of established FTC consumer protection principles.

## C. RETINA-X

The FTC brought its first action against a developer of stalking apps – software that allows purchasers to monitor the mobile devices on which they are installed, without users' knowledge. In its complaint, the FTC alleged, among other things, that Retina-X sold apps that required circumventing certain security protections implemented by the mobile device operating system or manufacturer, and did so without taking reasonable steps to ensure that the apps would be used only for legitimate and lawful purposes. The complaint alleged that the company's practices enabled use of its apps for stalking and other illegitimate purposes.

The proposed order requires the company and its owner to refrain from selling products or services that monitor devices, without taking steps to ensure that the products or services will be used for legitimate purposes.

## D. UNROLLME, INC.

Unrollme, Inc., an email management company, settled allegations that it deceived consumers about how it accesses and uses their personal emails. According to the complaint, Unrollme falsely told consumers that it would not "touch" their personal emails in order to persuade consumers to provide access to their email accounts. In fact, the complaint alleged, Unrollme was sharing the consumers' email receipts, which can include, among other things, the user's name, billing, and shipping addresses, and information about products or services purchased by the consumer with its parent company, Slice Technologies, Inc. According to the complaint, Slice used anonymous purchase information from Unrollme users' e-receipts in the market research analytics products it sells. As part of the settlement with the Commission, Unrollme is prohibited from misrepresenting the extent to which it collects, uses, stores, or shares information from consumers. It is also required to notify consumers and delete the data unlawfully collected from consumers, unless it obtains their affirmative, express consent to maintain the e-receipts.

## E. EFFEN ADS

In Effen Ads, LLC (iCloudWorx), the FTC obtained stipulated final orders against defendants that promoted a work-from-home program through unsolicited email, or spam, claiming that consumers could make significant income with little effort. The spam emails included misleading "from" lines and links to websites that falsely claimed that various news sources had favorably reviewed the program, and "subject" lines that displayed false celebrity endorsements. The stipulated final orders permanently ban defendants from marketing or selling either work-from-home programs or business opportunities or business coaching products, and permanently enjoined them from violating the CAN-SPAM Act. The orders also impose judgments totaling more than $12.6 million, and require defendants to pay nearly $1.5 million in partial satisfaction of the judgments.

## F. GLOBAL ASSET FINANCIAL SERVICES GROUP

In Global Asset Financial Services Group, LLC, the FTC shut down a phantom debt brokering and collection scheme. The Commission charged the defendants with purchasing and collecting on counterfeit debts fabricated from misappropriated information about consumers' identities as well as finances and debts purportedly owed on bogus "autofunded" payday loans. In numerous instances, defendants also disclosed consumers' purported debts to third parties. The final orders, imposing a combined judgment of more than $13 million, ban all the defendants from the debt collection business and from misleading consumers about debt. They also prohibit defendants from profiting from customers' personal information collected as part of the challenged practices, and failing to dispose of such information properly.

## G. HYLAN ASSET MANAGEMENT

In Hylan Asset Management, LLC, the FTC and the New York Attorney General's Office charged two operations – Hylan Asset Management, LLC and its related companies (Hylan) and Worldwide Processing Group, LLC (Worldwide) – as well as their principals with buying, placing for collection, and selling lists of phantom debts, including debts that were fabricated by the defendants or disputed by consumers. The Commission alleged that the defendants obtained consumers' private financial information and then used it to convince consumers they were legitimate collectors calling about legitimate debts. The FTC also alleged that, in numerous instances, the Worldwide defendants unlawfully communicated with third parties where they already possessed contact information for the consumer. The FTC secured final orders banning the Hylan defendants from the debt collection industry and prohibiting the Worldwide defendants from unlawful debt collection practices. The orders prohibit all defendants from using customers' personal information and failing to properly dispose of that information.

## H. ACDI GROUP

In ACDI Group, the Commission charged the defendants with collecting on a portfolio of counterfeit payday loan debts, which included financial information, such as social security and bank account numbers. When the defendants reported to the debt broker who had sold them the portfolio that they had received consumer complaints regarding the legitimacy of the debts, the broker returned the defendants' money and told them to stop collecting; however, the defendants allegedly continued to do so for at least

seven more months. The final order, entered in December 2019, requires the defendants to provide full redress to injured consumers and prohibits the defendants from disclosing, using, or benefitting from previously obtained consumer information that is unverified.

## I. DATA SECURITY AND IDENTITY THEFT

Since 2002, the FTC has brought more than 70 cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data. In 2019, the FTC strengthened its standard orders in data security cases. Each of the cases discussed below resulted in settlements that, among other things, required the companies to implement a comprehensive security program, obtain robust biennial assessments of the program, and submit annual certifications by a senior officer about the company's compliance with the order.

The FTC's complaint against Equifax alleged that the company failed to secure the massive amount of personal information stored on its network. Among other things, the company allegedly failed to patch well-known software vulnerabilities, failed to segment its database servers, and stored social security numbers in unencrypted, plain text. According to the complaint, these failures led to a breach that affected more than 147 million people, and exposed millions of names and dates of birth, social security numbers, physical addresses, and other personal information that could lead to identity theft and fraud. The settlement, which totals between $575 million and $700 million, was part of a global resolution where Equifax settled matters with a consumer class action, the Consumer Financial Protection Bureau, and 50 states and territories.

In July 2019, the FTC announced a complaint and settlement against the operator of ClixSense.com, an online rewards website that pays its users to view advertisements, perform online tasks, and complete online surveys. The complaint alleged that the website's operator, James V. Grago, Jr., deceived consumers by falsely claiming that ClixSense "utilizes the latest security and encryption techniques to ensure the security of your account information." In fact, ClixSense failed to implement minimal data security measures and stored personal information, including social security numbers, in clear text with no encryption, according to the complaint. The FTC alleged that ClixSense's failures allowed hackers to gain access to the company's network, resulting in a breach of 6.6 million consumers' information.

The FTC settled charges against Unixiz, dba i-Dressup.com, a dress-up games website, alleging that the company and its owners stored and transmitted users' personal information in plain text and failed to perform vulnerability testing of its network, implement an intrusion detection and prevention system, and monitor for potential security incidents. These failures led to a security breach in which a hacker accessed the information of approximately 2.1 million users, including approximately 245,000 users who indicated they were under 13.

As discussed above, the FTC alleged that Retina-X, a company that sold so-called "stalking apps," and its owner claimed that, "Your private information is safe with us." Despite this claim, the company and its owner failed to adopt and implement reasonable information security policies and procedures.

## J. CHILDREN'S PRIVACY

The Children's Online Privacy Protection Act of 1998 ("COPPA") generally requires websites and apps to obtain verifiable parental consent before collecting personal information from children under 13. Since 2000, the FTC has brought close to 30 COPPA cases and collected hundreds of millions of dollars in civil penalties. During 2019, the Commission took the following actions:

The FTC's settlement with Google and its subsidiary YouTube brought, in conjunction with the New York Attorney General, alleges that the company collected kids' personal data without parental consent, in violation of the COPPA Rule. The complaint alleges that YouTube violated the COPPA Rule by collecting personal information, including in the form of persistent identifiers that are used to track users across the Internet from viewers of child-directed channels, without first notifying parents and getting their consent. The $170 million judgment represents the largest civil penalty amount under COPPA.

Musical.ly, now known as TikTok, is the operator of a video social networking app that allows users to create short videos of themselves lip-syncing to music and to share those videos with other users. In 2019, the company paid $5.7 million to settle charges that it violated COPPA by illegally collecting personal information from children. The complaint alleged the app was child-directed, and that many users self-identified as being under 13.

The FTC's complaint against Unixiz, Inc., dba i-Dressup.com, alleged that the company and its principals violated COPPA by failing to obtain verifiable parental consent before collecting personal information from children under 13. To gain access to all the features on the website, including the social networking features, users had to register as members by submitting a username, password, birthdate, and email address. If a user indicated he or she was under 13, the registration field asked for a parent's consent. If a parent declined to provide consent, the under-13 users were given a "Safe Mode" membership allowing them to login to access i-Dressup's games and features but not its social features. The FTC alleges, however, that i-Dressup still collected personal information from these children, even if their parents did not provide consent.

## CHAPTER 2: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

| | |
|---|---|
| 1. | **What does the term "phishing" refer to:**<br><br>**A.** hiring a private investigator to find out who has stolen your identity<br><br>**B.** stealing mail to obtain personal information<br><br>**C.** the use of e-mails or the Internet to obtain sensitive personal information<br><br>**D.** making fraudulent phone calls to obtain personal information |
| 2. | **The Federal Trade Commission in 2019 imposed a $5 billion penalty on Facebook for which of the following actions:**<br><br>**A.** deceptively failing to alert Facebook users that it would use phone numbers that it collected for authentication purposes for targeted advertisements<br><br>**B.** violating the FTC's 2012 order against the company<br><br>**C.** failing to maintain a reasonable program to protect the privacy of consumers<br><br>**D.** all of the above |

## CHAPTER 2: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

| | |
|---|---|
| **1.** | **A.** Incorrect. Phishing refers to the actions of identity thieves, not the actions of the victims.<br><br>**B.** Incorrect. Stealing mail is a common method of obtaining personal information for identity thieves, but is not phishing.<br><br>**C.** **CORRECT**. Phishing is a very common tactic being used now by identity thieves. People need to be very careful about providing sensitive information through the Internet or e-mails.<br><br>**D.** Incorrect. Making fraudulent phone calls is referred to as "pretexting."<br><br>*(See page 20 of the course material.)* |
| **2.** | **A.** Incorrect. The FTC did impose a penalty on Facebook for inappropriately using phone numbers it collected for legitimate reasons for target advertisement. However, this is not the only correct option.<br><br>**B.** Incorrect. The 2019 complaint imposing a $5 billion fine did allege the company violated the FTC's 2012 order, but other actions also apply.<br><br>**C.** Incorrect. This was indeed part of the allegation that resulted in the fine, but it was only part of the allegation.<br><br>**D.** **CORRECT**. A, B and C all formed the basis of the FTC's imposition of a $5 billion fine on Facebook in 2019.<br><br>*(See page 27 of the course material.)* |

# CHAPTER 3: VICTIMS OF IDENTITY THEFT

## Chapter Objectives

**After completing this chapter, you should be able to:**

- Recall the impacts of using fraud alerts.
- Recall an individual's limited responsibility for unauthorized credit card charges.

As we saw in Chapter 1, one of the problems associated with identity theft is the large amount of time it often takes its victims to discover the crime. The process of determining whether or not you are a victim of this crime is therefore very important in combating its many adverse effects.

## Signs of Identity Theft

- Unexpected phone calls from creditors. If you receive a call from a creditor demanding payment for a purchase that you did not make, get all the information possible about the transaction and investigate it promptly;
- Strange credit card charges. It is easier to spot these if you keep all of your receipts from credit card charges and reconcile your statement at the end of the month;
- Unexpectedly being denied credit. If you try to open a store credit card and you have impeccable credit, it is a red flag if you get turned down;
- Account usernames and passwords for ATMs stop working. If this happens, it is a sign that an identity thief may have changed your access codes and passwords;
- Missing bills. If you stop receiving expected bills, it could be a sign that your address has been changed by an identity thief;
- Receiving credit cards for which you did not apply. This can happen in the absence of identity theft, but it is a red flag that should be looked into; and
- Strange information in your files. Anything that does not match could be a sign of a major problem. Investigate immediately.

## I. STEPS FOR VICTIMS OF IDENTITY THEFT

If anyone thinks that they have become the victim of identity theft or fraud – or even if they have merely lost personal identification – it is important that they act immediately to minimize the damage to their personal funds and financial accounts, as well as their reputation. The following are some actions that persons should take right away, including contacting the Federal Trade Commission to report the situation.

## A. IMMEDIATE ACTION RECOMMENDED

1. Place a Fraud Alert on Your Credit Report

Fraud alerts can help prevent an identity thief from opening any more accounts in the victim's name. Individuals can contact the toll-free fraud number of any of the three consumer reporting companies to place a fraud alert on their credit report. Individuals only need to contact one of the three companies to place an alert. The company the individual calls is required to contact the other two, which will also place an alert on their versions of the victim's credit report.

Once victims place the fraud alert in their file, they will become entitled to order free copies of their credit reports, and, if they request, only the last four digits of their social security number will appear on the credit reports. Once a victim obtains their credit report, they should review it carefully. They should look for companies they have not contacted, accounts they did not open, and debts on accounts that they cannot explain. They should also check that information like their social security number, address(es), name or initials, and employers are correct. When they find fraudulent or inaccurate information, they should contact the consumer reporting companies to get it removed. A victim should continue to check their credit reports periodically, especially for the first year after they discover the identity theft, to make sure no new fraudulent activity has occurred.

Victims may even wish to request a free copy of their credit report every few months so they can monitor for fraud. Laws in the victim's state may provide additional rights. Under a California law, for example, victims are able to receive one free report each month for the first 12 months upon request. (California Civil Code 1785.15.3, effective July 1, 2003.) In other states, a victim may be charged after the first report. Still, it is important that a victim check their credit report about every three months during the active phase of the crime.

California law also enables individuals to place a "security freeze" on their credit reports pursuant to Civil Code Section 1785.11.1, below. This essentially prevents anyone from accessing another person's credit file for any reason, until and unless they instruct the credit bureaus to unfreeze or "thaw" their report. It provides more protection than a fraud alert.

### California Civil Code 1785.11.1

1785.11.1. (a) A consumer may elect to place a security alert in his or her credit report by making a request in writing or by telephone to a consumer credit reporting agency. "Security alert" means a notice placed in a consumer's credit report, at the request of the consumer, that notifies a recipient of the credit report that the consumer's identity may have been used without the consumer's consent to fraudulently obtain goods or services in the consumer's name.

(b) A consumer credit reporting agency shall notify each person requesting consumer credit information with respect to a consumer of the existence of a security alert in the credit report of that consumer, regardless of whether a full credit report, credit score, or summary report is requested.

## California Civil Code 1785.11.1 (continued)

(c) Each consumer credit reporting agency shall maintain a toll-free telephone number to accept security alert requests from consumers 24 hours a day, seven days a week.

(d) The toll-free telephone number shall be included in any written disclosure by a consumer credit reporting agency to any consumer pursuant to Section 1785.15 and shall be printed in a clear and conspicuous manner.

(e) A consumer credit reporting agency shall place a security alert on a consumer's credit report no later than five business days after receiving a request from the consumer.

(f) The security alert shall remain in place for at least 90 days, and a consumer shall have the right to request a renewal of the security alert.

(g) Any person who uses a consumer credit report in connection with the approval of credit based on an application for an extension of credit, or with the purchase, lease, or rental of goods or non-credit-related services and who receives notification of a security alert pursuant to subdivision (a) may not lend money, extend credit, or complete the purchase, lease, or rental of goods or non-credit-related services without taking reasonable steps to verify the consumer's identity, in order to ensure that the application for an extension of credit or for the purchase, lease, or rental of goods or non-credit-related services is not the result of identity theft. If the consumer has placed a statement with the security alert in his or her file requesting that identity be verified by calling a specified telephone number, any person who receives that statement with the security alert in a consumer's file pursuant to subdivision (a) shall take reasonable steps to verify the identity of the consumer by contacting the consumer using the specified telephone number prior to lending money, extending credit, or completing the purchase, lease, or rental of goods or non-credit-related services. If a person uses a consumer credit report to facilitate the extension of credit or for another permissible purpose on behalf of a subsidiary, affiliate, agent, assignee, or prospective assignee, that person may verify a consumer' s identity under this section in lieu of the subsidiary, affiliate, agent, assignee, or prospective assignee.

(h) For purposes of this section, "extension of credit" does not include an increase in the dollar limit of an existing open-end credit plan, as defined in Regulation Z issued by the Board of Governors of the Federal Reserve System (12 C.F.R. 226.2), or any change to, or review of, an existing credit account.

## California Civil Code 1785.11.1 (continued)

(i) If reasonable steps are taken to verify the identity of the consumer pursuant to subdivision (b) of Section 1785.20.3, those steps constitute compliance with the requirements of this section, except that if a consumer has placed a statement including a telephone number with the security alert in his or her file, his or her identity shall be verified by contacting the consumer using that telephone number as specified pursuant to subdivision (g).

(j) A consumer credit reporting agency shall notify each consumer who has requested that a security alert be placed on his or her consumer credit report of the expiration date of the alert.

(k) Notwithstanding Section 1785.19, any consumer credit reporting agency that recklessly, willfully, or intentionally fails to place a security alert pursuant to this section shall be liable for a penalty in an amount of up to two thousand five hundred dollars ($2,500) and reasonable attorneys' fees.

If a victim's identity thief is particularly aggressive and gives no indication of ceasing to use their identity to obtain credit, and if the victim lives in California, they should consider using the security freeze to curtail access to their credit file.

2. Fraud Alerts

An initial alert stays on an individual's credit report for at least 90 days. An individual may ask that an initial fraud alert be placed on their credit report if they suspect they have been, or could be, a victim of identity theft. An initial alert is appropriate if an individual's wallet has been stolen or if an individual has been taken in by a "phishing" scam. When an individual places an initial fraud alert on their credit report, they are entitled to one free credit report from each of the three nationwide consumer-reporting companies.

An extended alert stays on an individual's credit report for seven years. Individuals can have an extended alert placed on their credit report if they have been a victim of identity theft and they provide the consumer reporting company with an "identity theft report." When individuals place an extended alert on their credit report, they are entitled to two free credit reports within 12 months from each of the three nationwide consumer-reporting companies.

To place either of these alerts on a credit report, or to have them removed, individuals will be required to provide appropriate proof of their identity: that may include their social security number, name, address, and other personal information requested by the consumer reporting company. When a business sees the alert on an individual's credit report, it must verify the person's identity before issuing them credit.

3. The Identity Theft Report

An identity theft report may have two parts.

The first part is a copy of a report filed with a local, state, or federal law enforcement agency, like a local police department, a state Attorney General, the FBI, the U.S. Secret Service, the FTC, or the U.S. Postal Inspection Service. There is no federal law requiring a federal agency to take a report about identity theft; however, some state laws require local police departments to take reports. When a victim files a report, they should provide as much information as they can about the crime, including anything they know about the dates of the identity theft, the fraudulent accounts opened, and the alleged identity thief.

The second part of an identity theft report depends on the policies of the consumer reporting company and the information provider (the business that sent the information to the consumer reporting company). That is, they may ask the victim to provide information or documentation in addition to that included in the law enforcement report to verify the identity theft. They must make their request within 15 days of receiving the victim's law enforcement report, or, if the victim already obtained an extended fraud alert on their credit report, the date they submit their request to the consumer reporting company for information blocking. The consumer reporting company and information provider then have 15 more days to work with the victim to make sure their identity theft report contains everything they need. They are entitled to take five days to review any information the victim gives them. For example, if a victim gives them information 11 days after they request it, they do not have to make a final decision until 16 days after they asked the victim for that information. If a victim gives them any information after the 15-day deadline, they can reject their identity theft report as incomplete. The victim will then have to resubmit their identity theft report with the correct information.

You may find that many federal and state agencies, and some local police departments, offer only "automated" reports (a report that does not require a face-to-face meeting with a law enforcement officer). Automated reports may be submitted online, by telephone, or by mail. If you have a choice, do not use an automated report. Why? It's more difficult for the credit reporting company or information provider to verify the information. Unless you are asking a credit reporting company to place an extended fraud alert on your credit report, you probably will have to provide additional information or documentation when you use an automated report.

4. Close Accounts

Identity theft victims should call and speak to someone in the security or fraud department of each company for each account they suspect has been tampered with. Victims should follow up in writing, and include copies (not originals) of supporting documents. *It's important to have written documentation with credit card companies and banks.* Every victim should keep a file of their correspondence and enclosures.

When victims of identity theft open new accounts, they should use new Personal Identification Numbers (PINs) and passwords. They should avoid using easily available information like their mother's maiden name, birth date, the last four digits of their social security number or phone number, or a series of consecutive numbers. If the identity thief has made charges or debits on the victim's accounts, or on fraudulently opened accounts, the victim should ask the company for the forms to dispute those transactions.

For charges and debits on existing accounts, a victim should ask the representative to send them the company's fraud dispute forms. If the company does not have special forms, victims should write a letter to dispute the fraudulent charges or debits. In either case, they should write to the company at the address given for "billing inquiries," NOT the address for sending their payments.

For new unauthorized accounts, victims should ask if the company accepts the ID Theft Affidavit. If not, they should ask the representative to send them the company's fraud dispute forms. If the company already has reported these accounts or debts on their credit report, victims should dispute this fraudulent information. Once a victim has resolved their identity theft dispute with the company, they should ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is the best proof if errors relating to this account reappear on their credit report or they are contacted again about the fraudulent debt.

5. File a Criminal Report

All victims of identity theft need to file a criminal report. They should then get a copy of the police report, or at the very least, the number of the report. It can help a victim deal with creditors who need proof of the crime. If the police are reluctant to take the report, a victim should ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like the state police.

## B. LOST OR STOLEN IDENTIFICATION

If individuals have lost personal information or identification, or if it has been stolen, they can minimize the potential for identity theft if they act quickly.

1. Financial Accounts

Accounts, like credit card and bank accounts, should be closed immediately. When opening new accounts, passwords should be placed on them. Using obvious ones, such as a phone number or a series of consecutive numbers, should be avoided.

2. Social Security Number

If someone loses their social security card, he or she should call the toll-free fraud number of any of the three nationwide consumer-reporting companies and place an initial fraud alert on their credit reports. An alert can help stop someone from opening new credit accounts in his or her name.

3. Driver's License and Other Government-Issued Identification

Individuals who lose a driver's license or other government-issued identification should contact the agency that issued the license or other identification document. Follow its procedures to cancel the document and to get a replacement. They should ask the agency to flag the file so that no one else can get a license or any other identification document from them in their name.

Once individuals have taken these precautions, they should watch for signs that their information is being misused, and that their identity has been stolen. If an individual's information has been misused, he or she should file a report about the theft with the police, and file a complaint with the FTC, as well.

If another crime was committed – for example, if an individual's purse or wallet was stolen or his or her house or car was broken into, it should be reported to the police immediately.

### C. WHAT TO DO IF YOU BECOME A VICTIM OF IDENTITY THEFT

Under the Identity Theft and Assumption Deterrence Act, the Federal Trade Commission is responsible for receiving and processing complaints from people who believe they may be victims of identity theft, providing informational materials to those people, and referring those complaints to appropriate entities, including the major credit reporting agencies and law enforcement agencies. For further information, check the FTC's identity theft Web pages. Individuals can also call their local office of the FBI or the U.S. Secret Service to report crimes relating to identity theft and fraud.

Individuals may also need to contact other agencies for other types of identity theft:

- The local office of the Postal Inspection Service if individuals suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect their mail, or has used the mail to commit frauds involving their identity;
- The Social Security Administration if individuals suspect that their social security number is being fraudulently used; and
- The Internal Revenue Service if individuals suspect the improper use of identification information in connection with a tax violation.

Call the fraud units of the three principal credit reporting companies: (a) Equifax; (b) Experian; and (c) TransUnion.

Contact all creditors with whom an individual's name or identifying data have been fraudulently used.

Contact all financial institutions where individuals have accounts that an identity thief has taken over or that have been created in the victim's name but without their knowledge. Individuals may need to cancel those accounts, place stop-payment orders on any outstanding checks that may not have cleared, and change their Automated Teller Machine (ATM) card, account, and Personal Identification Number (PIN).

Contact the major check verification companies if an individual has had checks stolen or bank accounts set up by an identity thief. In particular, if individuals know that a particular merchant has received a check stolen from them, they should contact the verification company that the merchant uses.

## II. CORRECTING FRAUDULENT INFORMATION IN CREDIT REPORTS

The Fair Credit Reporting Act (FCRA) establishes procedures for correcting fraudulent information on an individual's credit report and requires that his or her report be made available only for certain legitimate business needs.

Under the FCRA, both the consumer reporting company and the information provider (the business that sent the information to the consumer reporting company), such as a bank or credit card company, are responsible for correcting fraudulent information in a report. To protect their rights under the law, individuals should contact both the consumer reporting company and the information provider.

## A. CONSUMER REPORTING COMPANY OBLIGATIONS

Consumer reporting companies will block fraudulent information from appearing on an individual's credit report if victims take the following steps. First, the victim should send them a copy of an identity theft report and a letter telling them what information is fraudulent. The letter also should state that the information does not relate to any transaction that the victim made or authorized. In addition, the victim should provide proof of his or her identity that may include his or her social security number, name, address, and other personal information requested by the consumer reporting company.

The consumer reporting company has four business days to block the fraudulent information after accepting an identity theft report. It also must tell the information provider that it has blocked the information. The consumer reporting company may refuse to block the information or remove the block if, for example, an individual has not told the truth about the identity theft. If the consumer reporting company removes the block or refuses to place the block, it must let the victim know.

The blocking process is only one way for identity theft victims to deal with fraudulent information. There is also the "reinvestigation process," which was designed to help all consumers dispute errors or inaccuracies on their credit reports.

## B. INFORMATION PROVIDER OBLIGATIONS

Information providers stop reporting fraudulent information to the consumer reporting companies once victims have sent them an identity theft report and a letter explaining that the information that they are reporting resulted from identity theft. But victims must send their identity theft report and letter to the address specified by the information provider. Note that the information provider may continue to report the information if it later learns that the information does not result from identity theft.

If a consumer reporting company tells an information provider that it has blocked fraudulent information in a victim's credit report, the information provider may not continue to report that information to the consumer reporting company. The information provider also may not hire someone to collect the debt that relates to the fraudulent account, or sell that debt to anyone else who would try to collect it.

**Sample Blocking Letter Consumer Reporting Company**

*Date*
*Your Name*
*Your Address*
*Your City, State, Zip Code*

*Complaint Department*
*Name of Consumer Reporting Company*
*Address*
*City, State, Zip Code*

*Dear Sir or Madam:*

*I am a victim of identity theft. I am writing to request that you block the following fraudulent information in my file. This information does not relate to any transaction that I have made. The items also are circled on the attached copy of the report I received. (Identify item(s) to be blocked by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)*

*Enclosed is a copy of the law enforcement report regarding my identity theft. Please let me know if you need any other information from me to block this information on my credit report.*

*Sincerely,*

*Your name*

*Enclosures: (List what you are enclosing.)*

## C. CREDIT CARDS

The Fair Credit Billing Act establishes procedures for resolving billing errors on a consumer's credit card accounts, including fraudulent charges on the individual's accounts. The law also limits a consumer's liability for unauthorized credit card charges to $50 per card. To take advantage of the law's consumer protections, a consumer must:

- Write to the creditor at the address given for "billing inquiries," not the address for sending payments. The consumer should include his or her name, address, account number and a description of the billing error, including the amount and date of the error; and
- Send the letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed to them. If an identity thief changed the address on the victim's account and the victim did not receive the bill, the dispute letter must still reach the creditor within 60 days of when the creditor would have mailed the bill. This is one reason why it is essential for people to keep track of their billing cycles and follow up quickly if expected bills do not arrive in time.

The letter should be sent by certified mail, and request a return receipt. It becomes the consumer's proof of the date the creditor received the letter. The consumer should include copies (NOT originals) of the police report or other documents that support the consumer's position, and keep a copy of the dispute letter.

The creditor must acknowledge the complaint in writing within 30 days after receiving it, unless the problem has been resolved. The creditor must resolve the dispute within two billing cycles (but not more than 90 days) after receiving the letter.

## D. CRIMINAL VIOLATIONS

Procedures to correct a victim of identity theft's record within criminal justice databases can vary from state to state, and even from county to county. Some states have enacted laws with special procedures for identity theft victims to follow to clear their names.

If wrongful criminal violations are attributed to a victim's name, the victim should contact the police or sheriff's department that originally arrested the person using his or her identity, or the court agency that issued the warrant for the arrest. The victim should file an impersonation report with the police/sheriff's department or the court, and confirm his or her identity.

## E. DEBT COLLECTORS

The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection, even if those bills do not result from identity theft.

Victims of identity theft can stop a debt collector from contacting them in two ways:

- Write a letter to the collection agency telling them to stop. Once the debt collector receives the letter, the company may not contact them again with two exceptions: (a) to tell you there will be no further contact, and (b) they can tell the victim that the debt collector or the creditor intends to take some specific action, like filing a lawsuit; or
- Send a letter to the collection agency, within 30 days after receipt of written notice of the debt, telling them that they do not owe any money. A victim should include copies of documents that support their position. They should also include a copy of their police report. Under these circumstances, the collector can only renew collection efforts if they first send the victim a proof of the debt.

**Sample Dispute Letter For Existing Accounts**

*Date*
*Your Name*
*Your Address*
*Your City, State, Zip Code*
*Your Account Number*

*Name of Creditor*
*Billing Inquiries*
*Address*
*City, State, Zip Code*

*Dear Sir or Madam:*

*I am writing to dispute a fraudulent (charge or debit) on my account in the amount of $_____. I am a victim of identity theft, and I did not make this (charge or debit). I am requesting that the (charge be removed or the debit reinstated), that any finance and other charges related to the fraudulent amount be credited, as well, and that I receive an accurate statement.*

*Enclosed are copies of (use this sentence to describe any enclosed information, such as a police report) supporting my position. Please investigate this matter and correct the fraudulent (charge or debit) as soon as possible.*

*Sincerely,*

*Your name*

*Enclosures: (List what you are enclosing.)*

Victims of identity theft need to be as specific as possible when explaining to a debt collector why they are mistaken. The debt collector is responsible for sending them proof that they are wrong. For example, if the debt a victim is disputing originates from a credit card the victim never applied for, he or she should ask for a copy of the application with the applicant's signature. It should be easy to prove that the signature was not that of the victim.

If victims tell the debt collector that they are a victim of identity theft and it is collecting the debt for another company, the debt collector must tell that company that they may be a victim of identity theft. Remember, however, that stopping the debt collector is not the same thing as eliminating the debt. The victim must still contact the creditor to dispute the account.

## III. REQUESTING INFORMATION ON FRAUDULENT ACCOUNTS

Federal law and laws of some states give an identity theft victim the right to receive copies of documents relating to fraudulent transactions made or accounts opened using the victim's personal information. The information can help law enforcement investigate the crime and can prevent repeated violations.

## A. WORKING WITH LAW ENFORCEMENT

When a victim of identity theft files a report with the police, the officer may give the victim a form to use to request information from creditors or other business. After the victim receives the documentation from the businesses, he or she should turn it over to the officer investigating his or her case.

## B. CONTACTING A CREDITOR OR OTHER BUSINESS

When a victim calls a creditor or other business to report the identity theft, the victim should explain that he or she will be sending a request for applications and other business records relating to the fraudulent transactions or accounts. The victim should also ask where he or she should send his or her request and if any proof of his or her identity or affidavit of identity theft is also required.

## C. FRAUDULENT ACCOUNT INFORMATION REQUEST FORM

The form is provided to help victims request the information from businesses. Victims are not required to use it. If individuals choose to use the form, they should make copies of it. They should fill out one copy for each creditor or business, and send each creditor or business a completed and signed form. The victim should enclose a copy of the police report of identity theft. If a business asked the victim to send proof of identity, he or she should send the proof or affidavit requested.

**IDENTITY THEFT VICTIM'S REQUEST FOR FRAUDULENT TRANSACTION / ACCOUNT INFORMATION**

Made pursuant to section 609(e) of the Fair Credit Reporting Act (15 U.S.C. § 1681g), California Financial Code sections 4002 and 22470, Civil Code section 1748.95 and Penal Code section 530.8.

TO: _____ FAX: _____
ACCOUNT NO.: _____ REFERENCE NO.: _____
FROM: _____

I am a victim of identity theft. I am formally disputing a transaction or an account that I have learned has been made, opened or applied for with you. I did not make this transaction or open or apply for this account and have not authorized anyone else to do so for me. You may consider this transaction or account to be fraudulent. Below is my identifying information. I have filed a report of identity theft with my local police department and a copy is attached. Under federal and California laws, creditors and other business entities must provide a copy of application and business transaction records relating to fraudulent transactions or accounts opened or applied for using an identity theft victim's identity.

A copy of the relevant federal and California law is enclosed. The victim is generally permitted to authorize your release of the account information to a specified law enforcement officer. I am designating the investigator listed below as additional recipient of all account information and documents. I authorize the release of all account documents and information to the law enforcement officer designated. I am requesting that you provide copies of the following records related to the disputed transaction or account:

Application records or screen prints of Internet/phone applications

Statements

Payment/charge slips

Investigator's Summary

Delivery addresses

Any other documents associated with the account

All records of phone numbers used to activate the account or used to access the account

Name: _____ Social Security Number: _____
Address: _____
Phone: Fax: _____
Employer: Phone: _____
Designated Police Department: Report No.: _____
Designated Investigator: _____
Signed: _____ Date: _____

## Federal Law: Fair Credit Reporting Act, 15 U.S. Code Section 609e

(e) Information Available to Victims

(1) In general. For the purpose of documenting fraudulent transactions resulting from identity theft, not later than 30 days after the date of receipt of a request from a victim in accordance with paragraph (3), and subject to verification of the identity of the victim and the claim of identity theft in accordance with paragraph (2), a business entity that has provided credit to, provided for consideration products, goods, or services to, accepted payment from, or otherwise entered into a commercial transaction for consideration with, a person who has allegedly made unauthorized use of the means of identification of the victim, shall provide a copy of application and business transaction records in the control of the business entity, whether maintained by the business entity or by another person on behalf of the business entity, evidencing any transaction alleged to be a result of identity theft to –

## Federal Law: Fair Credit Reporting Act, 15 U.S. Code Section 609e (continued)

(A) the victim;

(B) any Federal, State, or local government law enforcement agency or officer specified by the victim in such a request; or

(C) any law enforcement agency investigating the identity theft and authorized by the victim to take receipt of records provided under this subsection.

(2) Verification of identity and claim. Before a business entity provides any information under paragraph (1), unless the business entity, at its discretion, otherwise has a high degree of confidence that it knows the identity of the victim making a request under paragraph (1), the victim shall provide to the business entity –

(A) as proof of positive identification of the victim, at the election of the business entity–

(i) the presentation of a government-issued identification card;

(ii) personally identifying information of the same type as was provided to the business entity by the unauthorized person; or

(iii) personally identifying information that the business entity typically requests from new applicants or for new transactions, at the time of the victim's request for information, including any documentation described in clauses (i) and (ii); and

(B) as proof of a claim of identity theft, at the election of the business entity--

(i) a copy of a police report evidencing the claim of the victim of identity theft; and

(ii) a properly completed--

(I) copy of a standardized affidavit of identity theft developed and made available by the Commission; or

(II) an affidavit of fact that is acceptable to the business entity for that purpose.

## Federal Law: Fair Credit Reporting Act, 15 U.S. Code Section 609e (continued)

(3) Procedures. The request of a victim under paragraph (1) shall –

(A) be in writing;

(B) be mailed to an address specified by the business entity, if any; and

(C) if asked by the business entity, include relevant information about any transaction alleged to be a result of identity theft to facilitate compliance with this section including –

(i) if known by the victim (or if readily obtainable by the victim), the date of the application or transaction; and

(ii) if known by the victim (or if readily obtainable by the victim), any other identifying information such as an account or transaction number.

(4) No charge to victim. Information required to be provided under paragraph (1) shall be so provided without charge.

(5) Authority to decline to provide information. A business entity may decline to provide information under paragraph (1) if, in the exercise of good faith, the business entity determines that –

(A) this subsection does not require disclosure of the information;

(B) after reviewing the information provided pursuant to paragraph (2), the business entity does not have a high degree of confidence in knowing the true identity of the individual requesting the information;

(C) the request for the information is based on a misrepresentation of fact by the individual requesting the information relevant to the request for information; or

(D) the information requested is Internet navigational data or similar information about a person's visit to a website or online service.

(6) Limitation on liability. Except as provided in section 621, sections 616 and 617 do not apply to any violation of this subsection.

## Federal Law: Fair Credit Reporting Act, 15 U.S. Code Section 609e (continued)

(7) Limitation on civil liability. No business entity may be held civilly liable under any provision of Federal, State, or other law for disclosure, made in good faith pursuant to this subsection.

(8) No new recordkeeping obligation. Nothing in this subsection creates an obligation on the part of a business entity to obtain, retain, or maintain information or records that are not otherwise required to be obtained, retained, or maintained in the ordinary course of its business or under other applicable law.

(9) Rule of Construction

(A) In general. No provision of subtitle A of title V of Public Law 106-102, prohibiting the disclosure of financial information by a business entity to third parties shall be used to deny disclosure of information to the victim under this subsection.

(B) Limitation. Except as provided in subparagraph (A), nothing in this subsection permits a business entity to disclose information, including information to law enforcement under subparagraphs (B) and (C) of paragraph (1), that the business entity is otherwise prohibited from disclosing under any other applicable provision of Federal or State law.

(10) Affirmative defense. In any civil action brought to enforce this subsection, it is an affirmative defense (which the defendant must establish by a preponderance of the evidence) for a business entity to file an affidavit or answer stating that –

(A) the business entity has made a reasonably diligent search of its available business records; and

(B) the records requested under this subsection do not exist or are not reasonably available.

(11) Definition of victim. For purposes of this subsection, the term "victim" means a consumer whose means of identification or financial information has been used or transferred (or has been alleged to have been used or transferred) without the authority of that consumer, with the intent to commit, or to aid or abet, an identity theft or a similar crime.

## Federal Law: Fair Credit Reporting Act, 15 U.S. Code Section 609e (continued)

(12) Effective date. This subsection shall become effective 180 days after the date of enactment of this subsection.

(13) Effectiveness study. Not later than 18 months after the date of enactment of this subsection, the Comptroller General of the United States shall submit a report to Congress assessing the effectiveness of this provision.

# IV. HOW TO REDUCE THE RISK OF BECOMING A VICTIM OF IDENTITY THEFT

Protecting your personal information can help reduce your risk of identity theft. There are four main ways to do it: know who you share information with; store and dispose of your personal information securely, especially your social security number; ask questions before deciding to share your personal information; and maintain appropriate security on your computers and other electronic devices.

## A. KEEPING YOUR PERSONAL INFORMATION SECURE OFFLINE

Lock your financial documents and records in a safe place at home, and lock your wallet or purse in a safe place at work. Keep your information secure from roommates or workers who come into your home.

Limit what you carry. When you go out, take only the identification, credit, and debit cards you need. Leave your social security card at home. Make a copy of your Medicare card and black out all but the last four digits on the copy. Carry the copy with you – unless you are going to use your card at the doctor's office.

Before you share information at your workplace, a business, your child's school, or a doctor's office, ask why they need it, how they will safeguard it, and the consequences of not sharing.

Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don't need them any longer.

Destroy the labels on prescription bottles before you throw them out. Don't share your health plan information with anyone who offers free health services or products.

Take outgoing mail to post office collection boxes or the post office. Promptly remove mail that arrives in your mailbox. If you won't be home for several days, request a vacation hold on your mail.

When you order new checks, don't have them mailed to your home, unless you have a secure mailbox with a lock.

Consider opting out of prescreened offers of credit and insurance by mail. You can opt out for 5 years or permanently. To opt out, call 1-888-567-8688 or go to optoutprescreen.com. The three nationwide credit

reporting companies operate the phone number and website. Prescreened offers can provide many benefits. If you opt out, you may miss out on some offers of credit.

## B. KEEPING YOUR PERSONAL INFORMATION SECURE ONLINE

Know who you share your information with. Store and dispose of your personal information securely.

1. Be Alert to Impersonators

Make sure you know who is getting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with. If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request.

2. Safely Dispose of Personal Information

Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive.

Before you dispose of a mobile device, check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.

3. Encrypt Your Data

Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the Internet. A "lock" icon on the status bar of your Internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.

4. Keep Passwords Private

Use strong passwords with your laptop, credit, bank, and other accounts. Be creative: think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, "I want to see the Pacific Ocean" could become 1W2CtPo.

5. Don't Overshare on Social Networking Sites

If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, social security number, address, phone number, or account numbers in publicly accessible sites.

6. Securing Your Social Security Number

Keep a close hold on your social security number and ask questions before deciding to share it. Ask if you can use a different kind of identification. If someone asks you to share your SSN or your child's, ask:

- Why they need it
- How it will be used
- How they will protect it
- What happens if you don't share the number

The decision to share is yours. A business may not provide you with a service or benefit if you don't provide your number. Sometimes you will have to share your number. Your employer and financial institutions need your SSN for wage and tax reporting purposes. A business may ask for your SSN so they can check your credit when you apply for a loan, rent an apartment, or sign up for utility service.

## C. KEEPING YOUR DEVICES SECURE

1. Use Security Software

Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.

2. Avoid Phishing Emails

Don't open files, click on links, or download programs sent by strangers. Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information you type.

3. Be Wise About Wi-Fi

Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

4. Lock Up Your Laptop

Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.

5. Read Privacy Policies

Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides

information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

## D. ACTIVE DUTY FRAUD ALERTS

Military personnel are particularly susceptible to identity theft because so many of their records, orders, and identification documents prominently display their social security number. Members of the military who are away from their usual duty station may place an active duty alert on their credit reports by contacting any one of the three major consumer-reporting companies. Active duty alerts can help minimize the risk of identity theft while an individual is deployed. To place an alert on a credit report, or to have it removed, an individual will have to provide appropriate proof of their identity, including their social security number, name, address, and other personal information requested by the consumer reporting company. An individual may use a personal representative to place or remove an alert.

Active duty alerts are in effect on the requester's report for one year. If an individual's deployment lasts longer, the individual can place another alert on his or her credit report.

When a business sees the alert on an individual's credit report, it must verify the user's identity before issuing any credit. As part of this verification process, the business may try to contact the individual directly. It is therefore important for individuals to keep their contact information updated. Persons who place an active duty alert on their credit report will also be removed from the credit reporting companies' marketing list for prescreened credit card offers for two years unless they ask to be put back on the list before then.

## CHAPTER 3: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

| | |
|---|---|
| 1. | **Which of the following prevents anyone from accessing another person's credit file for any reason:**<br><br>**A.** a fraud alert<br><br>**B.** a security freeze<br><br>**C.** a criminal report<br><br>**D.** an identity theft affidavit |
| 2. | **Each of the following is one of the three principal credit reporting agencies <u>except</u>:**<br><br>**A.** Equifax<br><br>**B.** Experian<br><br>**C.** TransUnion<br><br>**D.** Report Union |
| 3. | **Which of the following laws establishes procedures for resolving billing errors on a consumer's credit card accounts:**<br><br>**A.** Truth in Lending Act (TILA)<br><br>**B.** Fair Credit Billing Act (FCBA)<br><br>**C.** Identity Theft and Assumption Deterrence Act<br><br>**D.** Fair Debt Collection Practices Act (FDCPA) |

## CHAPTER 3: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

**1.**

**A.** Incorrect. A fraud alert can help prevent an identity thief from opening any more accounts in the victim's name as it indicates to anyone requesting your credit file that you suspect you are a victim of fraud. Individuals can contact the toll-free fraud number of any of the three consumer credit reporting companies to place a fraud alert on their credit report.

**B.** **CORRECT**. A security freeze provides more protection than a fraud alert because it essentially prevents anyone from accessing another person's credit file for any reason, until and unless the individual instructs the credit bureaus to unfreeze or "thaw" his or her report.

**C.** Incorrect. All victims of identity theft need to file a criminal report. They should then get a copy of the police report, or at the very least, the number of the report. It can help a victim deal with creditors who need proof of the crime, but it does not prevent anyone from accessing a person's credit file.

**D.** Incorrect. The ID Theft Affidavit provides a model form that can be used to report information to many companies, simplifying the process of alerting companies where a new account was opened in the victim's name. Previously, victims of identity theft often had to fill out a separate reporting form for each fraudulent account opened by the identity thief.

*(See page 38 of the course material.)*

**2.**

**A.** Incorrect. Equifax is the oldest of the three principal reporting companies and can be reached at 800-685-1111 regarding inquiries if you are denied credit or if you are entitled to a free credit report.

**B.** Incorrect. Experian is one of the three reporting companies and can be reached at 1-888-397-3742 to order a credit report.

**C.** Incorrect. TransUnion is one of the three reporting companies and can be reached at 1-800-680-7289 to request a free annual credit report.

**D.** **CORRECT**. There are only three principle reporting companies and Report Union is not one of them. Phishers may use web sites or unsolicited emails offering credit reports as a way to capture consumers' personal information. Know the three reporting companies and do not fall victim to scams from other solicitors that claim that they can give you a free credit report.

*(See page 43 of the course material.)*

| | |
|---|---|
| **3.** | **A.** Incorrect. TILA protects against inaccurate and unfair credit billing and credit card practices. It requires lenders to provide you with loan cost information so that you can comparison shop for certain types of loans.<br><br>**B.** **CORRECT**. FCBA is an amendment to the TILA and its purpose is to protect consumers from unfair billing practices such as unauthorized charges, charges that list the wrong date, math errors, and failure to post payments and other credit.<br><br>**C.** Incorrect. The Identity Theft and Deterrence Assumption Act enacted by Congress in October 1998 made identity theft a federal crime for the first time.<br><br>**D.** Incorrect. FDCPA prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection, even if those bills do not result from identity theft.<br><br>*(See page 45 of the course material.)* |

# CHAPTER 4: OTHER FORMS OF IDENTITY THEFT

## Chapter Objectives

**After completing this chapter, you should be able to:**

- Identify common sources for child identity theft.
- Recognize the impact on a victim of criminal identity theft.

There are various types of identity theft. The focus of this course is on financial identity theft, which is the use of someone else's financial information to steal his or her identity. With this information, the criminal can perpetrate the victim and steal money, set up a means to launder money, and ruin credit. This chapter will focus on other forms of identity theft, including medical identity theft, child identity theft, and criminal identity theft. In reality, there are financial implications for victims of all forms of identity theft. Victims of medical identity theft may be left with thousands of dollars in medical bills for services they did not get treated for. A freshman in college may try to apply for a student loan and find that she already has bad credit because she has been a victim of child identity theft for the past five years. A businessman may be driving to work and get pulled over for speeding, but end up being taken into custody because there is a warrant out for his arrest. He never knew that someone had given his name to police authorities after committing a crime. The process can be long and complicated to resolve issues that result from all of these forms of identity theft. This chapter will give some advice for prevention, as well as what to do if you become a victim of these other forms of identity theft.

## I. MEDICAL IDENTITY THEFT

A thief may use your name or health insurance number to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment record, and credit report may be affected.

If you see signs of medical identity theft, order copies of your records and check for mistakes. You have the right to see your records and have mistakes corrected.

### A. DETECTING MEDICAL IDENTITY THEFT

Read your medical and insurance statements regularly and completely. They can show warning signs of identity theft. Read the Explanation of Benefits (EOB) statement or Medicare Summary Notice that your health plan sends after treatment. Check the name of the provider, the date of service, and the service provided. Do the claims paid match the care you received? If you see a mistake, contact your health plan and report the problem.

Other signs of medical identity theft include:

- A bill for medical services you didn't receive

- A call from a debt collector about a medical debt you don't owe
- Medical collection notices on your credit report that you don't recognize
- A notice from your health plan saying you reached your benefit limit
- A denial of insurance because your medical records show a condition you don't have.

## B. CORRECTING MISTAKES IN YOUR MEDICAL RECORDS

1. Get Copies of Your Medical Records

If you know a thief used your medical information, get copies of your records. Federal law gives you the right to know what's in your medical files. Check them for errors. Contact each doctor, clinic, hospital, pharmacy, laboratory, health plan, and location where a thief may have used your information. For example, if a thief got a prescription in your name, ask for records from the health care provider who wrote the prescription and the pharmacy that filled it.

You may need to pay for copies of your records. If you know when the thief used your information, ask for records from just that time. Keep copies of your postal and email correspondence, and a record of your phone calls, conversations and activities with your health plan and medical providers.

A provider might refuse to give you copies of your medical or billing records because it thinks that would violate the identity thief's privacy rights. The fact is, you have the right to know what's in your file. If a provider denies your request for your records, you have a right to appeal. Contact the person the provider lists in its Notice of Privacy Practices, the patient representative, or the ombudsman. Explain the situation and ask for your file. If the provider refuses to provide your records within 30 days of your written request, you may complain to the U.S. Department of Health and Human Services' Office for Civil Rights.

2. Get an Accounting of Disclosures

Ask each of your health plans and medical providers for a copy of the "accounting of disclosures" for your medical records. The accounting is a record of who got copies of your records from the provider. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule establishes national standards to protect individuals' medical records and other personal health information. It applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. The law allows you to order one free copy of the accounting from each of your medical providers every 12 months.

The accounting includes details about:

- What medical information the provider sent.

- When it sent the information.
- Who got the information.
- Why the information was sent.

The accounting shows who has copies of your mistaken records and whom you need to contact. It may not have details about some routine disclosure of your information, like those from your doctor's office to another doctor's office, or disclosure of payment information to an insurer.

3. Ask for Corrections

Write to your health plan and medical providers and explain which information is not accurate. Send copies of the documents that support your position. You can include a copy of your medical record and circle the disputed items. Ask the provider to correct or delete each error. Keep the original documents.

Send your letter by certified mail, and ask for a "return receipt," so you have a record of what the plan or provider received. Keep copies of the letters and documents you sent.

The health plan or medical provider that made the mistakes in your files must change the information. It should also inform labs, other health care providers, and anyone else that might have gotten wrong information. If a health plan or medical provider won't make the changes you request, ask it to include a statement of your dispute in your record.

4. How to Correct Errors in Your Medical Records

- Contact each health care provider and ask for copies of your medical records.
    - Check your state's health privacy laws. Some state laws make it easier to get copies of your medical records.
    - Complete the request form and pay any fees required to get copies of your records.
- Review your medical records and report any errors to your health care provider.
    - Write to your health care provider to report mistakes in your medical records.
    - Include a copy of the medical record showing the mistake.
    - Explain why this is a mistake and how to correct it.
    - Include a copy of your police report or Identity Theft Report.
    - Send the letter by certified mail and ask for a return receipt.

  Your health care provider should respond to your letter within 30 days. It must fix the mistake and notify other health care providers who may have the same mistake in their records.

- Notify your health insurer and all 3 credit reporting companies.
    - Send copies of your police report or Identity Theft Report to your health insurer's fraud department and the 3 nationwide credit reporting companies.
- Order copies of your credit reports if you haven't already.
- Consider placing a fraud alert or security freeze on your credit files.
- Update your files.
    - Record the dates you made calls or sent letters.
    - Keep copies of letters in your files.

### C. PROTECTING YOUR MEDICAL INFORMATION

Your medical and insurance information are valuable to identity thieves. Be wary if someone offers you "free" health services or products, but requires you to provide your health plan ID number. Medical identity thieves may pretend to work for an insurance company, doctors' offices, clinic, or pharmacy to try to trick you into revealing sensitive information. Don't share medical or insurance information by phone or email unless you initiated the contact and know who you're dealing with.

Keep paper and electronic copies of your medical and health insurance records in a safe place. Shred outdated health insurance forms, prescription and physician statements, and the labels from prescription bottles before you throw them out. Before you provide sensitive personal information to a website that asks for your social security number, insurance account numbers, or details about your health, find out why it's needed, how it will be kept safe, whether it will be shared, and with whom. Read the Privacy Policy on the website. If you decide to share your information online, look for a lock icon on the browser's status bar or a URL that begins "https:" the "s" stands for secure.

## II. CHILD IDENTITY THEFT

Child identity theft is on the rise, and it happens when someone uses a child's personal information to commit fraud. A thief may steal and use a child's information to get a job, government benefits, medical care, utilities, car loans, secure a mortgage, open bank and credit card accounts, or even rent a place to live. There are a number of ways a child's sensitive, personal information can become available. For example, many school forms require personal and often sensitive information.

More than 1 million children, or 1.48 percent of minors, were victims of identity theft or fraud in 2017, according to a report from Javelin Strategy & Research. Two-thirds of those affected were age 7 or younger.

There are laws that safeguard the privacy rights of children and their families. One example is the federal Family Educational Rights and Privacy Act (FERPA), enforced by the U.S. Department of Education, which protects the privacy of student records. It also gives parents of school-age kids the right to opt-out of sharing contact or other directory information with third parties, including other families.

FERPA (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.

- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
    - School officials with legitimate educational interest;
    - Other schools to which a student is transferring;
    - Specified officials for audit or evaluation purposes;
    - Appropriate parties in connection with financial aid to a student;
    - Organizations conducting certain studies for or on behalf of the school;
    - Accrediting organizations;
    - To comply with a judicial order or lawfully issued subpoena;
    - Appropriate officials in cases of health and safety emergencies; and
    - State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

Children are desirable targets for identity thieves because they can use a child's social security number to establish a fraudulent "clean slate." Identity theft experts recommend parents monitor their children's credit reports to check for identity theft as often as their own.

## A. WARNING SIGNS

Several signs can tip you off to the fact that someone is misusing your child's personal information and committing fraud. For example, you or your child might:

- Be turned down for government benefits because the benefits are being paid to another account using your child's social security number.
- Get a notice from the IRS saying the child didn't pay income taxes, or that the child's social security number was used on another tax return.
- Get collection calls or bills for products or services you or the child didn't receive.

## B. CHECK FOR A CREDIT REPORT

If you think your child's information is at risk, check whether your child has a credit report.

1. Contact One of the 3 Nationwide Credit Reporting Companies

- Ask for a manual search of the child's file. The companies will check for files relating to the child's name and social security number, and for files related only to the child's social security number.
- The credit reporting companies may require copies of:
    - The child's birth certificate listing parents.
    - The child's social security card.
    - The parent or guardian's government-issued identification card, like a driver's license or military identification, or copies of documents proving the adult is the child's legal guardian.
    - Proof of address, like a utility bill, or credit card or insurance statement.

2. Update Your Files

- Record the dates you made calls or sent letters.
- Keep copies of letters in your files.

## C. REPAIR THE DAMAGE

The following are steps that should be taken if your child's credit report shows that the child's information is being misused:

- Contact one of the 3 nationwide credit reporting companies.

    - Send a letter asking the companies to remove all accounts, inquires and collection notices associated with the child's name or personal information.
    - Explain that the child is a minor and include a copy of the Uniform Minor's Status Declaration [PDF].
- Place a fraud alert.
- Learn about your rights.
    - The credit reporting company will explain that you can get a free credit report, and any other rights you have.
- Consider requesting a credit freeze.
    - The credit reporting companies may ask for proof of the child's and parent's identity.
- Order the child's credit reports.
    - Review the credit reports.
- Contact businesses where the child's information was misused.
- Create an Identity Theft Report.
- File a report with the FTC online or call 877-438-4338. If the fraud relates to medical services or taxes, you might need to file a police report, too.
- Update your files.
    - Record the dates you made calls or sent letters.
    - Keep copies of letters in your files.

## D. PREVENTION EQUALS PROTECTION

You can take steps to protect your child's identity from misuse:

- Find a safe location for all paper and electronic records that show your child's personal information.
- Don't share your child's social security number unless you know and trust the other party. Ask why it's necessary and how it will be protected. Ask if you can use a different identifier, or use only the last four digits of your child's social security number.
- Shred all documents that show your child's personal information before throwing them away.
- Be aware of events that put information at risk. For example, there's an adult in your household who might want to use a child's identity to start over; you lose a wallet, purse or paperwork that has your child's social security information; there's a break-in at your

home; or a school, doctor's office or business notifies you that your child's information was affected by a security breach.

## E. ELIMINATING THE RISKS OF CHILD IDENTITY THEFT

Laws safeguard your child and your family's personal information. For example, the federal Family Educational Rights and Privacy Act (FERPA), enforced by the U.S. Department of Education, protects the privacy of student records. It also gives parents of school-age kids the right to opt-out of sharing contact or other directory information with third parties, including other families.

If you're a parent with a child who's enrolled in school:

1. Find Out Who Has Access to Your Child's Personal Information

Verify that the records are kept in a secure location.

2. Pay Attention to Forms From School

Forms that ask for personal information may come home with your child, or you may get them through the mail or by email. Look for terms like "personally identifiable information," "directory information," and "opt-out." Find out how your child's information will be used, whether it will be shared, and with whom.

3. Read the Notices From Your Child's School

Your school will send home an annual notice that explains your rights under FERPA, including your right to:

- Inspect and review your child's education records;
- Approve the disclosure of personal information in your child's records; and
- Ask to correct errors in the records.

4. Ask Your Child's School About Its Directory Information Policy

Student directory information can include your child's name, address, date of birth, telephone number, email address, and photo. If you want to opt-out of the release of directory information to third parties, it's best to put your request in writing and keep a copy for your files. If you don't opt-out, directory information may be available to the people in your child's class and school, and to the general public.

5. Ask For a Copy of Your School's Policy on Surveys

The Protection of Pupil Rights Amendment gives you the right to see surveys and instructional materials before they are distributed to students.

6. Consider Other Programs That Take Place at the School

Your child may participate in programs, like sports and music activities, that aren't formally sponsored by the school. These programs may have web sites where children are named and pictured. Read the

privacy policies of these organizations to find out if, and how, your child's information will be used and shared.

7. Take Action If Your Child's School Experiences a Data Breach

Your child's school or the school district may notify you of a data breach. If not, and you believe your child's information has been compromised, contact the school to learn more. Talk with teachers, staff, or administrators about the incident and their practices. Keep a written record of your conversations. Write a letter to the appropriate administrator, and to the school board, if necessary.

You may file a written complaint with the U.S. Department of Education. Contact the Family Policy Compliance Office, U.S. Department of Education, 400 Maryland Ave., SW, Washington, DC 20202-5920, and keep a copy for your records.

You may have additional rights under state law: contact your local consumer protection agency or your state attorney general for details.

### F. WHEN YOUR CHILD TURNS 16

It's a good idea to check whether your child has a credit report close to the child's 16th birthday. If there is one – and it has errors due to fraud or misuse – you will have time to correct it before the child applies for a job, a loan for tuition or a car, or needs to rent an apartment.

## III. CRIMINAL IDENTITY THEFT

Criminal identity theft occurs when an imposter gives another person's name and personal information such as a drivers' license, date of birth, or social security number (SSN) to a law enforcement officer during an investigation or upon arrest. Or the imposter may present to law enforcement a counterfeit license containing another person's data.

Frequently, but not always, the imposter fraudulently obtained a driver's license or identification card in the victim's name and provides that identification document to law enforcement. Or the imposter, without showing any photo identification, uses the name of a friend or relative. In many cases, the imposter is cited for a traffic violation or for a misdemeanor violation and is released from the arrest. The imposter signs the citation and promises to appear in court. If the imposter does not appear in court, the magistrate may issue a bench warrant, but the warrant of arrest will be under the victim's name.

The identity theft victim may not know there is a warrant of arrest issued under his/her name. The victim may unexpectedly be detained pursuant to a routine traffic stop and then subsequently arrested and taken to county jail (booked) because of the outstanding bench warrant.

In some cases the imposter will appear in court for the traffic or misdemeanor violation and plead guilty without the victim being aware of this event. In other cases, the imposter is arrested and booked at the county jail for a felony such as a drunk driving or other serious public offense. The imposter provides the victim's name and personal information. This information is then recorded in the countywide data base

and is usually transferred to the State's criminal records data base and possibly to the national data base, the National Crime Information Center (NCIC).

Some identity theft victims, unaware of the earlier criminal activity by the imposter, may learn of the impersonation when the victim is denied employment or terminated from employment. In these cases, the employer conducted a background investigation and had relied upon the criminal history found under the victim's name. Note that the employer is legally obligated to inform the victim of the reason for the rejection of employment.

Unfortunately, as with financial identity theft, the burden of clearing one's name within the criminal justice system is primarily on the victim. The victim must act quickly and assertively to minimize the damage. Yet, the responsibility to correct the erroneous data in the various criminal justice computer systems is with the officials working within the criminal justice system. There are no established procedures for clearing one's wrongful criminal record.

When an individual is first "booked" or a warrant of arrest is issued, that person's name is likely to be entered into the county data base and the state's criminal records data base. In California, this system is called the Criminal Identification Index (CII).

In the situation of criminal identity theft, the name and other identifying information such as social security number that appear in the data bases are that of the victim. The information is also likely to be entered into the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC) data base (www.fbi.gov). Victims of criminal identity theft should assume that information is maintained in local, state, and federal criminal history files.

This presents a problem for the victim. The usual method of query by law enforcement into the various criminal justice data bases is by name, date of birth, and/or drivers' license number. Yet, law enforcement relies on the accuracy of such information for their investigations.

Once the victim's name is recorded on a criminal record data base, it will be unlikely that the victim's name will be totally removed from the official record. Should the imposters' true identity be determined, the victim should request a "key name" switch within the various criminal justice data bases. This means that the record will reflect the imposter's true name as the *primary* name and the victim's name will appear as an *alias* (aka). Law enforcement insists on this record-keeping system because it reflects more accurately the criminal event. The dilemma for law enforcement – and for the victim – is when the imposter's identity has not been determined.

The following are general steps you must take to clear your name of the erroneous criminal records attributed to you. Note that these procedures are likely to vary somewhat from jurisdiction to jurisdiction.

## A. STEPS FOR VICTIMS

Contact the arresting or citing law enforcement agency – that is, the police or sheriff's department that originally arrested the person using your identity, or the court agency that issued the warrant for the arrest. Explain that this is a case of misidentification and that someone is using your personal information. Insist that you are the victim.

1. Working with the Arresting Law Enforcement Agency

File an impersonation report. The law enforcement agency should first confirm your identity. This can be done by the police department taking a full set of your fingerprints, your photograph, and copying any photo identification documents such as a driver's license, passport, or U.S. legal presence documents.

Once your identity has been established, the law enforcement agency should retrieve the booking record of the criminal event that you dispute. This will include the booking prints and booking photograph or the citation which may or may not have a thumbprint impression. Request that the law enforcement agency compare the prints and/or photographs to establish your innocence.

Subsequently, the law enforcement agency should recall any warrants and issue a "clearance letter" or certificate of release (if you were arrested/booked) which you will need to keep in your possession at all times. Also, request that the law enforcement agency file with the district attorney's office and/or court of jurisdiction the follow-up investigation establishing your innocence which will entail an amended complaint being issued.

Request that the law enforcement agency change all records from your name to the imposter's true identity (if the true identity of the imposter is known). Some but not all of the levels that must be cleared include city, county, state, and federal data bases.

2. Working with the Court

You will need to determine the specific law(s) in your state that enable you to clear your name in the court records. In California, this is Penal Code Section 851.8, "Determination of Factual Innocence." Ask if something similar to Penal Code Section 851.8 is appropriate in your situation. A judge or magistrate will be required to make this determination.

The declaration should say that you are factually innocent of charges based upon the follow-up impersonation investigation by the law enforcement agency, or declarations, affidavits, or other material and relevant information. This action will change the name on the arrest records and the warrant of arrest to that of the imposter (if the true identity of the imposter is known). Your name will then be known as an alias of the imposter. The court should be requested to provide written verification for you to carry.

Arrangements will be made to schedule an "identity hearing" with the goal of obtaining a determination of factual innocence. At that hearing a judge will examine the evidence, whether it is proof you obtained on your own or subsequent police reports. If the court determines that you indeed are the wrong person named in the case/warrant, you will be issued a certificate that declares your innocence in this case.

For this and any other "certificates of clearance" that you obtain, make several copies. Carry one with you at all times. File another at home in a secure place. Give others to relatives and/or friends who can be contacted in situations where you might have forgotten yours.

Remember, this whole process can be complex. It involves the arresting agency, the court, and the administrators of the various criminal justice data base systems including the motor vehicle data bases. In the best-case scenario you might be able to completely separate your name from the imposter. In most cases, your name will remain a known alias of the imposter indefinitely.

## B. STEPS FOR PREVENTION

There is no “early detection” system to alert victims of criminal identity theft. However, there are some things that you can do as precautions. Besides ordering your credit history from the three credit bureaus each year, periodically obtain a copy of your driver’s license record from your local DMV. Also, order a copy of your Personal Earnings and Benefits Estimate Statement from the Social Security Administration.

Most victims learn of the perils of criminal identity theft by indirect means. These include notice of citation(s) from the courts, collection agency calls, and notice of warrant(s) of arrest. During a routine traffic stop, a police officer might inform the victim that their license was suspended or revoked. Or the victim might be arrested for crimes committed by the imposter.

We know of individuals who have been refused employment because of criminal identity theft. They learned of their wrongful criminal record from information obtained by the employer on the background check. Federal law requires employers to notify job applicants if they have been refused the job because of information on the background check. If you have repeatedly been rejected for employment, you might want to conduct a background check on yourself.

## CHAPTER 4: TEST YOUR KNOWLEDGE

The following question is designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). It is included as an additional tool to enhance your learning experience and does not need to be submitted in order to receive CPE credit.

We recommend that you answer the question and then compare your response to the suggested solution on the following page before answering the final exam question(s) related to this chapter (assignment).

| | |
|---|---|
| **1.** | **Which of the following is true regarding criminal identity theft:**<br>**A.** the burden of clearing one's name is primarily on the victim<br>**B.** the victim will find out immediately if there is a warrant out for his or her arrest<br>**C.** there are established procedures for clearing one's wrongful criminal record<br>**D.** the social security number that appears in the data bases is that of the criminal |

## CHAPTER 4: SOLUTION AND SUGGESTED RESPONSES

Below is the solution and suggested responses for the question on the previous page. If you choose an incorrect answer, you should review the page(s) as indicated for the question to ensure comprehension of the material.

| | |
|---|---|
| **1.** | **A.** CORRECT. Unfortunately, as with financial identity theft, the burden of clearing one's name within the criminal justice system is primarily on the victim and not the authorities. The victim must act quickly and assertively to minimize the damage.<br><br>**B.** Incorrect. The identity theft victim may not know there is a warrant of arrest issued under his or her name. The victim may unexpectedly be detained pursuant to a routine traffic stop and then subsequently arrested and taken to county jail because of the outstanding bench warrant.<br><br>**C.** Incorrect. There are general steps that should be taken to clear one's name of erroneous criminal records, but there are no established procedures for clearing one's wrongful criminal record.<br><br>**D.** Incorrect. The name and other identifying information such as social security number that appear in the data bases are that of the victim. The information is also likely to be entered into the FBI National Crime Information Center (NCIC) data base. Victims of criminal identity theft should assume that information is maintained in local, state, and federal criminal history files.<br><br>*(See page 70 of the course material.)* |

# CHAPTER 5: HOW TO PROTECT YOURSELF WHEN USING TECHNOLOGY

## Chapter Objective

**After completing this chapter, you should be able to:**

- Recognize the security measures that should be taken due to advances in wireless technology.

The increase of technology has made it difficult to prevent the misuse of information on the Internet and other channels. For years, criminals have been using discarded credit card receipts, bank statements, tax notices, and other documents to gain the personal information of others. On today's electronic playing field, however, these criminals have used technology to devise cunning new methods of theft in the form of cyber-crimes.

## I. MOBILE APP BASICS

If you have a smart phone or other mobile device, you probably use apps – to play games, get turn-by-turn directions, access news, books, weather, and more. Easy to download and often free, mobile apps can be so much fun and so convenient that you might download them without thinking about some key considerations: how they're paid for, what information they may gather from your device, or who gets that information.

### A. WHAT'S A MOBILE APP

A mobile app is a software program you can download and access directly using your phone or another mobile device, like a tablet or music player. You need a smart phone or another mobile device with Internet access. Not all apps work on all mobile devices. Once you buy a device, you're committed to using the operating system and the type of apps that go with it. You will typically go to the Apple App Store for Google Play where you can look for, download, and install apps. Some online retailers also offer app stores. To set up an account, you may have to provide a credit card number, especially if you're going to download an app that isn't free.

### B. QUESTIONS ABOUT YOUR PRIVACY

1. What types of data can apps access?

When you sign up with an app store or download individual apps, you may be asked for permission to let them access information on your device. Some apps may be able to access:

- Your phone and email contacts
- Call logs

- Internet data
- Calendar data
- Data about the device's location
- The device's unique IDs
- Information about how you use the app itself

Some apps access only the data they need to function; others access data that's not related to the purpose of the app. If you're providing information when you're using the device, someone may be collecting it – whether it's the app developer, the app store, an advertiser, or an ad network. And if they're collecting your data, they may share it with other companies. It's not always easy to know what data a specific app will access, or how it will be used. Before you download an app, consider what you know about who created it and what it does. The app stores may include information about the company that developed the app, if the developer provides it. If the developer doesn't provide contact information – like a website or an email address – the app may be less than trustworthy.

You may be offered an opportunity to read the "permissions" just before you install an app. Read them. It's useful information that tells you what information the app will access on your device. Ask yourself whether the permissions make sense given the purpose of the app; for example, there's no reason for an e-book or "wallpaper" app to read your text messages.

2. Why do some apps collect location data?

Some apps use specific location data to give you maps, coupons for nearby stores, or information about who you might know nearby. Some provide location data to ad networks, which may combine it with other information in their databases to target ads based on your interests and your location.

Once an app has your permission to access your location data, it can do so until you change the settings on your phone. If you don't want to share your location with advertising networks, you can turn off location services in your phone's settings. But if you do that, apps won't be able to give you information based on your location unless you enter it yourself. Your phone uses general data about its location so your phone carrier can efficiently route calls. Even if you turn off location services in your phone's settings, it may not be possible to completely stop it from broadcasting your location data.

## C. MALWARE AND SECURITY CONCERNS

1. Should I update my apps?

Your phone may indicate when updates are available for your apps. It's a good idea to update the apps you've installed on your device and the device's operating system when new versions are available. Updates often have security patches that protect your information and your device from the latest malware.

2. Could an app infect my phone with malware?

Some hackers have created apps that can infect phones and mobile devices with malware. If your phone sends email or text messages that you didn't write, or installs apps that you didn't download, you could be looking at signs of malware. If you think you have malware on your device, you have a few options: you can contact customer support for the company that made your device; you can contact your mobile phone carrier for help; or you can install a security app to scan and remove apps if it detects malware. Security apps for phones are relatively new; there are only a few on the market, including some with free versions.

### D. MOBILE APP USER REVIEWS

Most app stores include user reviews that can help you decide whether to download. But some app developers and their marketers have posed as consumers to post positive comments about their own products. In fact, the Federal Trade Commission recently sued a company for posting fake comments about the apps it was paid to promote.

### E. KIDS AND MOBILE APPS

In a recent survey of mobile apps for kids, FTC staff found that kids' apps might:

- Collect and share personal information
- Let your kids spend real money – even if the app is free
- Include ads
- Link to social media

What's more, the apps might not tell you they're doing it.

To learn more about an app before you download it, look at screen shots, read the description, content rating and any user reviews, and do some research on the developer. You also can look up outside reviews from sources you respect.

Before you pass the phone or tablet to your kids, take a look at your settings. You may be able to restrict content to what's right for your kid's age, set a password so apps can't be downloaded without it, and set a password so your kids can't buy stuff without it. You also can turn off Wi-Fi and data services or put your phone on airplane mode so it can't connect to the Internet. The best way to keep up with kids' apps is to try them out yourself and talk to your kids about your rules for using apps.

## II. COMPUTER SECURITY

### A. USE SECURITY SOFTWARE THAT UPDATES AUTOMATICALLY

The bad guys constantly develop new ways to attack your computer, so your security software must be up-to-date to protect against the latest threats. Most security software can update automatically; set

yours to do so. You can find free security software from well-known companies. Also, set your operating system and web browser to update automatically.

If you let your operating system, web browser, or security software get out-of-date, criminals could sneak their bad programs – malware – onto your computer and use it to secretly break into other computers, send spam, or spy on your online activities. There are steps you can take to detect and get rid of malware.

Don't buy security software in response to unexpected pop-up messages or emails, especially messages that claim to have scanned your computer and found malware. Scammers send messages like these to try to get you to buy worthless software, or worse, to "break and enter" your computer.

### B. TREAT YOUR PERSONAL INFORMATION LIKE CASH

Don't hand it out to just anyone. Your social security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. So every time you are asked for your personal information – whether in a web form, an email, a text, or a phone message – think about whether you can really trust the request. In an effort to steal your information, scammers will do everything they can to appear trustworthy. Learn more about scammers who phish for your personal information.

### C. CHECK OUT COMPANIES TO FIND OUT WHO YOU'RE DEALING WITH

When you're online, a little research can save you a lot of money. If you see an ad or an offer that looks good to you, take a moment to check out the company behind it. Type the company or product name into your favorite search engine with terms like "review," "complaint," or "scam." If you find bad reviews, you'll have to decide if the offer is worth the risk. If you can't find contact information for the company, take your business elsewhere. Don't assume that an ad you see on a reputable site is trustworthy. The fact that a site features an ad for another site doesn't mean that it endorses the advertised site, or is even familiar with it.

### D. GIVE PERSONAL INFORMATION OVER ENCRYPTED WEBSITES ONLY

If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. As mentioned in Chapter 4, in order to determine if a website is encrypted, look for **https** at the beginning of the web address (the "s" is for secure).

Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, the entire account could be vulnerable. Look for "https" on every page of the site you're on, not just where you sign in.

### E. PROTECT YOUR PASSWORDS

Here are a few principles for creating strong passwords and keeping them safe:

- The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.

- Mix letters, numbers, and special characters. Try to be unpredictable – don't use your name, birthdate, or common words.
- Don't use the same password for many accounts. If it's stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts.
- Don't share passwords on the phone, in texts or by email. Legitimate companies will not send you messages asking for your password. If you get such a message, it's probably a scam.
- Keep your passwords in a secure place, out of plain sight.

### F. BACK UP YOUR FILES

No system is completely secure. Copy important files onto a removable disc or an external hard drive, and store it in a safe place. If your computer is compromised, you'll still have access to your files.

## III. NETWORKS

If you don't secure your wireless network, strangers could use it to gain access to your computer – including personal and financial information you've stored on it. Protect your computer by using Wi-Fi Protected Access (WPA) encryption.

Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient, but they're often not secure. When using a hotspot, it's best to send information only to websites that are fully encrypted. You can be confident a hotspot is secure only if it asks you to provide a WPA password. If you're not sure, treat the network as if it were unsecured.

### A. UNDERSTAND HOW A WIRELESS NETWORK WORKS

Going wireless generally requires connecting an Internet "access point" – like a cable or DSL modem – to a wireless router, which sends a signal through the air, sometimes as far as several hundred feet. Any computer within range with a wireless card can pull the signal from the air and access the Internet.

Unless you take certain precautions, anyone nearby with a wireless-ready computer or mobile device can use your network. That means your neighbors – or any hacker nearby – could "piggyback" on your network, or access information on your computer. If an unauthorized person uses your network to commit crime or send spam, the activity could be traced back to your account.

### B. USE ENCRYPTION

Encryption scrambles the information you send over the Internet into a code so that it's not accessible to others. Using encryption is the most effective way to secure your network from intruders.

Two main types of encryption are available: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). Your computer, router, and other equipment must use the same encryption. WPA2 is strongest; use it if you have a choice. It should protect you against most hackers. Some older routers use only

WEP encryption, which may not protect you from some common hacking programs. Consider buying a new router with WPA2 capability. Wireless routers often come with the encryption feature turned off. You must turn it on. The directions that come with your router should explain how. If they don't, check the company's website.

Encryption is the key to keeping your personal information secure online. When using wireless networks, it's best to send personal information only if it's encrypted – either by an encrypted website or a secure Wi-Fi network. An encrypted website protects only the information you send to and from that site. A secure wireless network encrypts all the information you send using that network.

## C. DON'T ASSUME A WI-FI SPOT IS SECURE

Most Wi-Fi hotspots don't encrypt the information you send over the Internet and are not secure. If you use an unsecured network to log in to an unencrypted site – or a site that uses encryption only on the sign-in page – other users on the network can see what you see and what you send. They could hijack your session and log in as you. New hacking tools – available for free online – make this easy, even for users with limited technical know-how. Your personal information, private documents, contacts, family photos, and even your login credentials could be up for grabs.

An imposter could use your account to impersonate you and scam people you care about. In addition, a hacker could test your username and password to try to gain access to other websites – including sites that store your financial information.

## D. PROTECT YOURSELF WHEN USING PUBLIC WI-FI

So what can you do to protect your information? Here are a few tips:

- When using a Wi-Fi hotspot, only log in or send personal information to websites that you know are fully encrypted. To be secure, your entire visit to each site should be encrypted – from the time you log in to the site until you log out. If you think you're logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Don't stay permanently signed in to accounts. When you've finished using an account, log out.
- Do not use the same password on different websites. It could give someone who gains access to one of your accounts access to many of your accounts.
- Many web browsers alert users who try to visit fraudulent websites or download malicious programs. Pay attention to these warnings, and keep your browser and security software up-to-date.
- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN). VPNs encrypt traffic between your computer and the Internet, even on unsecured networks. You can obtain a personal VPN account from a VPN service provider. In addition, some organizations create VPNs to provide secure, remote access for their employees.

- Some Wi-Fi networks use encryption: WEP and WPA are the most common. WPA2 is the strongest. WPA encryption protects your information against common hacking programs. WEP may not. If you aren't certain that you are on a WPA network, use the same precautions as on an unsecured network.
- Installing browser add-ons or plug-ins can help, too. For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren't encrypted. They don't protect you on all websites – look for https in the URL to know a site is secure.

# IV. FILE SHARING AND BUSINESSES

## A. WHAT IS PEER-TO-PEER FILE SHARING SOFTWARE?

Peer-to-Peer (P2P) technology is a way to share music, videos, documents, and facilitate online telephone conversations. The technology enables computers using the same or compatible P2P programs to form a network and share digital files directly with other computers on the network. When P2P file sharing software is not configured properly, files not intended for sharing may be accessible to anyone on the P2P network.

Most businesses collect and store sensitive information about their employees and customers, like social security numbers, credit card and account information, and medical and other personal data. Many of them have a legal obligation to protect this information. If it gets into the wrong hands, it could lead to fraud and identity theft. That's why any company that collects and stores sensitive information must consider the security implications of using P2P file sharing software and minimize the risks associated with it.

People who use P2P file sharing software can inadvertently share files. They might accidentally choose to share drives or folders that contain sensitive information, or they could save a private file to a shared drive or folder by mistake, making that private file available to others. In addition, viruses and other malware can change the drives or folders designated for sharing, putting private files at risk. As a result, instead of just sharing music, a user's personal tax returns, private medical records or work documents could end up in general circulation on P2P networks. Once a user on a P2P network downloads someone else's files, the files can't be retrieved or deleted. What's more, files can be shared among computers long after they have been deleted from the original source computer. And if there are security flaws or vulnerabilities in the P2P file sharing software or on an organization's network, the P2P program could open the door to attacks on other computers on the network.

## B. INSTALL REBUTTABLE SECURITY SOFTWARE

Some file-sharing programs may hide malware or let malware onto your computer. That could allow criminals to monitor or control your computer activity. Before you use any file-sharing program:

- Install a reputable security program that includes anti-virus and anti-spyware protection.

- Set your security software and operating system to update automatically.
- Delete files the security program flags as problematic.
- Back up files that you'd want to keep if your computer crashes; store them on CDs, DVDs, or external drives, or use an online service.

Before you open or play any downloaded files, use your security software to scan them. If a P2P program asks you to disable or change the settings of your firewall, you might want to reconsider installing it. Disabling or changing the settings could weaken your computer's security. If you believe you've downloaded malware, take steps to remove it.

## C. LIMIT WHAT YOU SHARE AND HOW OFTEN

1. Know What Folders You Are Sharing

Install P2P programs carefully, and understand exactly which folders will be made public. These programs are designed to share files, and once they're installed on your computer, they may share files, folders, and subfolders you never intended to share. Don't save any personal information, files, or subfolders in your "shared" or "download" folders. In addition, security problems within the P2P program could open the door to attacks from hackers. Some malware is designed to change which folders you have designated for sharing, so criminals can access your personal information.

2. Close Your Connection

In many instances, closing the file-sharing program window (clicking the "x") doesn't close your connection to the network, so other users still have access to your shared files. This could increase your security risk and slow your computer. When you're not downloading files, close the program entirely: Double click on the file-sharing program, choose the file menu, and then choose exit. Some P2P programs open automatically every time you turn on your computer. You may want to change the settings so this doesn't happen.

3. Create Separate User Accounts

If more than one person uses your computer, consider setting up separate user accounts with limited rights. Only a user with administrator rights can install software. That's one strategy to protect against installing software you don't want. It also can keep certain users from accessing – or sharing – another user's folders and subfolders.

Use a password to protect the administrator account on your computer so someone else can't disable security features or grant themselves rights you may not want them to have.

## D. PROTECTING SENSITIVE INFORMATION ON YOUR NETWORK

There's no shortcut when it comes to dealing with P2P file sharing security concerns. Regardless of whether you choose to allow P2P file sharing programs, take these steps to ensure that the sensitive information on your network is secure:

- Delete sensitive information you don't need, and restrict where files with sensitive information can be saved.
- Minimize or eliminate the use of P2P file sharing programs on computers used to store or access sensitive information.
- Use appropriate file-naming conventions.
- Monitor your network to detect unapproved P2P file sharing programs.
- Block traffic associated with unapproved P2P file sharing programs at the network perimeter or network firewalls.
- Train employees and others who access your network about the security risks inherent in using P2P file sharing programs.

The decision to ban or allow P2P file sharing programs on your organization's network involves a number of factors. For example, what are the types and locations of sensitive information on your network? Which computers have access to files with sensitive information? What security measures are already in place to protect those files?

If your network has sensitive information that isn't necessary to conduct business, your best bet is to delete it – securely and permanently.

But if your network has sensitive information that is necessary to conduct business, weigh the benefits of using P2P file sharing programs against the security risks associated with the programs. Is there a business need to share files outside your organization? If so, are there more secure ways for your employees to share files?

Whether you decide to ban P2P file sharing programs on your network or allow them, it's important to create a policy and take the appropriate steps to implement and enforce it. That will reduce the risk that any sensitive information will be shared unintentionally.

Among the questions to consider:

- If you decide to ban P2P file sharing programs, how will you prevent these programs from being installed and used?
- If you decide to allow P2P file sharing programs, how will you protect the sensitive information stored on your organization's network?
- If you allow employees, contractors, or vendors to use non-network computers for remote access, what additional steps will you take to protect sensitive files from being shared through P2P file sharing programs installed on those computers?
- How will you train your employees about the risks of using P2P file sharing programs? Will you impose sanctions if your policies are not followed?
- How will you determine if your policies are effective?

A decision to ban P2P file sharing programs altogether requires policies and procedures to prevent these programs from being installed on computers on your network, and to detect any P2P programs that have been installed – and block traffic associated with them.

To prevent P2P file sharing programs from being installed:

- Use administrative security controls to block access from your network to sites used to download P2P file sharing programs. You can filter sites based on URL, IP address, filename and content, or you can use commercial products designed to do the job. The controls also should block access to sites that offer free software downloads; these sites often are sources of P2P file sharing programs.
- Use administrative security controls to prevent employees from installing unapproved programs on your organization's computers.

To detect P2P file sharing programs already installed – and block traffic associated with them:

- Use scanning tools on individual computers and networks often to find P2P file sharing programs and remove them. Commercially available scanning tools can identify many P2P programs.
- Install tools that allow network administrators to restrict, monitor and otherwise manage access to P2P file sharing networks from your corporate network, including intrusion detection systems (IDS), intrusion prevention systems (IPS) or firewalls that detect P2P traffic and restrict appropriate inbound and outbound connections to the Internet. Configuring these tools may require research because different P2P file sharing programs use different protocols. Commercial hardware and software providers may be helpful.
- Install tools that create records of file transfers based on the configuration of IDS, IPS and firewalls to detect and control P2P traffic.
- Use network monitoring tools and techniques like flow reconstruction to identify whether your network has P2P traffic and to determine the nature – and maybe the names and contents – of files that have been sent to and from your network using P2P file sharing programs.
- Review records and activity logs on your network to identify traffic volume spikes that may indicate big files or a large number of small files are being shared.
- Install data loss prevention tools that inspect files flowing from your network to determine whether they contain certain types of sensitive information, like social security numbers. Regularly review the records these tools create to determine whether sensitive information is being exported.

To protect sensitive information while allowing remote access:

- Provide dedicated company computers to employees who access your network remotely, rather than allowing them to use their own personal computers. The computers you

provide should have the same security measures and protections you use at work to prevent, detect and block unauthorized file sharing to P2P networks.

- Require remote access to proceed only through secure connections to your organization's network, like Virtual Private Network (VPN) software or Secure Sockets Layer (SSL). This is appropriate for employees who telework – or for customers or suppliers who need regular access to your system.
- Restrict the locations to which work files containing sensitive information can be saved or copied, and permit remote users to access, use or modify the files – but not to download them. If you allow people to use their personal computers to download files from your organization's network, consider requiring them to securely delete your files from their computers when they are not using the files.
- Exercise due diligence to ensure that customers, suppliers, contractors, vendors, service providers and other third parties that access your network use appropriate security policies and procedures to address risks associated with P2P file sharing programs.

### E. TRAINING EMPLOYEES AND OTHERS ABOUT P2P FILE SHARING PROGRAMS

These days, keeping sensitive information secure really is every employee's responsibility. Regardless of whether you ban the use of P2P file sharing programs or allow it, everyone who has access to sensitive information on your network should be trained about the security risks associated with these programs. If you allow the use of P2P file sharing programs, effective training should demonstrate how to restrict drives or folders to limit what other P2P users can view. It should emphasize the importance of keeping files with sensitive information out of P2P shared drives and folders and minimizing the amount of sensitive information on computers using P2P file sharing programs. Consider what sanctions might be appropriate if your organization's policies about using P2P file sharing programs are not followed or if files containing sensitive information are shared on P2P networks contrary to those policies. Training your employees about securing sensitive information sends the message that your organization believes in keeping personal information private.

Evaluate your security measures regularly to be sure they are doing the job. Circumstances change, equipment and software become outdated, and people make mistakes. As a result, effective security is dynamic, and requires monitoring and updating.

## V. DISPOSING OF OLD COMPUTERS

Getting rid of your old computer? You can ensure its hard drive doesn't become a treasure chest for identity thieves. Use a program that overwrites or wipes the hard drive many times. Or remove the hard drive, and physically destroy it.

### A. UNDERSTAND YOUR HARD DRIVE

Computers often hold personal and financial information, including:

- Passwords
- Account numbers
- License keys or registration numbers for software programs
- Addresses and phone numbers
- Medical and prescription information
- Tax returns
- Files created automatically by browsers and operating systems

When you save a file, especially a large one, it is scattered around the hard drive in bits and pieces. When you open a file, the hard drive gathers the bits and pieces and reconstructs them.

When you delete a file, the links to reconstruct the file disappear. But the bits and pieces of the deleted file stay on your computer until they're overwritten, and they can be retrieved with a data recovery program. To remove data from a hard drive permanently, the hard drive needs to be wiped clean.

## B. HOW TO CLEAN A HARD DRIVE

Before you clean a hard drive, save the files you want to keep to:

- A USB drive,
- A new computer,
- An external hard drive,
- A third-party site, like Dropbox, or
- The Cloud

Check your owner's manual, the manufacturer's website, or its customer support service for information on how to save data and transfer it to a new computer. Utility programs to wipe a hard drive are available both online and in stores where computers are sold. These programs generally are inexpensive; some are available on the Internet for free. These programs vary:

- Some erase the entire disk, while others allow you to select files or folders to erase.
- Some overwrite or wipe the hard drive many times, while others overwrite it only once.

Consider using a program that overwrites or wipes the hard drive many times; otherwise, the deleted information could be retrieved. Or remove the hard drive, and physically destroy it. If you physically destroy the hard drive, like smashing it with a hammer, you run the risk of leaving information that is recoverable if you do not do a thorough enough job.

If you use your home or personal computer for business purposes, check with your employer about how to manage the information on your computer that's business-related. The law requires businesses to follow data security and disposal requirements for certain information that's related to customers.

## C. HOW TO DISPOSE OF YOUR COMPUTER

Many computer manufacturers have programs to recycle computers and components. Check their websites or call their toll-free numbers for more information. The Environmental Protection Agency (EPA) has information about electronic product recycling programs. Your local community may have a recycling program, too. Check with your county or local government, including the local landfill office for regulations.

Many organizations collect old computers and donate them to charities. Some people and organizations buy old computers. Check online.

Remember, most computer equipment contains hazardous materials that don't belong in a landfill. For example, many computers have heavy metals that can contaminate the earth. The EPA recommends that you check with your local health and sanitation agencies for ways to dispose of electronics safely.

## CHAPTER 5: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

| | |
|---|---|
| 1. | **Which of the following is a recommended principle for creating strong passwords:**<br>**A.** use at least 6 characters<br>**B.** use the same password for all of your accounts<br>**C.** mix letters, numbers, and special characters<br>**D.** use something you can easily remember like a birthday or maiden name |
| 2. | **Which of the following is true regarding network security:**<br>**A.** wi-fi hotspots in coffee shops, airports, and hotels are always secure<br>**B.** it is not necessary to use encrypted websites when using a hotspot<br>**C.** a hotspot is secure if it asks you to provide a WPA password<br>**D.** installing browser add-ons puts the information on your device at risk of imposters |
| 3. | **Which of the following is the strongest and the recommended encryption:**<br>**A.** Wired Equivalent Privacy (WEP)<br>**B.** Wired Equivalent Privacy II (WEP2)<br>**C.** Wi-Fi Protected Access (WPA)<br>**D.** Wi-Fi Protected Access II (WPA2) |

## CHAPTER 5: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

| | |
|---|---|
| **1.** | **A.** Incorrect. The longer the password, the tougher it is to crack. It is recommended that you use at least 10 characters.<br><br>**B.** Incorrect. You should use different passwords for different accounts. If you use the same password for all accounts and someone obtains the password from one of the companies with which you do business, it can be used to take over all your accounts.<br><br>**C.** **CORRECT**. It is ideal if you mix letters, numbers, and special characters to create a unique password that is not predictable.<br><br>**D.** Incorrect. An identity thief can easily obtain personal information of victims such as a maiden name or a birthday. It is important that you choose passwords that are strong and not something that a criminal can easily guess.<br><br>*(See page 81 of the course material.)* |
| **2.** | **A.** Incorrect. Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient, but they're often not secure.<br><br>**B.** Incorrect. When using a hotspot, it's best to send information only to websites that are fully encrypted. If you don't secure your wireless network, strangers could use it and gain access to your computer – including personal and financial information you've stored on it.<br><br>**C.** **CORRECT**. When using a hotspot, it's best to send information only to websites that are fully encrypted. You can be confident a hotspot is secure only if it asks you to provide a WPA password. If you're not sure, treat the network as if it were unsecured.<br><br>**D.** Incorrect. Installing browser add-ons or plug-ins can help to protect your information. For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren't encrypted. Remember that they don't protect you on all websites.<br><br>*(See page 81 of the course material.)* |

| | |
|---|---|
| **3.** | **A.** Incorrect. Some older routers use only WEP encryption, which may not protect you from some common hacking programs.<br><br>**B.** Incorrect. WEP2 was introduced to fix problems with WEP, but it was dropped. It does exist, but is rarely used.<br><br>**C.** Incorrect. WPA is not the newest version and is therefore not the strongest encryption.<br><br>**D.** **CORRECT**. WPA2 is strongest; use it if you have a choice. It should protect you against most hackers.<br><br>*(See page 81 of the course material.)* |

# CHAPTER 6: SOCIAL SECURITY NUMBERS

## Chapter Objective

**After completing this chapter, you should be able to:**

- Identify the control recommendations for protecting the security of social security numbers.

Your social security number (SSN) has a unique status as a privacy risk. No other form of personal identification plays such a significant role in linking records that contain sensitive information that individuals generally wish to keep confidential. Created by the federal government in 1936 to track workers' earnings and eligibility for retirement benefits, the social security number is now used in both the public and private sectors for a myriad of purposes totally unrelated to this original purpose. It is used so widely because the SSN is a unique identifier that does not change, allowing it to serve many record management purposes.

Today, social security numbers are used as representations of individual identity, as secure passwords, and as the keys for linking multiple records together. The problem is that these uses are incompatible. The widespread use of the social security number as an individual identifier, resulting in its appearance on mailing labels, ID cards and badges, and various publicly displayed documents, makes it unfit to be a secure password providing access to financial records and other personal information.

The broad use and public exposure of social security numbers has been a major contributor to the tremendous growth in recent years in identity theft and other forms of credit fraud.

## I. CONFIDENTIALITY LAWS

### A. FEDERAL LAWS

The following federal laws establish a framework for restricting SSN disclosure:

1. The Freedom of Information Act (FOIA) (5 U.S.C. 552)

This act establishes a presumption that records in the possession of agencies and departments of the executive branch of the federal government are accessible to the people. FOIA, as amended, provides that the public has a right of access to federal agency records, except for those records that are protected from disclosure by nine stated exemptions. One of these exemptions allows the federal government to withhold information about individuals in personnel and medical files and similar files when the disclosure would constitute a clearly unwarranted invasion of personal privacy. According to Department of Justice guidance, agencies should withhold social security numbers under this FOIA exemption. This statute does not apply to state and local governments. States have their own open records statutes.

2. The Privacy Act of 1974 (5 U.S.C. 552a)

This Act regulates federal government agencies' collection, maintenance, use and disclosure of personal information maintained by agencies in a system of records. The Act prohibits the disclosure of any record contained in a system of records unless the disclosure is made on the basis of a written request or prior written consent of the person to whom the records pertain, or is otherwise authorized by law.

The Act authorizes exceptions under which an agency may disclose information in its records. However, these provisions do not apply to state and local governments, and state law varies widely regarding disclosure of personal information in state government agencies' control. There is one section of the Privacy Act, section 7, that does apply to state and local governments. Section 7 makes it unlawful for federal, state, and local agencies to deny an individual a right or benefit provided by law because of the individual's refusal to disclose his social security number. This provision does not apply:

- Where federal law mandates disclosure of individuals' social security numbers; or
- Where a law existed prior to January 1, 1975 requiring disclosure of social security numbers, for purposes of verifying the identity of individuals, to federal, state or local agencies maintaining a system of records existing and operating before that date.

Section 7 also requires federal, state and local agencies, when requesting social security numbers, to inform the individual of the following:

- Whether disclosure is voluntary or mandatory;
- By what legal authority the social security number is solicited; and
- What uses will be made of the social security number.

The Act contains a number of additional provisions that restrict federal agencies' use of personal information. For example, an agency must maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose required by statute or executive order of the president, and the agency must collect information to the greatest extent practicable directly from the individual when the information may result in an adverse determination about an individual's rights, benefits and privileges under federal programs.

3. The Social Security Act Amendments of 1990 (42 U.S.C. 405(c)(2)(C)(viii))

A provision of the Social Security Act bars disclosure by federal, state and local governments of social security numbers collected pursuant to laws enacted on or after October 1, 1990. This provision of the Act also contains criminal penalties for "unauthorized willful disclosures" of social security numbers; the Department of Justice would determine whether to prosecute a willful disclosure violation. Because the act specifically cites willful disclosures, careless behavior or inadequate safeguards may not be subject to criminal prosecution. Moreover, applicability of the provision is further limited in many instances because it only applies to disclosure of social security numbers collected in accordance with laws enacted on or after October 1, 1990. For social security numbers collected by government entities pursuant to laws enacted before October 1, 1990, this provision does not apply and therefore, would not restrict disclosing

the social security number. Finally, because the provision applies to disclosure of social security numbers collected pursuant to laws requiring social security numbers, it is not clear if the provision also applies to disclosure of social security numbers collected without a statutory requirement to do so. This provision applies to federal, state and local governmental agencies; however, the applicability to courts is not clearly spelled out in the law.

## TABLE 6.1 FEDERAL LAWS THAT AUTHORIZE OR MANDATE COLLECTION AND USE OF SOCIAL SECURITY NUMBERS

| Federal Statute | General Purpose for Collecting or Using SSN | Government Entity and Authorized or Required Use |
|---|---|---|
| Tax Reform Act of 1976<br>42 U.S.C. 405(c)(2)(c)(i) | General public assistance programs, tax administration, driver's license, motor vehicle registration | Authorizes states to collect and use social security numbers in administering any tax, general assistance, driver's license, or motor vehicle registration law |
| Food Stamp Act of 1977<br>7 U.S.C. 2025(e)(1) | Food stamp program | Mandates the secretary of agriculture and state agencies to require social security numbers for program participation |
| Deficit Reduction Act of 1984<br>42 U.S.C. 1320b-7(1) | Eligibility benefits under Medicaid program | Requires that, as a condition of eligibility for Medicaid benefits, applicants for and recipients of these benefits furnish their social security numbers to state administering program |
| Housing and Community Development Act of 1987<br>42 U.S.C. 3543(a) | Eligibility for HUD programs | Authorizes the secretary of the Department of Housing and Urban Development to require applicants and participants in HUD programs to submit their social security numbers as a condition of eligibility |
| Family Support Act of 1988<br>42 U.S.C. 405(c)(2)(C)(ii) | Issuance of birth certificates | Requires states to obtain parents' social security numbers before issuing a birth certificate unless there is good cause for not requiring the number |
| Technical and Miscellaneous Revenue Act of 1988<br>42 U.S.C. 405(c)(2)(D)(i) | Blood donation | Authorizes states and political subdivisions to require that blood donors provide social security numbers |

| Federal Statute | General Purpose for Collecting or Using SSN | Government Entity and Authorized or Required Use |
|---|---|---|
| Food, Agriculture, Conservation, and Trade Act of 1990<br>42 U.S.C. 405(c)(2)(C) | Retail and wholesale businesses participation in food stamp program | Authorizes the secretary of agriculture to require the social security numbers of officers or owners of retail and wholesale food concerns that accept and redeem food stamps |
| Omnibus Budget Reconciliation Act of 1990<br>38 U.S.C. 510(c) | Eligibility for Veterans Affairs compensation or pension benefits programs | Requires individuals to provide their social security numbers to be eligible for Veterans' Affairs compensation or pension benefits programs |
| Social Security Independence and Program Improvements Act of 1994<br>42 U.S.C. 405(c)(2)(E) | Eligibility of potential jurors | Authorizes states and political subdivisions of states to use social security numbers to determine eligibility of potential jurors |
| Personal Responsibility and Work Opportunity Reconciliation Act of 1996<br>42 U.S.C. 666(a)(13) | Various license applications; divorce and child support documents; death certificates | Mandates that states have laws in effect that require collection of social security numbers on applications for driver's licenses and other licenses; requires placement in the pertinent records of the social security number of the person subject to a divorce decree, child support order, paternity determination; requires social security numbers on death certificates; creates national database for child support enforcement purposes |
| Debt Collection Improvement Act of 1996<br>31 U.S.C. 7701(c) | Persons doing business with a federal agency | Requires those doing business with a federal agency, i.e., lenders in a federal guaranteed loan program; applicants for federal licenses, permits, rights-of-ways, or benefits payments; contractors of an agency and others to furnish social security numbers to the agency |
| Higher Education Act Amendments of 1988<br>20 U.S.C. 1090(a)(7) | Financial assistance | Authorizes the secretary of education to include the social security numbers of parents of dependent students on certain financial assistance forms |

| Federal Statute | General Purpose for Collecting or Using SSN | Government Entity and Authorized or Required Use |
|---|---|---|
| Internal Revenue Code (various amendments) 26 U.S.C. 6109 | Tax returns | Authorizes the commissioner of the Internal Revenue Service to require that taxpayers include their social security numbers on tax returns |

## B. STATE LAWS

The need to significantly reduce the risks to individuals of the inappropriate disclosure and misuse of social security numbers, has in recent years led many states to take steps to limit their use and display. California law, for example, Civil Code Sections 1798.85-1798.86 and 1786.60, applies to individuals and non-government entities. Under the laws provisions, which became fully effective July 1, 2005, companies must not do any of the following:

- Post or publicly display social security numbers;
- Print social security numbers on identification cards or badges;
- Require people to transmit a social security number over the Internet unless the connection is secure or the number is encrypted;
- Require people to log onto a web site using a social security number without a password; or
- Print social security numbers on anything mailed to a customer unless required by law or the document is a form or application.

Michigan law provides as follows:

**445.84. Social security numbers privacy policies**

*Sec. 4. (1) Beginning January 1, 2006, a person who obtains 1 or more social security numbers in the ordinary course of business shall create a privacy policy that does at least all of the following concerning the social security numbers the person possesses or obtains:*

*(a) Ensures to the extent practicable the confidentiality of the social security numbers.*

*(b) Prohibits unlawful disclosure of the social security numbers.*

*(c) Limits who has access to information or documents that contain the social security numbers.*

*(d) Describes how to properly dispose of documents that contain the social security numbers.*

*(e) Establishes penalties for violation of the privacy policy.*

*(2) A person that creates a privacy policy under subsection (1) shall publish the privacy policy in an employee handbook, in a procedures manual, or in 1 or more similar documents, which may be made available electronically.*

*(3) This section does not apply to a person who possesses social security numbers in the ordinary course of business and in compliance with the fair credit reporting act, 15 USC 1681 to 1681v, or subtitle A of title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6809.*

The law in New Mexico provides:

**§ 57-12B-3. Disclosure of social security number**

*A. Except as provided in Subsection B of this section, no business shall require a consumer's social security number as a condition for the consumer to lease or purchase products, goods or services from the business.*

*B. Nothing in this section prohibits a business from requiring or requesting a consumer's social security number if the number will be used in a manner consistent with state or federal law or as part of an application for credit or in connection with annuity or insurance transactions.*

*C. Nothing in this section prohibits a business from acquiring or using a consumer's social security number if the consumer consents to the acquisition or use.*

*D. A company acquiring or using social security numbers of consumers shall adopt internal policies that:*

> *(1) limit access to the social security numbers to those employees authorized to have access to that information to perform their duties; and*
>
> *(2) hold employees responsible if the social security numbers are released to unauthorized persons.*

In North Carolina, the law provides, effective October 1, 2006:

**§ 75-62. Social security number protection**

*(a) Except as provided in subsection (b) of this section, a business may not do any of the following:*

> *(1) Intentionally communicate or otherwise make available to the general public an individual's social security number.*
>
> *(2) Intentionally print or imbed an individual's social security number on any card required for the individual to access products or services provided by the person or entity.*
>
> *(3) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.*
>
> *(4) Require an individual to use his or her social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site.*

*(5) Print an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed.*

*(6) Sell, lease, loan, trade, rent, or otherwise intentionally disclose an individual's social security number to a third party without written consent to the disclosure from the individual, when the party making the disclosure knows or in the exercise of reasonable diligence would have reason to believe that the third party lacks a legitimate purpose for obtaining the individual's social security number.*

*(b) Subsection (a) of this section shall not apply in the following instances:*

*(1) When a social security number is included in an application or in documents related to an enrollment process, or to establish, amend, or terminate an account, contract, or policy; or to confirm the accuracy of the social security number for the purpose of obtaining a credit report pursuant to 15 U.S.C. § 1681(b)(2). A social security number that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.*

*(2) To the collection, use, or release of a social security number for internal verification or administrative purposes.*

*(3) To the opening of an account or the provision of or payment for a product or service authorized by an individual.*

*(4) To the collection, use, or release of a social security number to investigate or prevent fraud, conduct background checks, conduct social or scientific research, collect a debt, obtain a credit report from or furnish data to a consumer reporting agency pursuant to the Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq., undertake a permissible purpose enumerated under Gramm Leach Bliley, 12 C.F.R. § 216.13-15, or locate an individual who is missing, a lost relative, or due a benefit, such as a pension, insurance, or unclaimed property benefit.*

*(5) To a business acting pursuant to a court order, warrant, subpoena, or when otherwise required by law.*

*(6) To a business providing the social security number to a federal, state, or local government entity, including a law enforcement agency, court, or their agents or assigns.*

*(7) To a social security number that has been redacted.*

*(c) A business covered by this section shall make reasonable efforts to cooperate, through systems testing and other means, to ensure that the requirements of this Article are implemented.*

*(d) A violation of this section is a violation of G.S. 75-1.1.*

In light of the many recent changes, it is recommended that all businesses review the law of their state to determine if it imposes any specific requirements on the handling of social security numbers.

## C. RECOMMENDED PRACTICES

The following recommendations for protecting social security numbers were made by California's Office of Privacy Protection. They are relevant for private and public sector organizations regardless of what state they operate in, and they apply to the handling of all social security numbers in the possession of an organization: those of customers, employees and business partners.

1. Reduce the Collection of Social Security Numbers

These recommendations include:

- Collect social security numbers preferably only where required to do so by federal or state law;
- When collecting social security numbers as allowed, but not required, by law, do so only as reasonably necessary for the proper administration of lawful business activities; and
- If a unique personal identifier is needed, develop your own as a substitute for the social security number.

2. Inform Individuals When Requesting Social Security Numbers

In order to provide openness in business practices, the following steps are recommended:

- Whenever you collect social security numbers as required or allowed by law, inform the individuals of the purpose of the collection, the intended use, whether the law requires the number to be provided or not, and the consequences of not providing the number; and
- If required by law, notify individuals (customers, employees, business partners, etc.) annually of their right to request that you do not post or publicly display their social security number or do any of the other things prohibited by state law.

3. Eliminate Public Display

- Do not put social security numbers on documents that are widely seen by others, such as identification cards, badges, time cards, employee rosters, bulletin board postings, and other materials;
- Do not send documents with social security numbers on them through the mail, except on applications or forms or when required by law;
- When sending applications, forms or other documents required by law to carry social security numbers through the mail, place the social security number where it will not be revealed by an envelope window. Where possible, leave the social security number field on forms and applications blank and ask the individual to fill it in before returning the form or application;

- Do not send social security numbers by e-mail unless the connection is secure or the number is encrypted;
- Do not require an individual to send his or her social security number over the Internet or by e-mail, unless the connection is secure or the number is encrypted; and
- Do not require individuals to use social security numbers as passwords or codes for access to Internet web sites or other services.

4. Control Access

Another important way to safeguard social security numbers is to limit access to records containing this information. Businesses should therefore:

- Limit access to records containing social security numbers only to those who need to see the numbers for the performance of their duties;
- Use logs or electronic audit trails to monitor employees' access to records with social security numbers;
- Protect records containing social security numbers, including back-ups, during storage by encrypting the numbers in electronic records or storing records in other media in locked cabinets;
- Do not store records containing social security numbers on computers or other electronic devices that are not secured against unauthorized access;
- Avoid sharing social security numbers with other companies or organizations except where required by law;
- If you do share social security numbers with other companies or organizations, including contractors, use written agreements to protect their confidentiality;
- Prohibit such third parties from re-disclosing social security numbers, except as required by law;
- Require such third parties to use effective security controls on record systems containing social security numbers;
- Hold such third parties accountable for compliance with the restrictions you impose, including monitoring or auditing their practices; and
- If social security numbers are disclosed inappropriately and the individuals whose social security numbers were disclosed are put at risk of identity theft or other harm, promptly notify the individuals potentially affected.

5. Protect Social Security Numbers with Security Safeguards

- Develop a written security plan for record systems that contain social security numbers;
- Develop written policies for protecting the confidentiality of social security numbers, including but not limited to the following:
    - Adopt “clean desk/work area” policy requiring employees to properly secure records containing social security numbers;
    - Do not leave voice mail messages containing social security numbers and if you must send a social security number by fax, take special measures to ensure confidentiality;
    - Require employees to ask individuals (employees, customers, etc.) for identifiers other than the social security number when looking up records for the individual;
    - Require employees to promptly report any inappropriate disclosure or loss of records containing social security numbers to their supervisors or to the organization’s privacy officer; and
    - When discarding or destroying records in any medium containing social security numbers, do so in a way that protects their confidentiality, such as shredding.

6. Make the Organization Accountable for Protecting Social Security Numbers

Accountability is another key in safeguarding financial records, including social security numbers. In this area, the following steps are recommended:

- Provide training and written material for employees on their responsibilities in handling social security numbers;
- Conduct training at least annually;
- Train all new employees, temporary employees and contract employees;
- Impose discipline on employees for non-compliance with organizational policies and practices for protecting social security numbers;
- Conduct risk assessments and regular audits of record systems containing social security numbers; and
- Designate someone in the organization as responsible for ensuring compliance with policies and procedures for protecting social security numbers.

7. Ensuring Social Security Records Are Accurate

Each year your employer sends a copy of your W-2 (*Wage and Tax Statement*) to social security. We compare your name and social security number on the W-2 with the information in our files. We add the earnings shown on the W-2 to your social security record.

It is critical that your name and social security number on your social security card agree with your employer's payroll records and W-2 so that we can credit your earnings to your record. It is up to you to make sure that both social security's records and your employer's records are correct. If your social security card is incorrect, contact any social security office to make changes. Check your W-2 form to make sure your employer's record is correct and, if it isn't, give your employer the accurate information.

You also can check your earnings record on your *Social Security Statement*. The Statement is available online to workers age 18 and older. To review your Statement, go to www.socialsecurity.gov/myaccount and create an account.

## II. REPLACING A SOCIAL SECURITY CARD OR SECURING A NEW NUMBER

Individuals can replace a social security card for free if it is lost or stolen. However, card holders are limited to three replacement cards in a year and 10 during a lifetime. Legal name changes and other exceptions don't count toward these limits. For example, changes in noncitizen status that require card updates may not count toward these limits. Also, an individual may not be affected by these limits if they can prove you need the card to prevent a significant hardship.

To get a replacement social security card, an individual will need to:

- Complete an *Application for a Social Security Card*;
- Present an unexpired original document with identifying information, and preferably, a recent photograph that proves your identity;
- Show evidence of your U.S. citizenship if you were born outside the United States and did not show proof of citizenship when you got your card; and
- Show evidence of your current lawful noncitizen status if you are not a U.S. citizen.

Some victims of identity theft may prefer to get a new social security number. If someone has done all they can to fix the problems resulting from misuse of their social security number, and someone is still using their number, the Social Security Administration may assign them a new number.

A new number is not available if:

- An individual's social security card is lost or stolen, but there is no evidence that someone is using their number;
- To avoid the consequences of filing for bankruptcy; or

- If the individual intends to avoid the law or their legal responsibility.

If an individual decides to apply for a new number, they will need to prove their identity, age, and U.S. citizenship or immigration status. They will also need to provide evidence they are having ongoing problems because of the misuse.

Keep in mind that a new number probably will not solve all of a person's problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under an individual's old number. Along with other personal information, credit reporting companies use the number to identify that person's credit record. So using a new number will not guarantee a victim of identity theft a fresh start. This is especially true if the victim's other personal information, such as your name and address, remains the same.

For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with their new number, the absence of any credit history under their new number may make it more difficult for them to get credit.

## CHAPTER 6: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

| | |
|---|---|
| 1. | **Why were social security numbers originally created by the federal government:**<br><br>**A.** to help with drafting soldiers in World War II<br><br>**B.** to help with rationing food and fuel during World War II<br><br>**C.** to record workers' earnings and eligibility for retirement benefits<br><br>**D.** all of the above |
| 2. | **What authority do states have to regulate the use of social security numbers:**<br><br>**A.** individual states have no authority, under federal law, to regulate the collection or use of social security numbers<br><br>**B.** states may, consistent with federal law, regulate the collection but not the use of social security numbers<br><br>**C.** states may take steps to reduce the collection and use of social security numbers by the private sector, and a number have done so lately<br><br>**D.** while they have authority, no state has ever taken steps to regulate the collection or use of social security numbers |

## CHAPTER 6: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

| | |
|---|---|
| **1.** | **A.** Incorrect. Although used for a number of purposes, social security numbers were originally created for purposes other than aiding in the draft.<br><br>**B.** Incorrect. The original purpose of the issuance of social security numbers was not for food rationing.<br><br>**C.** **CORRECT**. Social security numbers were first issued by the federal government in 1936 to track wages and eligibility for retirement benefits. Today, it is used for many other things in both the public and private sector.<br><br>**D.** Incorrect. Only one of the answers was the intended use for social security numbers when first issued.<br><br>*(See page 95 of the course material.)* |
| **2.** | **A.** Incorrect. States may regulate the collection and use of social security numbers in the private sector.<br><br>**B.** Incorrect. States may regulate both the collection and use of social security numbers.<br><br>**C.** **CORRECT**. A number of states have taken steps to regulate the use and collection of social security numbers in an effort to protect consumers.<br><br>**D.** Incorrect. Many states, including California, have enacted regulation to limit the misuse of social security numbers.<br><br>*(See page 99 of the course material.)* |

# CHAPTER 7: IDENTITY THEFT AND BUSINESS

## Chapter Objective

**After completing this chapter, you should be able to:**

- Recognize ways businesses can help prevent identity theft.

These days, it is almost impossible to be in business and not collect or hold personally identifying information – names and addresses, social security numbers, credit card numbers, or other account numbers – about clients, customers, employees, business partners, students, or patients. If this information falls into the wrong hands, it could put these individuals at risk for identity theft. Perhaps no type of professional collects more personal financial information about its clients than CPAs and other accounting professionals like Enrolled Agents. The chapters that follow discuss federal laws that impose specific requirements on financial institutions, including tax preparers. However, many CPAs also provide general business advice to their clients. This chapter provides some basic ideas of how to make a business less susceptible to identity theft and provides suggestions of what to do if it does happen.

### TABLE 7.1 DO'S AND DON'TS OF IDENTITY THEFT

| Do's | Don'ts |
|---|---|
| Limit employees' access to personal information to what is truly necessary for them to perform their duties. | Leave documents containing sensitive personal information – such as social security numbers, driver's license numbers and the like – lying in the open where anyone can see them. |
| Require employees to use passwords for access to databases containing personal information. This will provide an "audit trail" for any abuses that might occur. | Use faxes, e-mail or voice mail to send messages containing sensitive personal information such as bank account numbers. |
| Adopt a "clean desk" policy of keeping records containing sensitive personal information that are not currently being used locked away and out of view. | Provide sensitive personal information over the telephone without firm policies to ensure that the caller is legitimate. |
| Train employees about their responsibilities to protect client/customer information from unauthorized access, including how to respond to telephone requests for personal information. | Allow customers/clients or third parties to be in areas where sensitive personal information is easily accessible. |
| Utilize generally accepted security practices to protect sensitive personal information. | Assume that your business is immune from identity theft and other privacy crimes. |

| Do's | Don'ts |
|---|---|
| Notify individuals in writing if certain items of their personal information are acquired by unauthorized persons. Such information includes social security numbers or driver's license numbers. | Dispose of or give away old computers, hard drives or other equipment containing personal information without first making the data unreadable. |
| Use a cross-cut shredder to destroy paper customer records containing personal information before throwing them away. | Throw paper records containing personal customer or client information – i.e., home address, account numbers – into the trash can without first shredding them. |

Unfortunately, many people have the attitude that things will not happen to them. In the case of identity theft, some business owners assume that they do not have the type of information that would be of interest to criminals. Do not make this mistake. Any business with employees, for example, has payroll records that contain Social security numbers and addresses. All businesses have occasion to ultimately discard confidential data. Without the proper safeguards, information ends up in the dumpster where it is readily, and legally, available to anybody. The trash is considered by business espionage professionals as the single most available source of competitive and private information from the average business. Any establishment that discards private and proprietary data without the benefit of destruction, exposes itself to the risk of criminal and civil prosecution, as well as the costly loss of business.

## I. RECORDS MANAGEMENT

In a survey conducted by the Conference Board, top executives from 300 companies ranked the security of company records as one of the top five critical issues facing business. When asked which issues required immediate attention and policy development, the security of company records ranked second only to employee health screening. This section makes some suggestions for all businesses, large and small.

### A. STORED RECORDS SHOULD BE DESTROYED ON A REGULAR BASIS

The period of time that business records are stored should be determined by a retention schedule that takes into consideration their useful value to the business and the governing legal requirements. No record should be kept longer than this retention period.

By not adhering to a program of routinely destroying stored records, a company exhibits suspicious disposal practices that could be negatively construed in the event of litigation or audit. Also, the statute requires that, in the event of a lawsuit, each party provide all relevant records to the opposing counsel within 85 days of the defendant's initial response. If either of the litigants does not fulfill this obligation, it will result in a summary finding against them. By destroying records according to a set schedule, a company appropriately limits the amount of materials it must search through to comply with this law.

From a risk management perspective, the only acceptable method of discarding stored records is to destroy them by a method that ensures that the information is obliterated. Documenting the exact date that a record is destroyed is a prudent and recommended legal precaution.

## B. INCIDENTAL BUSINESS RECORDS

Without a program to control it, the daily trash of every business contains information that could be harmful. This information is especially useful to competitors because it contains the details of current activities. Discarded daily records include phone messages, memos, misprinted forms, drafts of bids and drafts of correspondence.

All businesses suffer potential exposure due to the need to discard these incidental business records. The only means of minimizing this exposure is to make sure such information is securely collected and destroyed.

## C. LIMITS OF RECYCLING

To extract the scrap value from office paper, recycling companies use unscreened, minimum wage workers, to extensively sort the paper under unsecured conditions. The acceptable paper is stored for indefinite periods of time until there is enough of a particular type to sell. The sorted paper, still intact, is then baled and sold to the highest bidder, often overseas, where it may be stored again for weeks or even months until it is finally used to make new products. There is no fiduciary responsibility inherent in the recycling scenario. Paper is given away or sold and, by doing so, a company gives up the right to say how it is handled. There is, also, no practical means of establishing the exact date that a record is destroyed. In the event of an audit or litigation, this could be a legal necessity. And, further, if something of a private nature does surface, the selection of this unsecured process could be interpreted as negligent. For all these reasons, the choice of recycling as a means of information destruction is undesirable from a risk management perspective.

If environmental responsibility is a concern, materials may be recycled after they are destroyed or a firm can contract a service that will destroy the materials under secure conditions before recycling them. Any recycling company that minimizes the need for security has its own interests in mind and should be avoided.

## D. CERTIFICATES OF DESTRUCTION AND OUTSIDE VENDORS

Any company contracting an information destruction service should require that it provide them with a signed testimonial, documenting the date that the materials were destroyed. The certificate of destruction, as it is commonly referred, is an important legal record of compliance with a retention schedule. It does not, however, effectively transfer the responsibility to maintain the confidentiality of the materials to the contractor.

If private information surfaces after the vendor accepts it, the court is bound to question the process by which the particular contractor was selected. Any company not showing due diligence in their selection of a contractor that is capable of providing the necessary security could be found negligent. And, from a practical standpoint, if proprietary or private information is lost or leaked by the fraud or negligence of a vendor, the obligations of that vendor are irrelevant. The firm whose information falls into the wrong hands stands to lose the most, either from loss of business, prosecution or unfavorable publicity.

Since a business cannot transfer its responsibility to maintain confidentiality, it must be certain that it is dealing with a reputable company with superior security procedures. Unfortunately, there are those information destruction services that provide certificates of destruction while having no semblance of security and, in some cases, no destruction process available to them. Anyone interested in contracting a data destruction service is advised to thoroughly review their policies and procedures, conduct an initial site audit and conduct subsequent unannounced audits. On-site document destruction is also an option in most cities.

Many commercial records storage facilities offer records destruction as a service to their customers. However, in a survey conducted by the National Association for Information Destruction, a majority of the commercial storage firms were found lacking the equipment necessary to provide the service themselves. It is a common practice in that industry to subcontract the destruction of the records. In some cases, disreputable storage firms were found misleading their customers by charging for secure records destruction, while the materials were being sold to a recycling company for scrap. Any business using a commercial records storage firm should inquire as to the nature of the destruction services that are available. It is an unacceptable risk to permit a storage firm to select a subcontractor to provide the records destruction service. The owner of the records is ultimately responsible for their security and, therefore, should be selecting the vendor directly.

### E. USE OF INTERNAL PERSONNEL

Common sense dictates that payroll information and materials that involve labor relations or legal affairs, should not be entrusted to lower level employees for destruction. But, beyond that, competition sensitive information is best protected from them as well. It has been established, time and again, that employees are the most likely to realize the value of certain information to competitors. And, lower wage employees often have the economic incentive to capitalize on their access to it. The only acceptable alternatives are to have the materials destroyed under the supervision of upper management or by a carefully selected, high security service.

## II. PAYMENT METHODS

Every successful business collects payments. Common methods include checks, credit cards and, more recently, electronic payment. This section raises some issues with respect to each of these methods of payment.

### A. CHECKS

If a business elects to accept payment by check, the following policies are recommended:

- Do not write or enter a credit card number on any documents connected with the transaction;
- Do verify the customer's identity by looking at their driver's license or other picture identification; and

- Verify the consumer's identity by comparing the signature on their driver's license with the signature on their check.

While vigilance is important, remember that some states have laws that limit the conditions a business can place on the acceptance of a check. For example, California law limits credit card guarantees:

**§ 1725. Negotiable instruments; identification; credit card as condition of acceptance prohibited**

*(a) Unless permitted under subdivision (c), no person accepting a negotiable instrument as payment in full or in part for goods or services sold or leased at retail shall do any of the following:*

> *(1) Require the person paying with a negotiable instrument to provide a credit card as a condition of acceptance of the negotiable instrument, or record the number of the credit card.*
>
> *(2) Require, as a condition of acceptance of the negotiable instrument, or cause the person paying with a negotiable instrument to sign a statement agreeing to allow his or her credit card to be charged to cover the negotiable instrument if returned as no good.*
>
> *(3) Record a credit card number in connection with any part of the transaction described in this subdivision.*
>
> *(4) Contact a credit card issuer to determine if the amount of any credit available to the person paying with a negotiable instrument will cover the amount of the negotiable instrument.*

*(b) For the purposes of this section, the following terms have the following meanings:*

> *(1) "Check guarantee card" means a card issued by a financial institution, evidencing an agreement under which the financial institution will not dishonor a check drawn upon itself, under the terms and conditions of the agreement.*
>
> *(2) "Credit card" has the meaning specified in Section 1747.02, and does not include a check guarantee card or a card that is both a credit card and a check guarantee card.*
>
> *(3) "Negotiable instrument" has the meaning specified in Section 3104 of the Commercial Code.*
>
> *(4) "Retail" means a transaction involving the sale or lease of goods or services or both, between an individual, corporation, or other entity regularly engaged in business and a consumer, for use by the consumer and not for resale.*

*(c) This section does not prohibit any person from doing any of the following:*

> *(1) Requiring the production of reasonable forms of positive identification, other than a credit card, which may include a driver's license or a California state identification card, or where one of these is not available, another form of photo identification, as a condition of acceptance of a negotiable instrument.*

*(2) Requesting, but not requiring, a purchaser to voluntarily display a credit card as an indicia of creditworthiness or financial responsibility, or as an additional identification, provided the only information concerning the credit card which is recorded is the type of credit card displayed, the issuer of the card, and the expiration date of the card. All retailers that request the display of a credit card pursuant to this paragraph shall inform the customer, by either of the following methods, that displaying the credit card is not a requirement for check writing:*

*(A) By posting the following notice in a conspicuous location in the unobstructed view of the public within the premises where the check is being written, clearly and legibly: "Check writing ID: credit card may be requested but not required for purchases."*

*(B) By training and requiring the sales clerks or retail employees requesting the credit card to inform all check writing customers that they are not required to display a credit card to write a check.*

*(3) Requesting production of, or recording, a credit card number as a condition for cashing a negotiable instrument that is being used solely to receive cash back from the person.*

*(4) Requesting, receiving, or recording a credit card number in lieu of requiring a deposit*

*to secure payment in event of default, loss, damage, or other occurrence.*

*(5) Requiring, verifying, and recording the purchaser's name, address, and telephone number.*

*(6) Requesting or recording a credit card number on a negotiable instrument used to make a payment on that credit card account.*

*(d) This section does not require acceptance of a negotiable instrument whether or not a credit card is presented.*

*(e) Any person who violates this section is subject to a civil penalty not to exceed two hundred fifty dollars ($250) for a first violation, and to a civil penalty not to exceed one thousand dollars ($1,000) for a second or subsequent violation, to be assessed and collected in a civil action brought by the person paying with a negotiable instrument, by the Attorney General, or by the district attorney or city attorney of the county or city in which the violation occurred. However, no civil penalty shall be assessed for a violation of this section if the defendant shows by a preponderance of the evidence that the violation was not intentional and resulted from a bona fide error made notwithstanding the defendant's maintenance of procedures reasonably adopted to avoid such an error. When collected, the civil penalty shall be payable, as appropriate, to the person paying with a negotiable instrument who brought the action or to the general fund of whichever governmental entity brought the action to assess the civil penalty.*

*(f) The Attorney General, or any district attorney or city attorney within his or her respective jurisdiction, may bring an action in the superior court in the name of the people of the State of California to enjoin*

*violation of subdivision (a) and, upon notice to the defendant of not less than five days, to temporarily restrain and enjoin the violation. If it appears to the satisfaction of the court that the defendant has, in fact, violated subdivision (a), the court may issue an injunction restraining further violations, without requiring proof that any person has been damaged by the violation. In these proceedings, if the court finds that the defendant has violated subdivision (a), the court may direct the defendant to pay any or all costs incurred by the Attorney General, district attorney, or city attorney in seeking or obtaining injunctive relief pursuant to this subdivision.*

## B. CREDIT CARDS

According to the federal Fair and Accurate Credit Transaction Act (FACTA), which has been in effect for all businesses since December 1, 2006, the electronically printed credit and debit card receipts you give your customers must shorten – or truncate – the account information. You may include no more than the last five digits of the card number, and you must delete the card's expiration date. For example, a receipt that truncates the credit card number and deletes the expiration date could look like this:

ACCT: **********12345
EXP: ****

Why is it important for businesses to make sure they're complying with this law? Credit card numbers on sales receipts are a "golden ticket" for fraudsters and identity thieves. Savvy businesses appreciate the importance of protecting their customers – and themselves – from credit card crime.

But there are other important reasons to make sure your slips are ship-shape. Noncompliance could open a company up to an FTC law enforcement action, including civil penalties and injunctive relief. In addition, the law allows consumers to sue businesses that don't comply and to collect damages and attorney's fees.

All companies that electronically print credit or debit card receipts must truncate the information on the copy they give their customers. That's why it's important to make sure all your equipment complies with the law.

Several details of the law are worth noting: It applies only to electronically printed receipts, not to handwritten or imprinted ones. And it applies only to receipts you give your customer at point of sale, not to any transaction record you retain. Be aware, however, that when you keep your customers' personal information – including account data – you have an obligation to keep it safe.

When accepting payments by credit cards, it is recommended that businesses:

- Do not write or enter any personal information – home address, driver's license number, social security number, e-mail address, etc. – on any documents connected with the credit card transaction;
- Do not require individuals to provide personal information as a condition of completing the transaction;

- Do verify the consumer's identity by looking at a driver's license or identification card photo;
- Verify the consumer's identity by comparing the signature on the driver's license to the signature on the back of the credit card and on the receipt; and
- Verify the address and zip code of customers paying by credit card over the telephone, through the mail or by e-mail.

Once again, there are laws in some states limiting the type of personal information that can be collected.

***California Civil Code section 1747.08: Limits on collection of personal information when accepting payment by credit card.***

*(a) Except as provided in subdivision (c), no person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business shall do any of the following:*

> *(1) Request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to write any personal identification information upon the credit card transaction form or otherwise.*
>
> *(2) Request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to provide personal identification information, which the person, firm, partnership, association, or corporation accepting the credit card writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise.*
>
> *(3) Utilize, in any credit card transaction, a credit card form which contains preprinted spaces specifically designated for filling in any personal identification information of the cardholder.*

*(b) For purposes of this section "personal identification information," means information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number.*

*(c) Subdivision (a) does not apply in the following instances:*

> *(1) If the credit card is being used as a deposit to secure payment in the event of default, loss, damage, or other similar occurrence.*
>
> *(2) Cash advance transactions.*
>
> *(3) If the person, firm, partnership, association, or corporation accepting the credit card is contractually obligated to provide personal identification information in order to complete the credit card transaction or is obligated to collect and record the personal identification information by federal law or regulation.*

*(4) If personal identification information is required for a special purpose incidental but related to the individual credit card transaction, including, but not limited to, information relating to shipping, delivery, servicing, or installation of the purchased merchandise, or for special orders.*

*(d) This section does not prohibit any person, firm, partnership, association, or corporation from requiring the cardholder, as a condition to accepting the credit card as payment in full or in part for goods or services, to provide reasonable forms of positive identification, which may include a driver's license or a California state identification card, or where one of these is not available, another form of photo identification, provided that none of the information contained thereon is written or recorded on the credit card transaction form or otherwise. If the cardholder pays for the transaction with a credit card number and does not make the credit card available upon request to verify the number, the cardholder's driver's license number or identification card number may be recorded on the credit card transaction form or otherwise.*

*(e) Any person who violates this section shall be subject to a civil penalty not to exceed two hundred fifty dollars ($250) for the first violation and one thousand dollars ($1,000) for each subsequent violation, to be assessed and collected in a civil action brought by the person paying with a credit card, by the Attorney General, or by the district attorney or city attorney of the county or city in which the violation occurred. However, no civil penalty shall be assessed for a violation of this section if the defendant shows by a preponderance of the evidence that the violation was not intentional and resulted from a bona fide error made notwithstanding the defendant's maintenance of procedures reasonably adopted to avoid that error. When collected, the civil penalty shall be payable, as appropriate, to the person paying with a credit card who brought the action, or to the general fund of whichever governmental entity brought the action to assess the civil penalty.*

*(f) The Attorney General, or any district attorney or city attorney within his or her respective jurisdiction, may bring an action in the superior court in the name of the people of the State of California to enjoin violation of subdivision (a) and, upon notice to the defendant of not less than five days, to temporarily restrain and enjoin the violation. If it appears to the satisfaction of the court that the defendant has, in fact, violated subdivision (a), the court may issue an injunction restraining further violations, without requiring proof that any person has been damaged by the violation. In these proceedings, if the court finds that the defendant has violated subdivision (a), the court may direct the defendant to pay any or all costs incurred by the Attorney General, district attorney, or city attorney in seeking or obtaining injunctive relief pursuant to this subdivision.*

*(g) Actions for collection of civil penalties under subdivision (e) and for injunctive relief under subdivision (f) may be consolidated.*

*(h) The changes made to this section by Chapter 458 of the Statutes of 1995 apply only to credit card transactions entered into on and after January 1, 1996. Nothing in those changes shall be construed to affect any civil action which was filed before January 1, 1996.*

## C. ELECTRONIC PAYMENTS

The Internet has taken its place beside the telephone and television as an important part of people's lives. Consumers use the Internet to shop, bank and invest online. Most consumers use credit or debit cards to pay for online purchases, but other payment methods, like "e-wallets," are becoming more common.

Most online shoppers use credit cards to pay for their online purchases. But debit cards – which authorize merchants to debit your bank account electronically – are increasing in use. Your debit card may be an automated teller machine (ATM) card that can be used for retail purchases. To complete a debit card transaction, you may have to use a personal identification number (PIN), some form of a signature or other identification, or a combination of these identifiers. Some cards have both credit and debit features. You select the payment option at the point-of-sale. But remember, although a debit card may look like a credit card, the money for debit purchases is transferred almost immediately from your bank account to the merchant's account. In addition, your liability limits for a lost or stolen debit card and unauthorized use are different from your liability if your credit card is lost, stolen or used without your authorization.

Other electronic payment systems – sometimes referred to as "electronic money" or "e-money" – also are now common. Their goal is to make purchasing simpler. For example, "stored-value" cards let you transfer cash value to a card. They are commonly used on public transportation, at colleges and universities, at gas stations, and for prepaid telephone use. Many retailers also sell stored-value cards in place of gift certificates. Some stored-value cards work offline, say, to buy a candy bar at a vending machine; others work online, for example, to buy an item from a website; some have both offline and online features. Some cards can be "reloaded" with additional value, at a cash machine; other cards are "disposable" – you throw them away after you use all their value. Some stored-value cards contain computer chips that make them "smart" cards. These cards may act like a credit card as well as a debit card, and also may contain stored value.

Some Internet-based payment systems allow value to be transmitted through computers, sometimes called "e-wallets." You can use "e-wallets" to make "micro-payments" – very small online or offline payments for things like a magazine or fast food. There are two type of e-wallets: those owned by consumers, or those owned by sellers and websites.

The simplest e-wallets are those owned by sellers. When a website offers to store payment information for the next time a consumer visits the site, usually accessible by password, the website is offering to set up an e-wallet. The next time that user visits the site, the user will be able to enter his or her identifying information and usually then just have to click to pay. Never once must he or she reach for a real wallet, or enter any numbers into the site.

User-owned wallet systems allow users to manually enter their payment information, including credit cards and bank routing data, to create a personalized account. Again, that account is typically secured with a variety of passwords and authentication challenges. Once activated, the account can often be used across the web to make payments on any website that supports its technology. The accounts support electronic commerce by enabling purchases, debits, and deposits using information that has already been stored and validated. Examples of some of the more popular personal e-wallet programs

are PayPal™, Neteller®, and Moneybookers. Many digital wallets are also mobile-compatible, which means that users can access and manage accounts from their phones. More and more purchases are being made with web-enabled phones, so more and more phones support digital wallet programs.

The following tips are recommended for anyone making or accepting e-payments:

- **Use a secure browser** – software that encrypts or scrambles the purchase information customers send over the Internet – to help guard the security of customer information as it is transmitted to a website. Browsers should have the most up-to-date encryption capabilities by using the latest version available from the manufacturer. Customers can also download some browsers for free over the Internet. When submitting purchase information, customers should look for the "lock" icon on the browser's status bar, and the phrase "https" in the URL address for a website, to be sure their information is secure during transmission.
- **Check the site's privacy policy**, before you provide any personal financial information to a website. In particular, determine how the information will be used or shared with others. Also check the site's statements about the security provided for your information. Some websites' disclosures are easier to find than others – look at the bottom of the home page, on order forms or in the "About" or "FAQs" section of a site. If you are not comfortable with the policy, consider doing business elsewhere.
- **Keep your personal information private**. Do not disclose your personal information – your address, telephone number, social security number, bank account number or e-mail address – unless you know who is collecting the information, why they are collecting it and how they will use it.
- **Give payment information only to businesses you know and trust**, and only when and where it is appropriate – like an order form. Never give your password to anyone online, even your Internet service provider. Do not download files sent to you by strangers or click on hyperlinks from people you do not know. Opening a file could expose your system to a computer virus or a program that could hijack your modem.
- **Keep records of your online transactions and check your e-mail** for contacts by merchants with whom you are doing business. Merchants may send you important information about your purchases.
- **Review your monthly credit card and bank statements** for any errors or unauthorized purchases promptly and thoroughly. Notify your credit or debit card issuer immediately if your credit or debit card or checkbook is lost or stolen, or if you suspect someone is using your accounts without your permission.

### D. VERIFICATION BEFORE EXTENDING CREDIT

If you are contemplating extending credit to an individual, it is first important to verify the individual's identity. When reviewing an application for credit, a few steps are highly recommended, including the following:

- Do not ignore significant differences between the personal information provided by a consumer applying for credit and the information in his or her credit report, and
- Do not ignore a fraud alert or security alert on an applicant's credit report.

It is also recommended that the business make an effort to verify the identity of an applicant before granting credit.

**Example**

Ask to see a driver's license or state issued identification card and compare the photo and signature. You might ask to see three pieces of ID, such as a military ID, credit card, health plan card or passport, in addition to a driver's license.

Before extending credit, a business should also take extra steps to verify identity if there is a difference between the personal information the applicant provides and the information in his or her credit report. Look especially at the first and last name, address and social security number.

**Example**

If the name is significantly different – not "Bill" vs. "William," but "John" vs. "Catherine," ask to see additional pieces of identification. Or, if the residence address in the credit report is a different city or state, you might ask to see a utility bill or other proof of residency.

Additionally, businesses should:

- Tell customers that they are taking these steps to protect them from identity theft; and
- Call the phone number given with a fraud alert to verify the applicant's identity. Do this before approving the credit application.

## III. RESPONDING TO IDENTITY THEFT

The following are recommended courses of action if the worst-case scenario does happen and your business or that of your client is affected by identity theft.

## A. CONTACTING LAW ENFORCEMENT AND CREDIT BUREAUS

When the compromise could result in harm to a person or business, organizations are advised to contact their local law enforcement agency immediately, and report the situation, as well as the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective they can be. If your local police are not familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service. For incidents involving mail theft, contact the U.S. Postal Inspection Service.

Information compromises can have an impact on businesses other than yours, such as banks or credit issuers. If account access information – for example, credit card or bank account numbers – has been stolen from you, but you do not maintain the accounts, notify the institution that does so that it can monitor the accounts for fraudulent activity. If you collect or store personal information on behalf of other businesses, as accounting firms commonly do, also notify them of any information compromise.

If names and social security numbers have been stolen, you can contact the major credit bureaus for additional information or advice. If the compromise may involve a large group of people, advise the credit bureaus if you are recommending that people request fraud alerts for their files. Your notice to the credit bureaus can facilitate customer assistance. The following are the major credit bureaus that should be contacted:

**Equifax**
*P.O. Box 740241*
*Atlanta, GA 30374*
*Phone: 800-685-1111*

**Experian**
*Experian Security Assistance*
*P.O. Box 4500*
*Allen, TX 75013*
*Phone: 888-397-3742*

**TransUnion**
*P.O. Box 2000*
*Chester, PA 19022-2000*
*Phone: 1-800-680-7289*

If the information compromise resulted from the improper posting of personal information on your Web site, immediately remove the information from your site. Be aware that Internet search engines store, or "cache," information for a period of time. You can contact the search engines to ensure that they do not archive personal information that was posted in error.

## B. CONTACTING CLIENTS AND CUSTOMERS INVOLVED

Generally, early notification to individuals whose personal information has been compromised allows them to take steps to mitigate the misuse of their information. In deciding if notification is warranted, consider the nature of the compromise, the type of information taken, the likelihood of misuse, and the

potential damage arising from misuse. For example, thieves who have stolen names and social security numbers from a CPA's office can use this information to cause significant damage to a victim's credit record. Individuals who are notified early can take some steps to prevent or limit any harm.

When notifying individuals, it is recommended that you consult with your law enforcement contact about the timing of the notification so it does not impede the investigation. It is also recommended that you designate a contact person within your organization for releasing information. Give the contact person the latest information about the breach, your response, and how individuals should respond. Consider using letters (see sample below), e-mail, and toll-free numbers as methods of communication with those whose information may have been compromised.

It is also important that your notice:

- Describes clearly what you know about the compromise. Include how it happened; what information was taken, and, if you know, how the thieves have used the information; and what actions you have taken already to remedy the situation. Explain how to reach the contact person in your organization. Consult with your law enforcement contact on exactly what information to include so your notice does not hamper the investigation;
- Explains what responses may be appropriate for the type of information taken. For example, people whose social security numbers have been stolen should contact the credit bureaus to ask that fraud alerts be placed on their credit reports. See www.consumer.gov/idtheft for more complete information on appropriate follow-up after a compromise;
- Includes current information about identity theft. The FTC's website at www.consumer.gov/idtheft has information to help individuals guard against and deal with identity theft;
- Provides contact information for the law enforcement officer working on the case (as well as your case report number, if applicable) for victims to use. Be sure to alert the law enforcement officer working your case that you are sharing this contact information. Identity theft victims often can provide important information to law enforcement. Victims should request a copy of the police report and make copies for creditors who have accepted unauthorized charges. The police report is important evidence that can help absolve a victim of fraudulent debts; and
- Encourages those who discover that their information has been misused to file a complaint with the FTC at www.ftccomplaintassistant.gov/ or at 1-877-ID-THEFT (438-4338). Information entered into the Identity Theft Data Clearinghouse, the FTC's database, is made available to law enforcement.

The following letter is a model for notifying people whose names and social security numbers have been stolen. In cases of stolen social security numbers, it is important that people place a fraud alert on their credit reports. A fraud alert may hinder identity thieves from getting credit with stolen information because it is a signal to creditors to contact the consumer before opening new accounts or changing existing accounts. Potential victims of a theft also should review their credit reports periodically to keep track of

whether their information is being misused. For some victims, weeks or months may pass between the time the information is stolen and the time it is misused.

**MODEL LETTER FOR THE COMPROMISE OF SOCIAL SECURITY NUMBERS**

Dear _____:

We are contacting you about a potential problem involving identity theft.

[Describe the information compromise and how you are responding to it.]

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

| Equifax | Experian | TransUnionCorp |
|---|---|---|
| 800-685-1111 | 888-397-3742 | 1-800-680-7289 |

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call [insert contact information for law enforcement] and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.ftccomplaintassistant.gov/ or at 1-877-ID-THEFT (438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

We have enclosed a copy of ID Theft: When Bad Things Happen to Your Good Name, a comprehensive guide from the FTC to help you guard against and deal with identity theft.

[Insert closing]

Your Name

## CHAPTER 7: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

| | |
|---|---|
| 1. | **To help combat identity theft, how long are businesses advised to retain records:**<br><br>**A.** indefinitely<br><br>**B.** no more than three years, regardless of the type of record<br><br>**C.** no longer than they are useful to the business<br><br>**D.** no more than one year |
| 2. | **Which of the following is <u>not</u> one of the practices recommended for businesses that take personal checks from customers:**<br><br>**A.** they should record the check writer's social security number and driver's license number on the check<br><br>**B.** they should verify the customer's identification by looking at their driver's license<br><br>**C.** they should verify the customer's identification by comparing signatures on the check and on their driver's license<br><br>**D.** they should not record any credit card information on the check |
| 3. | **Which of the following is true of the Fair and Accurate Credit Transaction Act (FACTA) provision regarding credit and debit card payment receipts:**<br><br>**A.** it does not go into effect until January 2016<br><br>**B.** it applies to receipts that you give your customer at point of sale and to any transaction record you retain<br><br>**C.** it applies to electronically printed, handwritten, and imprinted receipts<br><br>**D.** businesses may include no more than the last five digits of the card on receipts |

# CHAPTER 7: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

| | |
|---|---|
| **1.** | **A.** Incorrect. Records should be kept only as long as necessary for that particular business.<br><br>**B.** Incorrect. Business necessity, not any specific time frame, should dictate how long records are maintained.<br><br>**C.** **CORRECT**. The nature of each business and the specific type of records will dictate how long they should be kept. When they are no longer necessary, they should be destroyed.<br><br>**D.** Incorrect. There is no specific recommended time period.<br><br>*(See page 112 of the course material.)* |
| **2.** | **A.** **CORRECT**. The business should not record such personal information on the check or anywhere that could put the information in jeopardy. This information is confidential and should be kept secure.<br><br>**B.** Incorrect. Businesses should verify the customer's identification by looking at their driver's license to ensure that the person is who they are purporting to be. Many companies do not take this imperative step, but should as it only takes a few seconds to verify a customer's identity.<br><br>**C.** Incorrect. Many businesses do not verify signatures, but should. This is a simple step that can help prevent and deter identity theft.<br><br>**D.** Incorrect. Businesses should not record any credit card information on the check in order to ensure that no more personal information is retained than necessary to complete the transaction and ensure the safety of the customer's identity.<br><br>*(See page 114 of the course material.)* |

| | |
|---|---|
| **3.** | **A.** Incorrect. Congress passed this provision in December 2003, and it was phased in gradually, requiring merchants with newer electronic card processing machines to comply by December 2004. Merchants with older machines were given until December 1, 2006.<br><br>**B.** Incorrect. FACTA applies only to receipts you give your customer at point of sale, not to any transaction record you retain. Be aware, however, that when you keep your customers' personal information – including account data – you have an obligation to keep it safe.<br><br>**C.** Incorrect. FACTA applies only to electronically printed receipts, but not to handwritten or imprinted ones.<br><br>**D.** **CORRECT**. According to (FACTA), the electronically printed credit and debit card receipts you give your customers must shorten – or truncate – the account information. You may include no more than the last five digits of the card number, and you must delete the card's expiration date.<br><br>*(See page 117 of the course material.)* |

# CHAPTER 8: THE FINANCIAL PRIVACY REQUIREMENTS OF THE GRAMM-LEACH-BLILEY ACT

## Chapter Objectives

**After completing this chapter, you should be able to:**

- Recall the requirements of the Gramm-Leach-Bliley Act.
- Identify what is governed by the Financial Privacy Rule.

## I. OVERVIEW

Protecting the privacy of consumer information held by "financial institutions" is at the heart of the financial privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999. The so-called "GLB Act" requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some – but not all – sharing of their information.

The Appendix at the end of this course contains the complete text of the IRS guidelines for tax preparers.

### A. FINANCIAL INSTITUTIONS

The GLB Act applies to "financial institutions" – companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance. The Federal Trade Commission has authority to enforce the law with respect to "financial institutions" that are not covered by the federal banking agencies, the Securities and Exchange Commission, the Commodity Futures Trading Commission, or state insurance authorities. Among the institutions that fall under FTC jurisdiction for purposes of the GLB Act are non-bank mortgage lenders, loan brokers, some financial or investment advisers, tax preparers, providers of real estate settlement services, and debt collectors. At the same time, the FTC's regulation applies only to companies that are "significantly engaged" in such financial activities.

The law requires that financial institutions protect information collected about individuals; it does not apply, however, to information collected in business or commercial activities.

### B. THE SAFEGUARDS RULE

The Safeguards Rule requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

The Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

- Designate one or more employees to coordinate its information security program;
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- Design and implement a safeguards program, and regularly monitor and test it;
- Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The requirements are designed to be flexible. Companies should implement safeguards appropriate to their own circumstances. For example, some companies may choose to put their safeguards program in a single document, while others may put their plans in several different documents – say, one to cover an information technology division and another to describe the training program for employees. Similarly, a company may decide to designate a single employee to coordinate safeguards or may assign this responsibility to several employees who will work together. In addition, companies must consider and address any unique risks raised by their business operations – such as the risks raised when employees access customer data from their homes or other off-site locations, or when customer data is transmitted electronically outside the company network.

## C. CONSUMERS AND CUSTOMERS

A company's obligations under the GLB Act depend on whether the company has consumers or customers who obtain its services. A "consumer" is an individual who obtains or has obtained a financial product or service from a financial institution for personal, family or household reasons. A "customer" is a consumer with a continuing relationship with a financial institution. Generally, if the relationship between the financial institution and the individual is significant and/or long-term, the individual is a customer of the institution. For example, a person who gets a mortgage from a lender or hires a broker to get a personal loan is considered a customer of the lender or the broker, while a person who uses a check-cashing service is a consumer of that service.

Why is the difference between consumers and customers so important? Because only customers are entitled to receive a financial institution's privacy notice automatically. Consumers are entitled to receive a privacy notice from a financial institution only if the company shares the consumers' information with companies not affiliated with it, with some exceptions. Customers must receive a notice every year for as long as the customer relationship lasts.

The privacy notice must be given to individual customers or consumers by mail or in-person delivery. Reasonable ways to deliver a notice may depend on the type of business the institution is in: for example, an online lender may post its notice on its website and require online consumers to acknowledge receipt as a necessary part of a loan application. A tax preparer, on the other hand, may be expected to provide written notification to each client's last known address.

## D. THE PRIVACY NOTICE

Many companies you do business with are required to give you privacy notices that explain their information-sharing practices. In turn, you have the right to limit some – but not all – sharing of your information. The law balances your right to privacy with the company's need to provide information for normal business purposes. The following information is intended to educate you or help you educate your client about privacy notices and when you can and cannot opt out of information sharing.

The privacy notice must be a clear, conspicuous, and accurate statement of the company's privacy practices; it should include what information the company collects about its consumers and customers, with whom it shares the information, and how it protects or safeguards the information. The notice applies to the "nonpublic personal information" the company gathers and discloses about its consumers and customers; in practice, that may be most – or all – of the information a company has about them. For example, nonpublic personal information could be information that a consumer or customer puts on an application; information about the individual from another source, such as a credit bureau; or information about transactions between the individual and the company, such as an account balance. Indeed, even the fact that an individual is a consumer or customer of a particular financial institution is nonpublic personal information. But information that the company has reason to believe is lawfully public – such as mortgage loan information in a jurisdiction where that information is publicly recorded – is not restricted by the GLB Act.

## E. OPT-OUT RIGHTS

Consumers and customers have the right to opt out of, that is, object to, having their information shared with certain third parties. The privacy notice must explain how the consumer or customer can do so and offer a manner that is reasonable. For example, providing a toll-free telephone number or a detachable form with a pre-printed address is a reasonable way for consumers or customers to opt out; requiring someone to write a letter as the only way to opt out is not.

The privacy notice also must explain that consumers have a right to say no to the sharing of certain information – credit report or application information – with the financial institution's affiliates. An affiliate is an entity that controls another company, is controlled by the company, or is under common control with the company. Consumers have this right under the Fair Credit Reporting Act. The GLB Act does not give consumers the right to opt out when the financial institution shares other information with its affiliates.

The GLB Act provides no opt-out right in several other situations. For example, an individual cannot opt out if:

- A financial institution shares information with outside companies that provide essential services like data processing or servicing accounts;

- The disclosure is legally mandated; or
- A financial institution shares customer data with outside service providers that market the financial company's products or services.

### F. RECEIVING NONPUBLIC PERSONAL INFORMATION

The GLB Act puts some limits on how anyone that receives nonpublic personal information from a financial institution can use or re-disclose the information. Take the case of a lender that discloses customer information to a service provider responsible for mailing account statements, where the consumer has no right to opt out. The service provider may use the information for limited purposes – namely for mailing account statements. It may not, however, sell the information to other organizations or use it for marketing. The situation is different, on the other hand, when a company receives nonpublic personal information from a financial institution that provided an opt-out notice – and the consumer did not opt out. In this case, the recipient steps into the shoes of the disclosing financial institution, and may use the information for its own purposes or re-disclose it to a third party, consistent with the financial institution's privacy notice. That is, if the privacy notice of the financial institution allows for disclosure to other unaffiliated financial institutions – like insurance providers – the recipient may re-disclose the information to an unaffiliated insurance provider.

### G. OTHER PROVISIONS

Other important provisions of the GLB Act also impact how a company conducts business. For example, financial institutions are prohibited from disclosing their customers' account numbers to non-affiliated companies when it comes to telemarketing, direct mail marketing or other marketing through e-mail, even if the individuals have not opted out of sharing the information for marketing purposes.

Another provision prohibits "pretexting" - the practice of obtaining customer information from financial institutions under false pretenses. The FTC has brought several cases against information brokers who engage in pretexting.

This chapter focuses on how businesses, particularly small businesses, must comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act.

## II. PRIVACY RULE REQUIREMENTS IN DETAIL

The Financial Modernization Act of 1999, also known as the GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions. This chapter will focus on the Privacy Rule.

The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are tax return

preparation, lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities. Such non-traditional "financial institutions" are regulated by the FTC.

The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, who receive such information.

The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions "such as credit reporting agencies" that receive customer information from other financial institutions.

The pretexting provisions of the GLB Act protect consumers from individuals and companies that obtain their personal financial information under false pretenses, a practice known as "pretexting."

## A. ENTITIES COVERED BY THE PRIVACY RULE

There are two ways that the Privacy Rule might cover a business. First, if the business is a "financial institution," it is covered. Second, if a business receives "nonpublic personal information" from a financial institution with which they are not affiliated, it may be limited in its use of that information.

1. Is the Entity a "Financial Institution"?

The Privacy Rule applies to businesses that are "significantly engaged" in "financial activities" as described in section 4(k) of the Bank Holding Company Act. Each entity's activities determine whether they are a "financial institution" under the Privacy Rule. According to the Bank Holding Company Act provision and regulations established by the Federal Reserve Board, "financial activities" include:

- Providing financial, investment or economic advisory services including credit counselors, financial planners, tax preparers, accountants and investment advisors;
- Lending, exchanging, transferring, investing for others, or safeguarding money or securities. These activities cover services offered by lenders, check cashers, wire transfer services, and sellers of money orders;
- Brokering loans, servicing loans, and debt collecting;
- Providing real estate settlement services; and
- Career counseling of individuals seeking employment in the financial services industry.

Under the Privacy Rule, only an institution that is "significantly engaged" in financial activities is considered a financial institution. In making this determination, it is essential to take into account all the facts and circumstances of an entity's financial activities to determine if they are "significantly engaged" in such activities. The FTC's "significantly engaged" standard is intended to exclude certain activities that might otherwise fall under the Privacy Rule. Two factors are particularly important in determining whether

an entity is "significantly engaged" in a financial activity. First, whether there is a formal arrangement is important.

**Example**

A storeowner or bartender who "runs a tab" for customers is not considered to be significantly engaged in financial activities, but a retailer that offers credit directly to consumers by issuing its own credit card would be covered.

Second, how often does the business engage in a financial activity?

**Example**

A retailer that lets some consumers make payments through an occasional lay-away plan is not "significantly engaged" in a financial activity. In contrast, a business that regularly wires money to and from consumers is significantly engaged in a financial activity.

2. Whether an Entity Has "Consumers" or "Customers"?

If a business entity is a financial institution, its obligations depend on whether its clients are "customers" or "consumers." In brief, the Privacy Rule requires entities to give notice to all of its "customers" about its privacy practices, and, if they share their information in certain ways, to their "consumers" as well.

Under the rule, a "consumer" is someone who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that person's legal representative. The term "consumer" does not apply to commercial clients, like sole proprietorships. Therefore, where a client is not an individual, or is an individual seeking your entity's product or service for a business purpose, the Privacy Rule does not apply to you.

Examples of a "consumer" relationship include the following:

- Cashing a check with a check-cashing company;
- Making a wire transfer; or
- Applying for a loan, whether or not the loan is actually obtained.

"Customers" are a subclass of consumers who have a continuing relationship with a financial institution. It is the nature of the relationship – not how long it lasts – that defines your customers. Even if an individual repeatedly uses an entity's services for unrelated transactions, he or she may not be the entity's "customer." For example, if an individual uses the ATM at a bank where she does not have an account, those isolated transactions, no matter how frequent, do not make her that bank's customer. She would still be a "consumer" of that bank, however.

A former customer "has obtained" a financial product or service from a financial institution but no longer has a continuing relationship with it. For purposes of an entity's obligations under the Privacy Rule, a former customer is considered to be a consumer.

Examples of a "customer" relationship include the following:

- Opening a credit card account with a financial institution;
- Leasing an automobile from an auto dealer;
- Using the services of a mortgage broker to secure financing;
- Obtaining the services of a tax preparer or an investment adviser; and
- Getting a loan from a mortgage lender or payday lender.

3. A Word about Customer Relationships and Loans

A special rule defines the customer relationship when several financial institutions participate in a loan transaction. A financial institution establishes a customer relationship with an individual when it originates a loan. If the financial institution sells the loan but maintains the servicing rights, it continues to have a customer relationship with the individual. If the financial institution transfers the servicing rights but retains an ownership interest in the loan, the individual is a "consumer" of that institution and a "customer" of the institution with the servicing rights. If other institutions hold an ownership interest in the loan (but not the servicing rights), the individual is their consumer, too.

4. Covered Information

The Privacy Rule protects a consumer's "nonpublic personal information" (NPI). NPI is any "personally identifiable financial information" that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise "publicly available." NPI is:

- Any information an individual gives an entity to get a financial product or service (for example, name, address, income, social security number, or other information on an application); or
- Any information an entity receives about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

NPI does not include information that you have a reasonable basis to believe is lawfully made "publicly available." In other words, information is not NPI when you have taken steps to determine: (a) that the information is generally made lawfully available to the public; and (b) that the individual can direct that it not be made public and has not done so. For example, while telephone numbers are listed in a public telephone directory, an individual can elect to have an unlisted number. In that case, her phone number would not be "publicly available." Publicly available information includes:

- Federal, state or local government records made available to the public, such as the fact that an individual has a mortgage with a particular financial institution; or

- Information that is in widely distributed media like telephone books, newspapers and websites that are available to the general public on an unrestricted basis, even if the site requires a password or fee for access.

Information in a list form may be NPI, depending on how the list is derived. For example, a list is not NPI if it is drawn entirely from publicly available information, such as a list of a lender's mortgage customers in a jurisdiction that requires that information to be publicly recorded. Also, it is not NPI if the list is taken from information that is not related to an entity's financial activities, for example, a list of individuals who respond to a newspaper ad promoting a non-financial product you sell.

On the other hand, a list derived even partially from NPI is still considered NPI. For example, a creditor's list of its borrowers' names and phone numbers is NPI even if the creditor has a reasonable basis to believe that those phone numbers are publicly available, because the existence of the customer relationships between the borrowers and the creditor is NPI.

| Examples of Nonpublic Personal Information (in List Form) |
|---|
| • List of a retailer's credit card customers |
| • List of a payday lender's customers |
| • List of auto loan customers merged with list of car magazine subscribers |

5. Businesses That Receive NPI from Nonaffiliated Financial Institutions

Even if a business is not a financial institution that has consumers or customers, the Privacy Rule may limit its use of NPI. An entity's ability to reuse and redisclose the information may be restricted if they receive NPI from a nonaffiliated financial institution. It depends on why it was received.

## B. AN ENTITY'S OBLIGATIONS UNDER THE PRIVACY RULE

As originally enacted, the privacy rule's notice provisions applied to CPAs. However, effective October 13, 2006, CPAs are exempt from the GLB Act's requirement that CPAs provide their clients with an annual privacy notice. The exemption was created with passage of the Financial Services Regulatory Relief Act of 2006, the key provisions of which are as follows:

**Sec. 609. Exemption From Disclosure of Privacy Policy for Accountants.**

(a) In General – Section 502 of the Gramm-Leach-Bliley Act (15 U.S.C. 6803) is amended by adding at the end the following:

> (1) IN GENERAL – The disclosure requirements of subsection (a) do not apply to any person, to the extent the person is –
>
> > (A) a certified public accountant;
> >
> > (B) certified or licensed for such purpose by a State; and

(C) subject to any provision of law, rule, or regulation issued by a legislative or regulatory body of the State, including rules of professional conduct or ethics, that prohibit disclosure of nonpublic personal information without the knowing and expressed consent of the consumer.

(2) LIMITATION – Nothing in this subsection shall be construed to exempt or otherwise exclude any financial institution that is affiliated or becomes affiliated with a certified public accountant described in paragraph (1) from any provision of this section.

1. Privacy Notices

Financial institutions must give their customers – and in some cases their consumers – a "clear and conspicuous" written notice describing its privacy policies and practices. When this notice is provided, and what it contains, depends on what the entity does with the information.

2. Persons Entitled to the Notice

**Customers**. Whether or not an entity shares customer NPI, it must give all of its customers a privacy notice. Each entity must provide an "initial notice" by the time the customer relationship is established. If this would substantially delay the customer's transaction, the entity may provide the notice within a reasonable time after the customer relationship is established, but only if the customer agrees.

If an entity shares NPI with nonaffiliated third parties outside of the exceptions described within, the entity also must give its customers:

- An "opt-out" notice explaining the individual's right to direct the entity not to share his or her NPI with non-affiliated third parties;
- A reasonable method for opting out; and
- A reasonable amount of time to opt out prior to disclosing the NPI.

Covered entities must also give their customers an "annual notice" – a copy of their full privacy notice – for as long as the customer relationship lasts.

**Consumers Who Are Not Customers**. Before an entity shares NPI with nonaffiliated third parties outside of the exceptions described within, it must provide its non-customer consumers a privacy notice, including an opt-out notice. If the entity does not share information with nonaffiliated third parties, or if it only shares within the exceptions, the entity is not required to provide a privacy notice to its consumers.

If an entity is required to provide a privacy notice to its consumers, the entity may choose to give them a "short-form notice" instead of a full privacy notice. The short-form notice must:

- Explain that the full privacy notice is available upon request;
- Describe a reasonable way for consumers to get the full privacy notice; and
- Include an opt-out notice.

3. Contents of the Privacy Notice

A covered entity's privacy notice must accurately describe how it collects, discloses, and protects NPI about consumers and customers, including former customers. The notice must include, where applicable, the following information:

- Categories of information collected. For example, nonpublic personal information obtained from an application or a third party such as a consumer-reporting agency;
- Categories of information disclosed. For example, information from an application, such as name, address, phone number, social security number, account information and account balances;
- Categories of affiliates and nonaffiliated third parties to whom the entity discloses the information. For example, financial services providers, such as mortgage brokers and insurance companies or non-financial companies such as magazine publishers, retailers, direct marketers and nonprofit organizations. An entity may describe categories of other nonaffiliated parties to whom it may disclose NPI in the future;
- Categories of information disclosed and to whom it is disclosed under the joint marketing and service provider exception in Section 313.13 of the Privacy Rule;
- Whether the entity is disclosing NPI to nonaffiliated third parties under the exceptions in sections 313.14 (exceptions for processing or administering a financial transaction) and 313.15 (exceptions, including fraud prevention or complying with federal or state law and others) of the Privacy Rule;
- Whether the entity is disclosing NPI to nonaffiliated third parties and the disclosure does not fall within any of the exceptions in sections 313.14 and 313.15, an explanation of consumers' and customers' rights to opt out of these disclosures;
- Any disclosures required by the Fair Credit Reporting Act;
- The entity's policies and practices with respect to protecting the confidentiality and security of NPI.

An entity needs to address only those items above that apply to its particular operations.

## Example

If an accounting firm does not share NPI with affiliates or nonaffiliated third parties except as permitted under sections 313.14 and 313.15, it can provide a simplified notice that: (1) describes its collection of NPI; (2) states that it only discloses NPI to nonaffiliated third parties "as permitted by law;" and (3) explains how the entity protects the confidentiality and security of NPI.

4. The Appearance and Delivery of the Privacy Notice

The privacy notice must be "clear and conspicuous," whether it is on paper or on a website. It must be reasonably understandable, and designed to call attention to the nature and significance of the information. The notice should use plain language, be easy to read, and be distinctive in appearance. A notice on a website should be placed on a page that consumers use often, or it should be hyperlinked directly from a page where transactions are conducted.

The Privacy Rule requires that an entity's privacy notice provide an accurate description of its current policies and practices with respect to protecting the confidentiality and security of NPI. For example, if the entity restricts access to NPI to employees who need the information to provide products or services to its consumers or customers, the notice should so state.

Every covered entity must deliver its privacy notices to each consumer or customer in writing, or, if the consumer or customer agrees, electronically. Written notices may be delivered by mail or by hand. For individuals who conduct transactions with an entity electronically, the entity may post its privacy notice on its website and require them to acknowledge receiving the notice as a necessary part of obtaining a particular product or service. For annual notices, an entity may reasonably expect that its customers have received the notice if they use their website to access their financial products or services and agree to receive notices at the website, and the entity posts its notice continuously in a clear and conspicuous manner on the website. Notices given orally or posted in an entity's office do not comply with the rule.

## C. OPT-OUT NOTICES

1. General Obligations

If a covered entity shares its NPI with nonaffiliated third parties outside of three exceptions, it must provide its consumers and customers an "opt-out notice" that clearly and conspicuously describes their right to opt out of the information being shared. An opt-out notice must be delivered with a privacy notice, and it can be part of the privacy notice.

The opt-out notice must describe a "reasonable means" for consumers and customers to opt out. They must receive the notice and have a reasonable opportunity to opt out before the entity can disclose their NPI to these nonaffiliated third parties. Acceptable "reasonable means" to opt out include a toll-free telephone number or a detachable form with a check-off box and mailing information. Requiring the consumer or customer to write a letter as the only option is not a "reasonable means" to opt out.

While the GLB Act does not require an entity to provide an opt-out notice if it only discloses NPI to affiliates, if the entity shares certain information with its affiliates the entity may have an independent obligation to provide an opt-out notice under the Fair Credit Reporting Act. That opt-out notice must be included in the entity's GLB privacy notice.

2. Exercising the Opt-Out Right

Covered entities must give consumers and customers a "reasonable opportunity" to exercise their right to opt out, for example, 30 days, after they send the initial notice either on- or off-line, before they can share their information with nonaffiliated third parties outside the exceptions. For an isolated consumer transaction, like buying a money order, an entity may require its consumers to make their opt-out decision before completing the transaction.

Consumers and customers who have the right to opt out may do so at any time. Once an entity receives an opt-out direction from existing consumers or customers, it must comply with it as soon as is reasonably possible.

3. The Shelf Life of an Opt-Out Direction

An opt-out direction by a consumer or customer is effective – even after the customer relationship is terminated – until it is canceled in writing, or if the consumer agrees, electronically. However, if a former customer establishes a new customer relationship with an entity and the entity is required to provide an opt-out notice, the customer must make a new opt-out direction that will apply only to the new relationship.

## D. EXCEPTIONS

1. Exceptions to the Notice and Opt-Out Requirements

There are a number of exceptions to the notice and opt-out requirements. These exceptions are located in sections 313.14 ("section 14 exceptions") and 313.15 ("section 15 exceptions") of the Privacy Rule. If you share information only under these sets of exceptions, you do not need to give your *consumers* a privacy notice, but you will need to give your *customers* a simplified initial and, if applicable, an annual privacy notice. Customers and consumers have no right to opt out of these disclosures of NPI.

The section 14 exceptions apply to various types of information sharing that are necessary for processing or administering a financial transaction requested or authorized by a consumer. This includes, for example, disclosing NPI to service providers who help mail account statements and perform other administrative activities for a consumer's account. It also includes disclosures to and by creditors listed by a consumer on a credit application to perform a credit check.

The section 15 exceptions apply to certain types of information sharing, including disclosures for purposes of preventing fraud, responding to judicial process or a subpoena, or complying with federal, state, or local laws. Examples of appropriate information disclosures under this exception include those made to technical service providers who maintain the security of your records; your attorneys or auditors; a purchaser of a portfolio of consumer loans you own; and a consumer-reporting agency, consistent with the Fair Credit Reporting Act.

## TABLE 8.1 SUMMARY OF NOTICE REQUIREMENTS

| Type of Notice | To Whom | When | Contents |
|---|---|---|---|
| Initial | Customers | Not later than when the entity establishes the customer relationship, unless it would substantially delay the transaction and the customer agrees | A description of information-collecting and sharing practices and an opt-out notice (for entities that share NPI with nonaffiliated third parties outside of certain exceptions) |
| | Consumers who are not customers (including former customers) | Before you disclose their NPI to a nonaffiliated third party outside of certain exceptions | Full description of information-collection and sharing practices *or* "short-form" notice, along with opt-out notice |
| Annual | Customers | Delivery on a consistent basis at least once in any period of 12 consecutive months for the duration of the customer relationship | Description of information-collection and sharing practices, and opt-out notice (if you share NPI with nonaffiliated third parties outside of certain exceptions) |

2. Exception to the Opt-Out Requirement: Service Providers and Joint Marketing

Another exception can be found in section 313.13 ("section 13 exception") of the Privacy Rule. If an entity shares information under this exception, it must give its customers – and its consumers if it shares their information – a privacy notice that describes this disclosure. However, consumers and customers do not have a right to opt out of this information sharing.

The section 13 exception covers disclosures for certain service providers and for certain marketing activities. The section 13 exception covers disclosures to third party service providers whose services *for the entity* do not fall within the section 14 exceptions. For example, if an entity hires a nonaffiliated third party to provide services in connection with marketing its products or to market financial products jointly for it and another financial institution, or to do a general analysis of its customer transactions, its disclosure of NPI for these purposes does not fall under the section 14 exceptions. Therefore, the entity can use the section 13 exception for these types of service providers.

The section 13 exception also applies to marketing financial products or services offered through a "joint agreement" with one or more other financial institutions. The "joint agreement" requirement means that an entity has entered into a written contract with one or more *financial* institutions about its joint offering, endorsement, or sponsorship of a *financial* product or service. This does not apply to any kind of joint marketing the entity does, but only joint marketing with other financial institutions and only the marketing of financial products or services.

To take advantage of the section 13 exception, an entity must enter into a contract with those nonaffiliated third parties with whom it shares NPI. The agreement must guarantee the confidentiality of the information by prohibiting the third party or parties from using or disclosing the information for any purpose other than the one for which it was received.

## E. LIMITS ON REUSE AND REDISCLOSURE OF NPI

If an entity receives NPI from a nonaffiliated financial institution, its ability to reuse and redisclose that information is limited. The limits depend on how the information is disclosed to the entity. It does not matter whether or not the entity is a financial institution.

1. Restrictions on Reuse and Redisclosure If NPI Is Received Under the Section 14 or 15 Exceptions

An entity may receive NPI from a nonaffiliated financial institution ("originating financial institution") *under* the section 14 or 15 exceptions. In these situations, the entity may only disclose and use the information in the ordinary course of business to carry out the purpose for which it was received. That purpose may include disclosures to other parties under the section 14 or 15 exceptions in order to carry out that activity, or as otherwise necessary, such as to respond to a subpoena. The entity may also disclose the information to its affiliates, who are limited in their reuse and redisclosure of the information in the same way as they are, and to affiliates of the originating financial institution.

2. Restrictions on Reuse and Redisclosure If NPI Is Received Outside the Section 14 or 15 Exceptions

Alternatively, an entity may receive NPI from a nonaffiliated financial institution *outside* the section 14 or 15 exceptions. For example, an entity may want to purchase a financial institution's customer list in order to market its own products to those individuals. In these cases, the originating financial institution may disclose NPI about those consumers or customers who were informed about this type of disclosure in the privacy notice, and who did not opt out after receiving notice and the opportunity to opt out.

In this situation, the entity may *use* the information internally for its own purposes. However, it may only *redisclose* the information consistent with the privacy policy of the originating financial institution. In other words, the entity steps into the shoes of the originating financial institution and may disclose the same kinds of NPI to the same entities as the originating institution. For example, if the originating financial institution's privacy notice informed its consumers and customers that it would only share their NPI with "nonfinancial institutions, such as charitable organizations," the entity may redisclose the NPI to charitable institutions as well. However, because the originating institution does not disclose NPI to another financial institution, such as an insurance provider, the entity cannot because that type of company is not covered by the privacy policy.

## F. DISCLOSURE OF ACCOUNT NUMBERS IS PROHIBITED

The GLB Act prohibits financial institutions from sharing account numbers or similar access numbers or codes for marketing purposes. This prohibition applies even when a consumer or customer has not opted-out of the disclosure of NPI concerning her account. The prohibition applies to disclosures of account numbers for an individual's credit card account, deposit account, or "transaction account" to any nonaffiliated third party to use in telemarketing, direct mail marketing, or other marketing through

electronic mail to any consumer. A "transaction account" is any account to which a third party may initiate a charge. This provision does not prohibit the sharing of an encrypted account number, if the third party receiving the information has no way to decode it.

This prohibition applies to the complete marketing transaction, including posting a charge to an account. However, it does not apply when a financial institution discloses an account number to its agent or service provider just to market its own products or services, as long as the party receiving the information cannot directly initiate charges to the account.

The exceptions in sections 313.14 and 313.15 of the Privacy Rule do not apply to the disclosure of account numbers for marketing purposes. For example, an entity may not obtain its customer's consent to disclose her account number for marketing purposes.

# III. OTHER ISSUES

## A. THE FAIR CREDIT REPORTING ACT

The Gramm-Leach-Bliley Act's notice and opt-out provisions are in addition to the obligations imposed by the Fair Credit Reporting Act (FCRA). If the FCRA currently requires that a business entity make clear and conspicuous disclosures to its consumers regarding its sharing of certain information (such as consumer report and application information) with its affiliates, the entity must continue to do so. The GLB Act requires these disclosures to be made as part of any privacy policy the financial institution provides to its consumers or customers.

## B. ENFORCEMENT

The FTC, the federal banking agencies, other federal regulatory authorities, and state insurance authorities enforce the GLB Act. Each agency has issued substantially similar rules implementing GLB's privacy provisions. The states are responsible for issuing regulations and enforcing the law with respect to insurance providers. The FTC has jurisdiction over any financial institution or other person not regulated by other government agencies.

The FTC may bring enforcement actions for violations of the Privacy Rule. The FTC can bring actions to enforce the Privacy Rule in federal district court, where it may seek the full scope of injunctive and ancillary equitable relief. The FTC also has authority under Section 5 of the FTC Act to examine privacy policies and practices for deception and unfairness.

## CHAPTER 8: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

| | |
|---|---|
| 1. | **What types of businesses are subject to the provisions of the Gramm-Leach-Bliley Act:**<br><br>**A.** the Act applies only to retail stores that offer revolving credit<br><br>**B.** the Act applies to all businesses that take credit cards<br><br>**C.** the Act applies to financial institutions only<br><br>**D.** the Act applies only to businesses with at least 100 employees |
| 2. | **All of the following are rights given to customers or consumers under the Gramm-Leach-Bliley Act <u>except</u>:**<br><br>**A.** the right to request that their financial institution not share their personal data with third parties<br><br>**B.** the right to a notice of the company's privacy practices<br><br>**C.** the right to inspect the company's books<br><br>**D.** the right to say no to the sharing of credit report or application information with the financial institution's affiliates |
| 3. | **When does the Gramm-Leach-Bliley Act require covered financial institutions to provide customers with an initial privacy notice:**<br><br>**A.** within 30 days of establishing the business relationship<br><br>**B.** no later than when the entity establishes the relationship<br><br>**C.** within 90 days of establishing the business relationship<br><br>**D.** only after the customer has been doing business with the entity for at least one year |

# CHAPTER 8: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

| | |
|---|---|
| **1.** | **A.** Incorrect. Some institutions that fall under FTC jurisdiction for purposes of the GLB Act are nonbank mortgage lenders, loan brokers, some financial or investment advisors, tax preparers, and debt collectors.<br><br>**B.** Incorrect. The Act does not apply to such a broad category.<br><br>**C.** **CORRECT**. Financial institutions include companies that offer financial products including insurance, loans, or investment advice.<br><br>**D.** Incorrect. The number of employees has no effect; rather, it is the type of business that is determinative.<br><br>*(See page 131 of the course material)* |
| **2.** | **A.** Incorrect. Consumers and customers have the right to opt out of, that is, object to, having their information shared with certain third parties. This right must be explained in the financial institution's privacy notice.<br><br>**B.** Incorrect. The Act requires financial institutions to provide customers with a copy of its privacy practices written in clear, conspicuous language.<br><br>**C.** **CORRECT**. The Act protects consumer and customer identity and privacy but does not give individuals access to corporate or business financial information.<br><br>**D.** Incorrect. The privacy notice must explain that consumers have a right to say no to the sharing of certain information – credit report or application information – with the financial institution's affiliates.<br><br>*(See page 133 of the course material.)* |
| **3.** | **A.** Incorrect. The initial notice must be provided sooner than 30 days out.<br><br>**B.** **CORRECT**. A financial institution must provide customers with their initial notice not later than when the business relationship is established. There is no grace period unless provision would unreasonably delay the transaction and the customer waives their right to immediate receipt.<br><br>**C.** Incorrect. There is no such 90 day grace period.<br><br>**D.** Incorrect. An annual notice must be given every year, but the initial notice must be provided sooner than one year after the business relationship is established.<br><br>*(See page 139 of the course material.)* |

# CHAPTER 9: FINANCIAL INSTITUTIONS AND CUSTOMER DATA: COMPLYING WITH THE SAFEGUARDS RULE

## Chapter Objective

**After completing this chapter, you should be able to:**

- Recognize who is impacted by the Safeguards Rule.

## I. OVERVIEW

Many financial institutions collect personal information from their customers, such as banks and credit card numbers, income and credit histories, and social security numbers. If not stored properly, this information can get into the wrong hands and lead to identity theft. The Gramm-Leach-Bliley (GLB) Act – in addition to requiring privacy policy notification discussed in Chapter 8 – requires financial institutions to ensure the security and confidentiality of this type of information. As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) has issued the Safeguards Rule. This rule requires financial institutions under FTC jurisdiction to secure customer records and information.

However, whether your entity is covered by this rule or not, remember that in this day and age, adequately securing customer information makes good business sense. When a business shows customers that it cares about the security of their personal information, the business increases the level of confidence its customers and clients have in their institution.

The Safeguards Rule applies to businesses, regardless of size, that are "significantly engaged" in providing financial products or services to consumers. This includes tax preparers, check-cashing businesses, data processors, mortgage brokers, non-bank lenders, personal property or real estate appraisers and retailers that issue credit cards to customers. The Safeguards Rule also applies to financial companies – such as credit-reporting agencies and ATM operators – that receive information from other institutions about their customers. In addition to developing their own safeguards, financial institutions are responsible for taking steps to ensure that their affiliates and service providers safeguard the customer information in their care.

The FTC began enforcing the provisions of the Safeguards Rule as soon as it took effect. At the end of 2004, the FTC charged two mortgage companies with violating the Safeguards Rule as part of a nationwide compliance sweep.

In an administrative action filed against Nationwide Mortgage Group, Inc. (Nationwide) and its president John D. Eubank, the FTC alleged that the Fairfax, Virginia-based mortgage broker failed to implement safeguards to protect its customers' names, social security numbers, credit histories, bank account numbers, income tax returns, and other sensitive financial information. Sunbelt Lending Services, Inc.

(Sunbelt), a subsidiary of Cendant Mortgage Corporation with headquarters in Clearwater, Florida, agreed to settle similar FTC charges. The settlement with Sunbelt bars future violations of the Safeguards Rule and requires biannual audits of Sunbelt's information security program by a qualified, independent professional for 10 years. These were the FTC's first cases enforcing the Safeguards Rule.

The FTC targeted Nationwide and Sunbelt as part of a nationwide sweep of automobile dealers and mortgage companies to assess compliance with the rule. Although the sweep showed compliance by many of the companies targeted, it also showed significant failures to comply by Nationwide and Sunbelt. According to the FTC's complaints, both companies failed to comply with the rule's basic requirements, including that they assess the risks to sensitive customer information and implement safeguards to control these risks. In addition, Nationwide failed to train its employees on information security issues; oversee its loan officers' handling of customer information; and monitor its computer network for vulnerabilities. Sunbelt also failed to oversee the security practices of its service providers and of its loan officers working from remote locations throughout the state of Florida.

Finally, the complaint alleges that both companies violated the GLB Privacy Rule, which requires financial institutions to provide customers with privacy notices describing how they use and disclose customers' personal information. According to the complaints, Nationwide did not provide the privacy notices to its customers, and Sunbelt did not provide the notices to its online customers.

The proposed consent order with Sunbelt bars the company from future violations of the Safeguards Rule and the Privacy Rule. In addition, the company must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional within six months and every other year thereafter for 10 years. The order also contains standard record-keeping provisions to allow the FTC to monitor Sunbelt's compliance.

# II. THE SAFEGUARDS RULE

## A. WRITTEN PLAN REQUIRED

The Safeguards Rule requires financial institutions to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the information it handles. The plan for Bank of America would not be the same, therefore, as the plan for John Smith & Associates, a small accounting and tax preparation business. As part of its plan, however, each financial institution should do the following:

- Designate one or more employees to coordinate the safeguards;
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- Design and implement a safeguards program, and regularly monitor and test it;
- Select appropriate service providers and contract with them to implement safeguards;

- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring the safeguards.

The above requirements are designed to be flexible. Each financial institution should implement safeguards appropriate to its own circumstances. For example, some financial institutions may choose to describe their safeguards in a single document while others may memorialize their plans in several different documents such as one to cover an information technology division and another to describe the training program for employees. Similarly, a company may decide to designate a single employee to coordinate the safeguards program or may spread this responsibility among several employees in different departments. Again, the size and complexity of a business will dictate what makes sense in each case.

## B. SECURING INFORMATION

When a firm implements its safeguards, the Safeguards Rule requires it to consider all areas of its operation, including those areas that are particularly important to information security:

- Employee management and training;
- Information systems; and
- Managing system failures.

Firms are encouraged to implement the following practices in these areas.

1. Employee Management and Training

The success or failure of a firm's information security plan depends largely on the employees who implement it. As such, firms may wish to do the following:

- Check references prior to hiring employees who will have access to customer information;
- Ask every new employee to sign an agreement to follow the firm's confidentiality and security standards for handling customer information;
- Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, such as:
    - Locking rooms and file cabinets where paper records are kept;
    - Using password-activated screensavers;
    - Using strong passwords (at least 10 characters in length);
    - Changing passwords periodically, and not posting passwords near employees' computers;
    - Encrypting sensitive customer information when it is transmitted electronically over networks or stored online;

- Referring calls or other requests for customer information to designated individuals who have had safeguards training; and
- Recognizing any fraudulent attempt to obtain customer information and reporting it to appropriate law enforcement agencies.

- Instruct and regularly remind all employees of the firm's policy – and the legal requirement – to keep customer and client information secure and confidential. Firms may want to provide employees with a detailed description of the type of customer information it handles and post reminders about their responsibilities in areas where such information is stored – i.e., in a file room;
- Limit access to customer information to employees with a business need for seeing it. For example, grant access to customer information files to employees who respond to customer inquiries, but only to the extent necessary to do their jobs; and
- Impose disciplinary measures for breaches of the firm's policies.

2. Information Systems

Information systems include network and software design, and information processing, storage, transmission, retrieval and disposal. The following are suggestions for maintaining security throughout the life cycle of customer or client information – that is, from data entry to data disposal:

- Store records in a secure area. Make sure only authorized employees have access to the area. For example:
  - Store paper records in a room, cabinet or other container that is locked when unattended;
  - Ensure that storage areas are protected against destruction or potential damage from natural hazards like fire or flood;
  - Store electronic consumer or client information on a secure server that is accessible only with a password – or has other security protections – and is kept in a physically-secure area;
  - Do not store sensitive customer data on a machine with an Internet connection; and
  - Maintain secure backup media and keep archived data secure, for example, by storing offline or in a physically secure area.
- Provide for secure data transmission (with clear instructions and simple security tools) when the firm collects or transmits customer information. Specifically:
  - If a firm collects credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection so that the information is encrypted in transit;

    - If a firm collects information directly from customers or clients, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via electronic mail; and
    - If a firm must transmit sensitive data by electronic mail, ensure that such messages are password protected so that only authorized employees have access.
- Dispose of customer information in a secure manner. For example:
    - Hire or designate a records retention manager to supervise disposal of records containing nonpublic personal information;
    - Shred customer information recorded on paper;
    - Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contains customer information;
    - Effectively destroy the hardware; and
    - Promptly dispose of outdated customer information.
- Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. For example, supplement each of the firm's customer lists with at least one entry (such as an account number or address) that it controls, and monitor use of this entry to detect all unauthorized contacts or charges; and
- Maintain a close inventory of computers.

3. Managing System Failures

Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures. Consider the following suggestions in implementing a firm's safeguards:

- Maintain up-to-date and appropriate programs and control by:
    - Following a written contingency plan to address all breaches of the firm's physical, administrative or technical safeguards;
    - Checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities;
    - Using anti-virus software that updates automatically;
    - Maintaining up-to-date firewalls, particularly if the firm uses broadband Internet access or allows employees to connect to the firm's network from home or other off-site locations; and
    - Providing central management of security tools for employees and passing along updates about any security risks or breaches.
- Take steps to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure. For example, back up all customer information regularly;

- Maintain systems and procedures to ensure that access to nonpublic consumer information is granted only to legitimate and valid users. For example, use tools like passwords combined with personal identifiers to authenticate the identity of customers and others seeking to do business with the financial institution electronically; and
- Notify customers promptly if their nonpublic personal information is subject to loss, damage or unauthorized access.

## III. FEDERAL REGULATIONS

**Part 314. Standards for Safeguarding Customer Information**

**§ 314.1 Purpose and scope.**

(a) Purpose. This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) Scope. This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. This part refers to such entities as "you." This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

**§ 314.2 Definitions.**

(a) In general. Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) Customer information means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(c) Information security program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(d) Service provider means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

**314.3 Standards for safeguarding customer information.**

(a) Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity,

the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) Objectives. The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

**§ 314.4 Elements.**

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

**§ 314.5 Effective date.**

(a) Each financial institution subject to the Commission's jurisdiction must implement an information security program pursuant to this part no later than May 23, 2003.

(b) Two-year grandfathering of service contracts. Until May 24, 2004, a contract you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of § 314.4(d), even if the contract does not include a requirement that the service provider maintain appropriate safeguards, as long as you entered into the contract not later than June 24, 2002.

# IV. LIMITING IDENTITY THEFT

Given the particularly sensitive nature of the banking industry, this section focuses on suggestions from the Office of Controller of the Currency to limit identity theft in the banking industry. Many of these suggestions can be used in other financial services businesses as well.

## A. PROCEDURES AND GUIDELINES

1. Verification Procedures for New Accounts

To reduce the risk of fraudulent applications, banks should establish verification procedures to ensure the accuracy and veracity of application information. In conjunction with their existing account opening procedures, banks should consider how best to independently verify information provided on account applications to detect incidents of identity theft. Verification of personal information may be accomplished in a number of ways. Some alternatives to consider include: (a) *positive verification* to ensure material information provided by an applicant is accurate; (b) *logical verification*; and (c) *negative verification* to ensure information provided has not previously been associated with fraudulent activity.

***Positive verification*** entails consulting third-party sources to assess the veracity of information submitted by a consumer. For example, an identity thief may provide the true name of an individual and a correct phone number, but an erroneous address. An institution could detect this discrepancy simply by checking a telephone directory. Under appropriate circumstances, a bank may obtain an individual's consumer report that would permit more detailed verification. Banks should consider calling a customer to confirm that the individual has opened a credit card or checking account, using a telephone number that has been verified independently. A phone call to a customer may alert an individual that his or her identity has been stolen. Additionally, a bank could contact an applicant's employer. An identity thief may provide the name of a legitimate employer, but may not provide the correct telephone number. A bank should attempt to contact an employer using an independently verified telephone number. Contacting an employer may expose a fraudulent application.

***Logical verification*** entails assessing the consistency of information presented in an application. Such steps may reveal inconsistencies in the information provided by an applicant. For instance, a bank could verify if the zip code and telephone area code provided on the application cover the same geographical area. Products currently available from service providers can assist banks in verifying logical zip and area codes.

***Negative verification*** entails ensuring that information provided on an application has not previously been associated with fraudulent activity.

2. Other New Account Procedures

Consumer reports can be an important source for preventing fraud. When processing an application for a new account, a bank may rely on a consumer report from a consumer-reporting agency. A consumer report of a victim of identity theft may be issued with a fraud alert. When a bank has an automated system for credit approval, these systems should be designed to identify fraud alerts. Banks should not process an application when there is an existing fraud alert without contacting the individual in accordance with instructions that usually accompany a fraud alert (i.e., a victim's statement), or otherwise employing additional steps to verify the individual's identity. The bank should have procedures in place to share a fraud alert across its various lines of business.

Consumer reports also may be a source for detecting fraud. Signs of possible fraudulent activity that may appear on consumer reports include late payments on a consumer's accounts in the absence of a previous history of late payments, numerous credit inquiries in a short period of time, higher-than-usual monthly credit balances, and a recent change of address in conjunction with other signs.

Finally, when an applicant fails to provide all requested information on an application, a bank should not process the incomplete application without further explanation.

3. Verifying Change of Address Requests

A change of address request on an existing account may be a sign of fraudulent activity. A bank should verify the customer information before executing an address change and send a confirmation of the address change to both the new address and the address of record. If an institution gets a request for a new credit card or new checks in conjunction with a change of address notification, the bank should verify the request with the customer within a reasonable period of time after receiving the request.

4. Security Standards

Federal Guidelines for Safeguarding Customer Information require banks to implement a comprehensive information security program that includes appropriate administrative, technical, and physical safeguards for customer information. Information security programs must be designed to ensure the security and confidentiality of customer information, protect against anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.

Banks should take steps to secure the transmission and storage of electronic information to prevent identity thieves from gaining access to such information. This may include the use of encryption, firewalls, and other electronic data security systems and preventative measures. Identity thieves may also seek access to information that an institution discards. For instance, identity thieves may rummage through trash to collect customer information (dumpster diving). A bank should implement appropriate measures to restrict access to its customer records, such as by shredding documents, to protect against dumpster diving and other forms of unauthorized access.

Banks and their service providers should implement appropriate controls and procedures to limit access to customer records. Because insiders may be identity thieves, a bank should consider conducting background checks for its employees, in accordance with applicable law. Where indicated by its risk assessment, a bank should also monitor its service providers to confirm that they have implemented appropriate measures to limit access to customer records.

## B. PRETEXT CALLING

As mentioned in Chapter 2, pretext callers use pieces of personal information to impersonate an account holder in order to gain access to that individual's account information. Armed with personal information, such as an individual's name, address, and social security number, a pretext caller may try to convince a bank's employee to provide confidential account information. While it may be difficult to spot, there are measures banks can take to reduce the incidence of pretext calling, such as limiting the circumstances under which customer information may be disclosed by telephone.

The Guidelines for Safeguarding Customer Information require banks to establish written policies and procedures to control risks to customer information, and consider access controls on customer information as part of these policies and procedures. Banks should take appropriate precautions against the disclosure of customer information to unauthorized individuals such as (1) limiting the circumstances under which employees may disclose customer information over the telephone, (2) training employees to recognize and report fraudulent attempts to obtain customer information, and (3) testing to determine the effectiveness of controls designed to thwart pretext callers.

1. Limiting Telephone Disclosures

There are a number of ways in which banks may limit access to customer information. One way is to permit employees to release information over the telephone only if the individual requesting the information provides a proper authorization code. The code should be different than other commonly used numbers or identifiers, such as social security numbers, savings, checking, loan, or other financial account numbers, or the maiden name of the customer's mother. The authorization code should be unique to, and capable of being changed readily by, the authorized account holder. To be most effective, the authorization code should be used in conjunction with other customer and account identifiers.

Another means of preventing unauthorized disclosures of customer information is to use a caller identification system (i.e., CallerID™). If the telephone number displayed differs from that in the customer's account records, it may be an indication that the request is not legitimate and the employee should not disclose the requested account information without taking additional steps to verify that the true customer is making the request. In the absence of a caller identification system, banks could require employees who receive calls for account information to ask the caller for the number from which he or she is calling, or for a call-back number. If the individual refuses to provide the number, or it does not match the information in the customer's records, the employee should not disclose the information without additional measures to verify that the caller is the true customer.

2. Employee Training

Banks should train staff to recognize unauthorized or fraudulent attempts to obtain customer information. In addition to an employee's inability to match a caller's telephone number with that on file, there may be other indicators of a pretext call. For instance, a caller who cannot provide all relevant information requested, or a caller who is abusive, or who tries to distract the employee, may be a pretext caller. Employees should be trained to recognize such devices and, under such circumstances, protect customer information through appropriate measures, such as by taking additional steps to verify that the caller is a bona fide customer.

Employees should be trained to implement the bank's written policies and procedures governing the disclosure of customer information, and should be informed not to deviate from them. Moreover, employees must know to whom and how to report suspicious activity that may be a pretext call. Banks may have a fraud department or contact to whom the employee reports suspicious activities, or may establish another means for reporting possible fraud. Known or suspected federal criminal violations should be reported to law enforcement in accordance with the procedures discussed below.

3. Testing

Banks should test the key controls and procedures of their information security systems and consider using independent staff or third parties to conduct unscheduled pretext phone calls to various departments to evaluate the institution's susceptibility to unauthorized disclosures of customer information. Any weaknesses should be addressed through enhanced training, procedures, or controls, or a combination of these elements.

## C. REPORTING SUSPECTED IDENTITY THEFT AND PRETEXT CALLING

Federal regulations currently require banks to report all known or suspected criminal violations to law enforcement and the Office of the Controller of the Currency (OCC) by the use of the Suspicious Activity Report ("SAR").

Criminal activity related to identity theft or pretext calling has historically manifested itself as credit or debit card fraud, loan or mortgage fraud, or false statements to the bank, among other things. Presumably, banks have been reporting such known or suspected criminal violations through the use of the SARs, in accordance with existing regulations.

As a means of better identifying and tracking known or suspected criminal violations related to identity theft and pretext calling, a bank should, in addition to reporting the underlying fraud (such as credit card or loan fraud) on a SAR, also indicate within the SAR that such a known or suspected violation is the result of identity theft or pretext calling.

Consistent with the SAR instructions, in situations involving violations requiring immediate attention, such as when a reportable violation is ongoing, a bank should immediately notify, by telephone, the OCC and appropriate law enforcement, in addition to filing a timely suspicious activity report.

## D. CUSTOMER ASSISTANCE

1. Teaching Prevention

Educating consumers about preventing identity theft and identifying potential pretext calls may help reduce their vulnerability to these fraudulent practices. Banks should consider making available to their customers brochures, newsletters, or notices posted in their lobbies or on their Web sites describing preventative measures consumers can take to avoid becoming victims of these types of fraud. Banks are strongly encouraged to inform their customers of the following precautionary measures that law enforcement recommends to protect against identity theft and pretext calling:

- Do not give personal information, such as account numbers or social security numbers, over the telephone, through the mail, or over the Internet unless you initiated the contact or know with whom you are dealing;
- Store personal information in a safe place and tear up old credit card receipts, ATM receipts, old account statements, and unused credit card offers before throwing them away;
- Protect your PINs and other passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your social security number, your phone number, etc;
- Carry only the minimum amount of identifying information and the number of credit cards that you need;
- Pay attention to billing cycles and statements. Inquire of the bank if you do not receive a monthly bill; it may mean the bill has been diverted by an identity thief;
- Check account statements carefully to ensure all charges, checks, or withdrawals were authorized;
- Guard your mail from theft. If you have the type of mailbox with a flag to signal the box contains mail, do not leave bill payment envelopes in your mailbox with the flag up. Instead, deposit them in a post office collection box or at the local post office. Promptly remove incoming mail;
- Order copies of your credit report from each of the three major credit bureaus once a year to ensure they are accurate. All Americans are entitled to receive free credit reports every year. Each of the three major credit agencies, Equifax, TransUnion, and Experian are required to provide consumers, upon request, with a free copy of their credit report once per year;
- If you prefer not to receive preapproved offers of credit, you can opt out of such offers by calling 1-888-5-OPT OUT;

- If you want to remove your name from many national direct mail lists, send your name and address to:

DMA Mail Preference Service
P.O. Box 9008
Farmingdale, NY 11735-9008

- If you want to reduce the number of telephone solicitations from many national marketers, send your name, address and telephone number to:

DMA Telephone Preference Service
P.O. Box 9014
Farmingdale, NY 11735-9014

2. Assistance for Victims

There are a number of measures banks can take to assist victims of such fraud. These include:

- Having trained personnel respond to customer calls regarding identity theft or pretext calling;
- Determining if it is necessary to close an account immediately after a customer reports unauthorized use of that account, and issuing the customer a new credit card, ATM card, debit card or checks, as appropriate. Where a customer has multiple accounts with an institution, the institution should assess whether any other account has been the subject of potential fraud; and
- Educating customers about appropriate steps to take if they have been victimized.

# CHAPTER 9: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

| | |
|---|---|
| 1. | **What is the term for consulting third-party sources to assess the veracity of information submitted by a consumer:**<br><br>**A.** positive verification<br><br>**B.** logical verification<br><br>**C.** negative verification<br><br>**D.** independent verification |
| 2. | **Each of the following is a recommended practice to prevent pretext calling <u>except</u>:**<br><br>**A.** require individuals requesting information to provide a proper social security number or a savings account number<br><br>**B.** do not disclose information if the caller is calling from a number different than the one in the customer's records<br><br>**C.** train staff to recognize a caller who is being abusive or trying to distract the employee<br><br>**D.** use independent staff or third parties to conduct unscheduled pretext phone calls in order to test the key controls and procedures |

# CHAPTER 9: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

| | |
|---|---|
| **1.** | **A.** **CORRECT**. An identity thief may provide the true name of an individual and a correct phone number, but an erroneous address. An institution could detect this discrepancy simply by checking a telephone directory. This would be positive verification.<br><br>**B.** Incorrect. Logical verification entails assessing the consistency of information presented in an application.<br><br>**C.** Incorrect. Negative verification entails ensuring that information provided on an application has not previously been associated with fraudulent activity.<br><br>**D.** Incorrect. Independent verification is a nonsense term regarding the verification procedures of new accounts.<br><br>*(See page 158 of the course material.)* |
| **2.** | **A.** **CORRECT**. One way is to permit employees to release information over the telephone only if the individual requesting the information provides a proper authorization code. The code should be different than other commonly used numbers or identifiers, such as social security numbers, savings, checking, loan, or other financial account numbers, or the maiden name of the customer's mother.<br><br>**B.** Incorrect. In the absence of a caller identification system, banks could require employees who receive calls for account information to ask the caller for the number from which he or she is calling, or for a call-back number. If the individual refuses to provide the number, or it does not match the information in the customer's records, the employee should not disclose the information without additional measures to verify that the caller is the true customer.<br><br>**C.** Incorrect. Banks should train staff to recognize unauthorized or fraudulent attempts to obtain customer information. In addition to an employee's inability to match a caller's telephone number with that on file, there may be other indicators of a pretext call. For instance, a caller who cannot provide all relevant information requested, or a caller who is abusive, or who tries to distract the employee, may be a pretext caller.<br><br>**D.** Incorrect. Banks should test the key controls and procedures of their information security systems and consider using independent staff or third parties to conduct unscheduled pretext phone calls to various departments to evaluate the institution's susceptibility to unauthorized disclosures of customer information.<br><br>*(See page 161 of the course material.)* |

# CHAPTER 10: THE DISPOSAL RULE AND THE RED FLAGS RULE

## Chapter Objectives

**After completing this chapter, you should be able to:**

- Recognize the impact of the federal Disposal Rule.
- Recall who must comply with the Red Flags Rule.

## I. OVERVIEW

The Red Flags Rule and the Disposal rule are two anti-fraud regulations. The Red Flags Rule requires creditors and financial institutions with covered accounts to execute mechanisms to identify, detect, and respond to the warning signs, or 'red flags,' that could signify identity theft. The Disposal Rule requires any business or individual who uses a consumer report for a business purpose to follow the requirements of the Disposal Rule, a part of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which calls for the proper disposal of information in consumer reports and records to protect against unauthorized access to or use of the information.

## II. THE DISPOSAL RULE

In an effort to protect the privacy of consumer information and reduce the risk of fraud and identity theft, federal regulations requires businesses to take appropriate measures to dispose of sensitive information obtained from consumer reports.

Any business or individual who uses a consumer report for a business purpose is subject to the requirements of the so-called "Disposal Rule." In a nutshell, the rule requires the proper disposal of information in consumer reports and records to protect against "unauthorized access to or use of the information." The Federal Trade Commission (FTC) is responsible for enforcing the disposal rule.

The disposal rule is a part of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which calls for the proper disposal of information in consumer reports and records to protect against "unauthorized access to or use of the information." The rules took effect June 1, 2005.

The rule requires that covered entities "take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." The standard for disposal is flexible to allow entities covered by the rule to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and relevant changes in technology over time.

The rule applies to "any person that, for a business purpose, maintains or otherwise possesses consumer information, or any compilation of consumer information." Any company, regardless of industry or size, that possesses or maintains consumer information for a business purpose will be subject to the rule. Therefore, numerous small entities across almost every industry could potentially be subject to the rule.

According to the FTC, the standard for the proper disposal of information derived from a consumer report is flexible, and allows the firms and individuals covered by the rule to determine what measures are reasonable based on a number of factors, including:

- The sensitivity of the information;
- The costs and benefits of different disposal methods; and
- Changes in technology.

The disposal rule applies to consumer reports or information derived from consumer reports. The Fair Credit Reporting Act defines the term consumer report to include information obtained from a consumer reporting company that is used – or expected to be used – in establishing a consumer's eligibility for credit, employment, or insurance, among other purposes. Credit reports and credit scores are consumer reports. So are reports businesses or individuals receive with information relating to employment background, check writing history, insurance claims, residential or tenant history, or medical history.

Although the disposal rule applies to consumer reports and the information derived from consumer reports, the FTC encourages those who dispose of any records containing a consumer's personal or financial information to take similar protective measures.

## A. COVERAGE OF THE DISPOSAL RULE

1. Persons and Firms Who Must Comply

The disposal rule applies to people, and both large and small organizations, that use consumer reports. Among those who must comply with the rule are:

- Consumer reporting companies;
- Tax preparers;
- Lenders;
- Insurers;
- Employers;
- Landlords;
- Government agencies;
- Mortgage brokers;
- Automobile dealers;

- Attorneys or private investigators;
- Debt collectors;
- Individuals who obtain a credit report on prospective nannies, contractors, or tenants; and
- Entities that maintain information in consumer reports as part of their role as service providers to other organizations covered by the Rule.

2. Proper Disposal Defined

The disposal rule requires disposal practices that are reasonable and appropriate to prevent the unauthorized access to – or use of – information in a consumer report. For example, reasonable measures for disposing of consumer report information could include establishing and complying with policies to:

- Burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed;
- Destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed;
- Conduct due diligence and hire a document destruction coordinator to dispose of material specifically identified as consumer report information consistent with the rule. Due diligence could include any of the following:
    - Reviewing an independent audit of a disposal company's operations and/or its compliance with the rule;
    - Obtaining information about the disposal company from several references;
    - Requiring that the disposal company be certified by a recognized trade association; or
    - Reviewing and evaluating the disposal company's information security policies and procedures.

According to the FTC, financial institutions that are subject to both the disposal rule and the Gramm-Leach-Bliley (GLB) Safeguards Rule (discussed in detail in Chapter 9) should incorporate practices dealing with the proper disposal of consumer information into the information security program that the Safeguards Rule requires.

The Fair and Accurate Credit Transactions Act, which was enacted in 2003, directed the FTC, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and National Credit Union Administration and the Securities and Exchange Commission to adopt comparable and consistent rules regarding the disposal of sensitive consumer report information.

3. Anticipated Costs of Compliance

Because the rule does not mandate specific disposal measures, a precise estimate of compliance costs is not feasible. However, there are certain basic steps that are likely to be appropriate for many small entities. For example, shredding or burning paper records containing consumer information will generally be appropriate. Depending upon the volume of records at issue and the office equipment available to the small entity, this method of disposal may be accomplished by the small entity itself at no cost, may require the purchase of a paper shredder (available at office supply stores for as little as $25), or may require the hiring of a document disposal service on a periodic basis (the costs of which will vary based on the volume of material, frequency of service, and geographic location).

If a small entity has stored consumer information on electronic media (for example, computer discs or hard drives), disposal of such media could be accomplished by a small entity at almost no cost by simply smashing the material with a hammer. In some cases, appropriate disposal of electronic media might also be accomplished by overwriting or "wiping" the data prior to disposal. Utilities to accomplish such wiping are widely available for under $25; indeed, some such tools are available for download on the Internet at no cost.

Whether "wiping," as opposed to destruction, of electronic media is reasonable, as well as the adequacy of particular utilities to accomplish that "wiping," will depend upon the circumstances.

The FTC believes that all businesses, regardless of size, will need to educate and train their employees on proper disposal. The actual amount of time it will take to ensure that consumer report information is properly disposed will vary, depending on a variety of circumstances, including the amount and nature of covered records. However, the Commission believes many businesses may already be following industry best practices, which may include disposing of documents through shredders, using waste disposal companies, or other confidential disposal methods; and continuing to do so would not impose additional costs on such businesses.

## B. FINAL RULE

**16 CFR Part 682**

Consumer reports, Consumer reporting agencies, Credit, Fair Credit Reporting Act, Trade practices.

**PART 682 – DISPOSAL OF CONSUMER REPORT INFORMATION AND RECORDS**

Sec.

682.1 Definitions.

682.2 Purpose and scope.

682.3 Proper disposal of consumer information.

682.4 Relation to other laws.

682.5 Effective date.

**Authority:** Pub. L. 108-159, sec.216.

**§ 682.1 Definitions.**

*(a) In general. Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.*

*(b) "Consumer information" means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data.*

*(c) "Dispose," "disposing," or "disposal" means:*

*(1) the discarding or abandonment of consumer information, or*

*(2) the sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored.*

**§ 682.2 Purpose and scope.**

*(a) Purpose. This part ("rule") implements section 216 of the Fair and Accurate Credit Transactions Act of 2003, which is designed to reduce the risk of consumer fraud and related harms, including identity theft, created by improper disposal of consumer information.*

*(b) Scope. This rule applies to any person over which the Federal Trade Commission has jurisdiction, that, for a business purpose, maintains or otherwise possesses consumer information.*

**§ 682.3 Proper disposal of consumer information.**

*(a) Standard. Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.*

*(b) Examples. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include the following examples.*

*These examples are illustrative only and are not exclusive or exhaustive methods for complying with this rule.*

*(1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed.*

*(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.*

*(3) After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material,*

*specifically identified as consumer information, in a manner consistent with this rule. In this context, due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.*

*(4) For persons or entities who maintain or otherwise possess consumer information through their provision of services directly to a person subject to this part, implementing and monitoring compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with examples (1) and (2) above.*

*(5) For persons subject to the Gramm-Leach-Bliley Act, 15 U.S.C. 6081 et seq., and the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR Part 314 ("Safeguards Rule"), incorporating the proper disposal of consumer information as required by this rule into the information security program required by the Safeguards Rule.*

**§ 682.4 Relation to other laws. Nothing in this rule shall be construed:**

*(a) to require a person to maintain or destroy any record pertaining to a consumer that is not imposed under other law; or*

*(b) to alter or affect any requirement imposed under any other provision of law to maintain or destroy such a record.*

**§ 682.5 Effective date.**

*This rule is effective on June 1, 2005.*

## III. RED FLAGS RULE

Developed under the Fair and Accurate Credit Transactions Act, in which Congress directed the FTC and other agencies to develop regulations requiring "creditors" and "financial institutions" to address the risk of identity theft, the Red Flags Rule requires all such entities that have "covered accounts" to develop and implement written identity theft prevention programs to help identify, detect, and respond to patterns, practices, or specific activities – known as "red flags" – that could indicate identity theft.

The Rule became effective on January 1, 2008, with full compliance for all covered entities originally required by November 1, 2008. The Commission has issued several Enforcement Policies delaying enforcement of the Rule to allow Congress time to finalize legislation that would limit the scope of business covered by the Rule.

The Red Flag Program Clarification Act of 2010 signed into law on December 18th narrows that applicability of the Red Flags identity theft requirements and now excludes service providers such as CPAs, lawyers, and doctors.

The SEC's identity theft red flags rules require certain SEC-regulated entities to adopt a written identity theft program that includes policies and procedures designed to:

- Identify relevant types of identity theft red flags;
- Detect the occurrence of those red flags;
- Respond appropriately to the detected red flags; and
- Periodically update the identity theft program.

Entities that are required to adopt identity theft programs also must provide for the administration of the program, including staff training and oversight of service providers. The rules do not single out specific red flags as mandatory, require specific policies and procedures to identify possible red flags, or provide a specific method of detecting red flags. The rules do, however, include guidelines and examples of red flags to help firms administer their programs. An identity theft program should be appropriate to the size and complexity of the entity and the nature and scope of its activities.

The SEC's rules also require SEC-regulated entities that issue debit cards or credit cards to take certain precautionary actions when they receive a request for a new or replacement card soon after they receive a notification of a change of address for a consumer's account. The SEC expects few, if any, SEC-regulated entities to be subject to these "card issuer" rules.

The Red Flags Rule tells you how to develop, implement, and administer an identity theft prevention program. A program must include four basic elements that create a framework to deal with the threat of identity theft.

- A program must include reasonable policies and procedures to identify the red flags of identity theft that may occur in your day-to-day operations. Red Flags are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft. For example, if a customer has to provide some form of identification to open an account with your company, an ID that doesn't look genuine is a "red flag" for your business.
- A program must be designed to detect the red flags you've identified. If you have identified fake IDs as a red flag, for example, you must have procedures to detect possible fake, forged, or altered identification.
- A program must spell out appropriate actions you'll take when you detect red flags.
- A program must detail how you'll keep it current to reflect new threats.

Just getting something down on paper won't reduce the risk of identity theft. That's why the Red Flags Rule has requirements on how to incorporate your program into the daily operations of your business. Fortunately, the Rule also gives you the flexibility to design a program appropriate for your company

– its size and potential risks of identity theft. While some businesses and organizations may need a comprehensive program to address a high risk of identity theft, a streamlined program may be appropriate for businesses facing a low risk.

Securing the data you collect and maintain about customers is important in reducing identity theft. The Red Flags Rule seeks to prevent identity theft, too, by ensuring that your business or organization is on the lookout for the signs that a crook is using someone else's information, typically to get products or services from you without paying for them. That's why it's important to use a one-two punch in the battle against identity theft: implement data security practices that make it harder for crooks to get access to the personal information they use to open or access accounts, and pay attention to the red flags that suggest that fraud may be afoot.

## A. WHO MUST COMPLY: A TWO-PART ANALYSIS

The Red Flags Rule requires "financial institutions" and some "creditors" to conduct a periodic risk assessment to determine if they have "covered accounts." The determination isn't based on the industry or sector, but rather on whether a business' activities fall within the relevant definitions. A business must implement a written program only if it has covered accounts.

1. Financial Institutions

The Red Flags Rule defines a "financial institution" as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or a person that, directly or indirectly, holds a transaction account belonging to a consumer. While many financial institutions are under the jurisdiction of the federal bank regulatory agencies or other federal agencies, state-chartered credit unions are one category of financial institution under the FTC's jurisdiction.

2. Creditors

An SEC-regulated entity will generally qualify as a creditor if it advances or loans money to consumers. However, an entity will not qualify as a creditor if it advances money for expenses incidental to a service provided by the entity.

The Red Flags Rule defines "creditor" based on conduct.

To determine if your business is a creditor under the Red Flags Rule, ask these questions:

Does my business or organization regularly:

- Defer payment for goods and services or bill customers?
- Grant or arrange credit?
- Participate in the decision to extend, renew, or set the terms of credit?

If you answer:

- No to all, the Rule does not apply.

- Yes to one or more, ask:

Does my business or organization regularly and in the ordinary course of business:

- Get or use consumer reports in connection with a credit transaction?
- Give information to credit reporting companies in connection with a credit transaction?
- Advance funds to – or for – someone who must repay them, either with funds or pledged property (excluding incidental expenses in connection with the services you provide to them)?

If you answer:

- No to all, the Rule does not apply.
- Yes to one or more, you are a creditor covered by the Rule.

3. Covered Accounts

If you conclude that your business or organization is a financial institution or a creditor covered by the Rule, you must determine if you have any "covered accounts," as the Red Flags Rule defines that term. You'll need to look at existing accounts and new ones.

Two categories of accounts are covered:

- A consumer account for your customers for personal, family, or household purposes that involves or allows multiple payments or transactions. Examples are credit card accounts, mortgage loans, automobile loans, checking accounts, and savings accounts.
- "Any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks." Examples include small business accounts, sole proprietorship accounts, or single transaction consumer accounts that may be vulnerable to identity theft. Unlike consumer accounts designed to allow multiple payments or transactions – always considered "covered accounts" under the Rule – other types of accounts are "covered" only if the risk of identity theft is reasonably foreseeable.

In determining if accounts are covered under the second category, consider how they're opened and accessed. For example, there may be a reasonably foreseeable risk of identity theft in connection with business accounts that can be accessed remotely – say, through the Internet or the telephone. Your risk analysis must consider any actual incidents of identity theft involving accounts like these.

If you don't have any covered accounts, you don't need a written program. But business models and services change. You may acquire covered accounts through changes to your business structure, process, or organization. That's why it's good policy and practice to conduct a periodic risk assessment.

## B. HOW TO COMPLY: A FOUR-STEP PROCESS

Many companies already have plans and policies to combat identity theft and related fraud. If that's the case for your business, you're already on your way to full compliance.

1. Identify Relevant Red Flags

What are "red flags"? They're the potential patterns, practices, or specific activities indicating the possibility of identity theft. Consider:

**Risk Factors**. Different types of accounts pose different kinds of risk. For example, red flags for deposit accounts may differ from red flags for credit accounts, and those for consumer accounts may differ from those for business accounts. When you are identifying key red flags, think about the types of accounts you offer or maintain; the ways you open covered accounts; how you provide access to those accounts; and what you know about identity theft in your business.

**Sources of Red Flags**. Consider other sources of information, including the experience of other members of your industry. Technology and criminal techniques change constantly, so it's important to keep up-to-date on new threats.

**Categories of Common Red Flags.** Supplement A to the Red Flags Rule lists specific categories of warning signs to consider including in your program. The examples here are one way to think about relevant red flags in the context of your own business.

- Alerts, Notifications, and Warnings from a Credit Reporting Company. Changes in a credit report or a consumer's credit activity might signal identity theft:
    - a fraud or active duty alert on a credit report
    - a notice of credit freeze in response to a request for a credit report
    - a notice of address discrepancy provided by a credit reporting company
    - a credit report indicating a pattern inconsistent with the person's history, for example, an increase in the volume of inquiries or the use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account that was closed because of an abuse of account privileges

**Suspicious Documents**. Documents can offer hints of identity theft:

- Identification looks altered or forged
- The person presenting the identification doesn't look like the photo or match the physical description
- Information on the identification differs from what the person with identification is telling you or doesn't match a signature card or recent check
- An application looks like it's been altered, forged, or torn up and reassembled

**Personal Identifying Information**. Personal identifying information can indicate identity theft:

- Inconsistencies in the information a customer has submitted to you
- An address, phone number, or other personal information already used on an account you know to be fraudulent
- A bogus address, an address for a mail drop or prison, a phone number that's invalid, or one that's associated with a pager or answering service
- A social security number used by someone else opening an account
- An address or telephone number used by several people opening accounts
- A person who omits required information on an application and doesn't respond to notices that the application is incomplete
- A person who can't provide authenticating information beyond what's generally available from a wallet or credit report – for example, someone who can't answer a challenge question

**Account Activity**. How the account is being used can be a tip-off to identity theft:

- Shortly after you're notified of a change of address, you're asked for new or additional credit cards, or to add users to the account
- A new account used in ways associated with fraud – for example, the customer doesn't make the first payment, or makes only an initial payment; or most of the available credit is used for cash advances or for jewelry, electronics, or other merchandise easily convertible to cash
- An account used outside of established patterns
- An account that is inactive is used again
- Mail sent to the customer that is returned repeatedly as undeliverable although transactions continue to be conducted on the account
- Information that the customer isn't receiving an account statement by mail or email
- Information about unauthorized charges on the account

**Notice from Other Sources.** A customer, a victim of identity theft, a law enforcement authority, or someone else may be trying to tell you that an account has been opened or used fraudulently.

2. Detect Red Flags

Sometimes, using identity verification and authentication methods can help you detect red flags. Consider whether your procedures should differ if an identity verification or authentication is taking place in person, by telephone, mail, or online.

- **New accounts**. When verifying the identity of the person who is opening a new account, reasonable procedures may include getting a name, address, and identification number and, for in-person verification, checking a current government-issued identification card, like a driver's license or passport. Depending on the circumstances, you may want to compare that to information you can find out from other sources, like a credit reporting company or data broker, or the social security Number Death Master File. Asking questions based on information from other sources can be a helpful way to verify someone's identity.
- **Existing accounts**. To detect red flags for existing accounts, your program may include reasonable procedures to confirm the identity of the person you're dealing with, to monitor transactions, and to verify the validity of change-of-address requests. For online authentication, consider the Federal Financial Institutions Examination Council's guidance on authentication as a starting point. It explores the application of multi-factor authentication techniques in high-risk environments, including using passwords, PINs, smart cards, tokens, and biometric identification. Certain types of personal information – like a social security number, date of birth, mother's maiden name, or mailing address – are not reliable authenticators because they're so easily accessible.

You may be using programs to monitor transactions, identify behavior that indicates the possibility of fraud and identity theft, or validate changes of address. If so, incorporate these tools into your program.

3. Prevent and Mitigate Identity Theft

When you spot a red flag, be prepared to respond appropriately. Your response will depend on the degree of risk posed. It may need to accommodate other legal obligations, like laws about providing and terminating service.

The Guidelines in the Red Flags Rule offer examples of some appropriate responses, including:

- Monitoring a covered account for evidence of identity theft
- Contacting the customer
- Changing passwords, security codes, or other ways to access a covered account
- Closing an existing account
- Reopening an account with a new account number
- Not opening a new account
- Not trying to collect on an account or not selling an account to a debt collector
- Notifying law enforcement
- Determining that no response is warranted under the particular circumstances

The facts of a particular case may warrant using one of these options, several of them, or another response altogether. Consider whether any aggravating factors raise the risk of identity theft. For example, a recent breach that resulted in unauthorized access to a customer's account records would call for a stepped-up response because the risk of identity theft rises, too.

4. Update the Program

The Rule recognizes that new red flags emerge as technology changes or identity thieves change their tactics, and requires periodic updates to your program. Factor in your own experience with identity theft; changes in how identity thieves operate; new methods to detect, prevent, and mitigate identity theft; changes in the accounts you offer; and changes in your business, like mergers, acquisitions, alliances, joint ventures, and arrangements with service providers.

## C. ADMINISTERING YOUR PROGRAM

Your Board of Directors – or an appropriate committee of the Board – must approve your initial plan. If you don't have a board, someone in senior management must approve it. The Board may oversee, develop, implement, and administer the program – or it may designate a senior employee to do the job. Responsibilities include assigning specific responsibility for the program's implementation, reviewing staff reports about compliance with the Rule, and approving important changes to your program.

The Rule requires that you train relevant staff only as "necessary." Staff who have taken fraud prevention training may not need to be re-trained. Remember that employees at many levels of your organization can play a key role in identity theft deterrence and detection.

In administering your program, monitor the activities of your service providers. If they're conducting activities covered by the Rule – for example, opening or managing accounts, billing customers, providing customer service, or collecting debts – they must apply the same standards you would if you were performing the tasks yourself. One way to make sure your service providers are taking reasonable steps is to add a provision to your contracts that they have procedures in place to detect red flags and either report them to you or respond appropriately to prevent or mitigate the crime. Other ways to monitor your service providers include giving them a copy of your program, reviewing the red flag policies, or requiring periodic reports about red flags they have detected and their response.

It's likely that service providers offer the same services to a number of client companies. As a result, the Guidelines are flexible about service providers using their own programs as long as they meet the requirements of the Rule.

The person responsible for your program should report at least annually to your Board of Directors or a designated senior manager. The report should evaluate how effective your program has been in addressing the risk of identity theft; how you're monitoring the practices of your service providers; significant incidents of identity theft and your response; and recommendations for major changes to the program.

## CHAPTER 10: TEST YOUR KNOWLEDGE

The following questions are designed to ensure that you have a complete understanding of the information presented in the chapter (assignment). They are included as an additional tool to enhance your learning experience and do not need to be submitted in order to receive CPE credit.

We recommend that you answer each question and then compare your response to the suggested solutions on the following page(s) before answering the final exam questions related to this chapter (assignment).

| | |
|---|---|
| 1. | **Which of the following is the most accurate definition of the "Disposal Rule":**<br>**A.** the rule mandates the disposal of certain sensitive information in consumer reports and protects against unauthorized access<br>**B.** the rule prohibits CPAs from sharing information with their partners<br>**C.** the rule is designed to make it harder on the IRS to conduct audits<br>**D.** the rule is aimed at preventing banks and credit card companies from collecting certain financial data |
| 2. | **Which of the following is true regarding the Disposal Rule:**<br>**A.** it requires businesses to use the "wiping" method of disposal<br>**B.** the Securities and Exchange Commission is responsible for enforcing the Disposal Rule<br>**C.** government agencies and attorneys are exempt from the rule<br>**D.** numerous small entities across almost every industry could potentially be subject to the rule |
| 3. | **What is the first step in complying with the Red Flags Rule:**<br>**A.** identify relevant red flags<br>**B.** detect red flags<br>**C.** prevent and mitigate identity theft<br>**D.** update the program |

# CHAPTER 10: SOLUTIONS AND SUGGESTED RESPONSES

Below are the solutions and suggested responses for the questions on the previous page(s). If you choose an incorrect answer, you should review the pages as indicated for each question to ensure comprehension of the material.

| | |
|---|---|
| **1.** | **A.** CORRECT. The rule is intended to safeguard sensitive information by mandating its disposal in a way that protects unauthorized access.<br><br>**B.** Incorrect. Nothing in the law prevents lawful sharing of information amongst CPAs.<br><br>**C.** Incorrect. The rule has no impact on the IRS.<br><br>**D.** Incorrect. The rule is aimed at safeguarding information after it has been collected, not at preventing its collection.<br><br>*(See page 169 of the course material.)* |
| **2.** | **A.** Incorrect. The rule does not mandate specific disposal measures. Whether "wiping," as opposed to destruction, of electronic media is reasonable, as well as the adequacy of particular utilities to accomplish that "wiping," will depend upon the circumstances.<br><br>**B.** Incorrect. The disposal rule is a part of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), and the Federal Trade Commission (FTC) is responsible for enforcing the disposal rule.<br><br>**C.** Incorrect. The entities covered by the rule include consumer reporting agencies, insurers, landlords, mortgage brokers, automobile dealers, and any other business that possesses or maintains consumer information, including attorneys and government agencies.<br><br>**D.** CORRECT. Any company, regardless of industry or size, that possesses or maintains consumer information for a business purpose will be subject to the rule. Therefore, numerous small entities across almost every industry could potentially be subject to the rule.<br><br>*(See page 170 of the course material.)* |

| | |
|---|---|
| **3.** | **A.** **CORRECT**. The first step in complying with the Red Flags rule is to identify relevant red flags. In doing so, you should consider the risk factors, the sources of red flags, categories of red flags, suspicious documents, personal identity information, and account activity.<br><br>**B.** Incorrect. The second step is to detect red flags. Sometimes, using identity verification and authentication methods can help you detect red flags. Consider whether your procedures should differ if an identity verification or authentication is taking place in person, by telephone, mail, or online.<br><br>**C.** Incorrect. The third step is to prevent and mitigate identity theft. When you spot a red flag, be prepared to respond appropriately. Your response will depend on the degree of risk posed. It may need to accommodate other legal obligations, like laws about providing and terminating service.<br><br>**D.** Incorrect. The last step is to update the program. The Rule recognizes that new red flags emerge as technology changes or identity thieves change their tactics, and requires periodic updates to your program.<br><br>*(See page 178 of the course material.)* |

# APPENDIX: IRS PRIVACY RULES FOR TAX PREPARERS

The Internal Revenue Service passed a measure offering guidance to tax return preparers on the disclosure and use of tax return information. This guidance became effective for the uses of tax return information on or after January 1, 2009. The key principle underlying the proposed guidance is that tax return preparers may not disclose or use tax return information for purposes other than tax return preparation without the knowing, informed, and voluntary consent of the taxpayer.

In addition, the pre-existing regulations under Internal Revenue Code section 7216 were drafted in the early 1970s, prior to the advent of many of the business practices and technology uses that define the electronic preparation and transmission of tax returns by preparers. That section, which is still in effect, provides:

**§ 7216. Disclosure or use of information by preparers of returns**

*(a) General rule. – Any person who is engaged in the business of preparing, or providing services in connection with the preparation of, returns of the tax imposed by chapter 1, or any person who for compensation prepares any such return for any other person, and who knowingly or recklessly –*

> *(1) discloses any information furnished to him for, or in connection with, the preparation of any such return, or*
>
> *(2) uses any such information for any purpose other than to prepare, or assist in preparing, any such return, shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not more than $1,000, or imprisoned not more than 1 year, or both, together with the costs of prosecution.*

*(b) Exceptions. –*

> *(1) Disclosure. – Subsection (a) shall not apply to a disclosure of information if such disclosure is made –*
>
> > *(A) pursuant to any other provision of this title, or*
> >
> > *(B) pursuant to an order of a court.*
>
> *(2) Use. – Subsection (a) shall not apply to the use of information in the preparation of, or in connection with the preparation of, State and local tax returns and declarations of estimated tax of the person to whom the information relates.*
>
> *(3) Regulations. – Subsection (a) shall not apply to a disclosure or use of information which is permitted by regulations prescribed by the Secretary under this section. Such regulations shall permit (subject to such conditions as such regulations shall provide) the disclosure or use of information for quality or peer reviews.*

Another federal statute, section 6103 mandates confidentiality of tax return information by government officials. This voluminous statute governs everything from the circumstances under which the IRS may share information with state tax collecting agencies to how the IRS and other federal agencies must safeguard individual records.

The new IRS regulations broaden the definitions of “tax return preparer” and “tax return information,” revise the manner and form of obtaining taxpayer consent to use or disclose tax return information, and add a requirement to obtain taxpayer consent before preparers send tax return information offshore.

The new regulations also take into account the presence and wide-spread use of computers in tax preparation. If a tax return preparer hires contractors who will need access to tax return information to repair computers or data files, the tax return preparer must notify those contractors that they will also be subject to restrictions on their use or disclosure of tax return information.

**Background**

Internal Revenue Code section 7216 imposes criminal penalties on tax return preparers who make unauthorized disclosures or uses of information furnished to them in connection with the preparation of an income tax return. In addition, tax return preparers are subject to civil penalties under section 6713 for disclosure or use of this information unless an exception under the rules of section 7216(b) applies to the disclosure or use. Section 7216 was enacted by section 316 of the Revenue Act of 1971, Public Law 92-178 (85 Stat. 529, 1971). In 1988, Congress modified the section by limiting the criminal sanction to knowing or reckless unauthorized disclosures. At the same time, Congress enacted the civil penalty that is now found in section 6713. In 1989, Congress further modified section 7216, directing the Treasury Department to issue regulations permitting disclosures of tax return information for quality or peer reviews.

The Treasury Department and the IRS proposed regulations under section 7216 on December 20, 1972 (37 FR 28070). Final regulations were issued on March 29, 1974 (39 FR 11537). These regulations are divided into three parts: section 301.7216- 1 for general provisions and definitions; section 301.7216-2 for disclosures and uses that do not require formal taxpayer consent; and section 301.7216-3 for disclosures and uses that require formal taxpayer consent. Since the regulations were adopted in 1974, the Treasury Department and the IRS have amended §301.7216-2 on occasion, but §§301.7216-1 and 301.7216-3 had remained unchanged until 2009.

The previous regulations were written in a paper-filing era. They did not address current common industry practices, such as electronic preparation or filing of tax returns. The regulations were silent on taxpayers’ consent to the disclosure or use of tax return information in an electronic environment. The new regulations address these issues.

The new regulations also contain other modifications to reflect the principle that taxpayers may provide knowing, informed, and voluntary consent to a tax return preparer’s use of tax return information for purposes other than tax return preparation. While the ability of a tax return preparer to solicit consent from a taxpayer remains limited under certain circumstances, such as when the taxpayer has already rejected a substantially similar request for consent, these regulations allow a tax return preparer to

solicit a taxpayer's consent to use tax return information under certain circumstances that the existing regulations currently prohibit. For example, the new regulations allow tax return preparers to obtain consents to use tax return information for solicitation of services or facilities furnished by any person rather than limiting solicitations to the services or facilities offered by the tax return preparer or member of the tax return preparer's "affiliated group."

The IRS has also published an updated revenue procedure that provides guidance to tax return preparers on the format and content of consents to disclose and consents to use tax return information under §301.7216-3. The revenue procedure also provides specific guidance for electronic signatures when a taxpayer executes an electronic consent to the disclosure or use of the taxpayer's tax return information.

**Amendment to the Regulations**

Accordingly, 26 CFR part 301 is amended as follows:

PART 301 – PROCEDURE AND ADMINISTRATION

Paragraph 1. The authority citation for part 301 continues to read, in part, as follows:

Authority: 26 U.S.C. 7805 * * *

Par. 2. Section 301.7216-0 is added to read as follows:

§301.7216-0 Table of contents.

This section lists captions contained in §§301.7216-1 through 301.7216-3.

§301.7216-1 Penalty for disclosure or use of tax return information.

(a) In general.

(b) Definitions.

(c) Gramm-Leach-Bliley Act.

(d) Effective date.

§301.7216-2 Permissible disclosures or uses without consent of the taxpayer.

(a) Disclosure pursuant to other provisions of Internal Revenue Code.

(b) Disclosures to the IRS.

(c) Disclosures or uses for preparation of a taxpayer's return.

(d) Disclosures to other tax return preparers.

(e) Disclosure or use of information in the case of related taxpayers.

(f) Disclosure pursuant to an order of a court, or an administrative order, a demand, request, summons or subpoena which is issued in the performance of its duties by a Federal or State agency, the United States

Congress, a professional association ethics committee or board, or the Public Company Accounting Oversight Board.

(g) Disclosure for use in securing legal advice, Treasury investigations or court proceedings.

(h) Certain disclosures by attorneys and accountants.

(i) Corporate fiduciaries.

(j) Disclosure to taxpayer's fiduciary.

(k) Disclosure or use of information in preparation or audit of State or local tax returns or assisting a taxpayer with foreign country tax obligations.

(l) Payment of tax preparation services.

(m) Retention of records.

(n) Lists for solicitation of tax return business.

(o) Producing statistical information in connection with tax return preparation business.

(p) Disclosure or use of information for quality or peer reviews.

(q) Disclosure to report the commission of a crime.

(r) Disclosure of tax return information due to a tax return preparer's incapacity or death.

(s) Effective date.

§301.7216-3 Disclosure or use permitted only with the taxpayer's consent.

(a) In general.

(b) Timing requirements and limitations.

(c) Special rules.

(d) Effective date.

Par. 3. Section 301.7216-1 is revised to read as follows:

**§301.7216-1 Penalty for disclosure or use of tax return information.**

(a) In general. Section 7216(a) prescribes a criminal penalty for tax return preparers who knowingly or recklessly disclose or use tax return information for a purpose other than preparing a tax return. A violation of section 7216 is a misdemeanor, with a maximum penalty of up to one year imprisonment or a fine of not more than $1,000, or both, together with the costs of prosecution. Section 7216(b) establishes exceptions to the general rule in section 7216(a) prohibiting disclosure and use. Section 7216(b) also authorizes the Secretary to promulgate regulations prescribing additional permitted disclosures and uses. Section 6713(a) prescribes a related civil penalty for disclosures and uses that constitute a violation of section 7216.

The penalty for violating section 6713 is $250 for each disclosure or use, not to exceed a total of $10,000 for a calendar year. Section 6713(b) provides that the exceptions in section 7216(b) also apply to section 6713. Under section 7216(b), the provisions of section 7216(a) will not apply to any disclosure or use permitted under regulations prescribed by the Secretary.

(b) Definitions. For purposes of section 7216 and §§301.7216-1 through 301.7216-3:

(1) Tax return. The term tax return means any return (or amended return) of income tax imposed by chapter 1 of the Internal Revenue Code.

(2) Tax return preparer –

(i) In general. The term tax return preparer means:

(A) Any person who is engaged in the business of preparing or assisting in preparing tax returns;

(B) Any person who is engaged in the business of providing auxiliary services in connection with the preparation of tax returns, including a person who develops software that is used to prepare or file a tax return and any Authorized IRS e-file Provider;

(C) Any person who is otherwise compensated for preparing, or assisting in preparing, a tax return for any other person; or

(D) Any individual who, as part of their duties of employment with any person described in paragraph (b)(2)(i)(A), (B), or (C) of this section performs services that assist in the preparation of, or assist in providing auxiliary services in connection with the preparation of, a tax return.

(ii) Business of preparing returns. A person is engaged in the business of preparing tax returns as described in paragraph (b)(2)(i)(A) of this section if, in the course of the person's business, the person holds himself out to tax return preparers or taxpayers as a person who prepares tax returns or assists in preparing tax returns, whether or not tax return preparation is the person's sole business activity and whether or not the person charges a fee for tax return preparation services.

(iii) Providing auxiliary services. A person is engaged in the business of providing auxiliary services in connection with the preparation of tax returns as described in paragraph (b)(2)(i)(B) of this section if, in the course of the person's business, the person holds himself out to tax return preparers or to taxpayers as a person who performs auxiliary services, whether or not providing the auxiliary services is the person's sole business activity and whether or not the person charges a fee for the auxiliary services. Likewise, a person is engaged in the business of providing auxiliary services if, in the course of the person's business, the person receives a taxpayer's tax return

information from another tax return preparer pursuant to the provisions of §301.7216-2(d)(2).

(iv) Otherwise compensated. A tax return preparer described in paragraph (b)(2)(i)(C) of this section includes any person who –

(A) Is compensated for preparing a tax return for another person, but not in the course of a business; or

(B) Is compensated for helping, on a casual basis, a relative, friend, or other acquaintance to prepare their tax return.

(v) Exclusions. A person is not a tax return preparer merely because he leases office space to a tax return preparer, furnishes credit to a taxpayer whose tax return is prepared by a tax return preparer, furnishes information to a tax return preparer at the taxpayer's request, furnishes access (free or otherwise) to a separate person's tax return preparation website through a hyperlink on his own website, or otherwise performs some service that only incidentally relates to the preparation of tax returns.

(vi) Examples. The application of §301.7216-1(b)(2) may be illustrated by the following examples:

## Example 1

Bank B is a tax return preparer within the meaning of paragraph (b)(2)(i)(A) of this section, and an Authorized IRS e-file Provider. B employs one individual, Q, to solicit the necessary tax return information for the preparation of a tax return; another individual, R, to prepare the return on the basis of the information that is furnished; a secretary, S, who types the information on the returns into a computer; and an administrative assistant, T, who uses a computer to file electronic versions of the tax returns. Under these circumstances, only R is an income tax return preparer for purposes of section 7701(a)(36), but all four employees are tax return preparers for purposes of section 7216, as provided in paragraph (b) of this section.

## Example 2

Tax return preparer P contracts with department store D to rent space in D's store. D advertises that taxpayers who use P's services may charge the cost of having their tax return prepared to their charge account with D. Under these circumstances, D is not a tax return preparer because it provides space, credit, and services only incidentally related to the preparation of tax returns.

(3) Tax return information –

(i) In general. The term tax return information means any information, including, but not limited to, a taxpayer's name, address, or identifying number, which is furnished in any form or manner for, or in connection with, the preparation of a tax return of the taxpayer. This information includes information that the taxpayer furnishes to a tax return preparer and information furnished the tax return preparer by a third party. Tax return information also includes information the tax return preparer derives or generates from tax return information in connection with the preparation of a taxpayer's return.

(A) Tax return information can be provided directly by the taxpayer or by another person. Likewise, tax return information includes information received by the tax return preparer from the IRS in connection with the processing of such return, including an acknowledgment of acceptance or notice of rejection of an electronically filed return.

(B) Tax return information includes statistical compilations of tax return information, even in a form that cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer. See §301.7216-2(o) for limited use of tax return information to make statistical compilations without taxpayer consent and to use the statistical compilations for limited purposes.

(C) Tax return information does not include information identical to any tax return information that has been furnished to a tax return preparer if the identical information was obtained otherwise than in connection with the preparation of a tax return.

(D) Information is considered "in connection with tax return preparation," and therefore tax return information, if the taxpayer would not have furnished the information to the tax return preparer but for his intention to engage, or the engagement of, the tax return preparer to prepare the tax return.

(ii) Examples. The application of this paragraph (b)(3) may be illustrated by the following examples:

## Example 1

Taxpayer A purchases computer software designed to assist with the preparation and filing of her income tax return. When A loads the software onto her computer, it prompts her to register her purchase of the software. In this situation, the software provider is a tax return preparer under paragraph (b)(2)(i)(B) of this section and the information that A provides to register her purchase is tax return information because she is providing it in connection with the preparation of a tax return.

## Example 2

Corporation A is a brokerage firm that maintains a website through which its clients may access their accounts, trade stocks, and generally conduct a variety of financial activities. Through its website, A offers its clients free access to its own tax preparation software. Taxpayer B is a client of A and has furnished A his name, address, and other information when registering for use of A's website to use A's brokerage services. In addition, A has a record of B's brokerage account activity, including sales of stock, dividends paid, and IRA contributions made. B uses A's tax preparation software to prepare his tax return. The software populates some fields on B's return on the basis of information A already maintains in its databases. A is a tax return preparer within the meaning of paragraph (b)(2)(i)(B) of this section because it has prepared and provided software for use in preparing tax returns. The information in A's databases that the software accesses to populate B's return, i.e., the registration information and brokerage account activity, is not tax return information because A did not receive that information in connection with the preparation of a tax return. Once A uses the information to populate the return, however, the information associated with the return becomes tax return information. If A retains the information in a form in which A can identify that the information was used in connection with the preparation of a return, the information in that form is tax return information. If, however, A retains the information in a database in which A cannot identify whether the information was used in connection with the preparation of a return, then that information is not tax return information.

(4) Use –

(i) In general. Use of tax return information includes any circumstance in which a tax return preparer refers to, or relies upon, tax return information as the basis to take or permit an action.

(ii) Example. The application of this paragraph (b)(4) may be illustrated by the following example:

## Example

Preparer G is a tax return preparer as defined by paragraph (b)(2)(i)(A) of this section. If G determines, upon preparing a return, that the taxpayer is eligible to make a contribution to an individual retirement account (IRA), G will ask whether the taxpayer desires to make a contribution to an IRA. G does not ask about IRAs in cases in which the taxpayer is not eligible to make a contribution. G is using tax return information when it asks whether a taxpayer is interested in making a contribution to an IRA because G is basing the inquiry upon knowledge gained from information that the taxpayer furnished in connection with the preparation of the taxpayer's return.

(5) Disclosure. The term disclosure means the act of making tax return information known to any person in any manner whatever. To the extent that a taxpayer's use of a hyperlink results in the transmission of tax return information, this transmission of tax return information is a disclosure by the tax return preparer subject to penalty under section 7216 if not authorized by regulation.

(6) Hyperlink. For purposes of section 7216, a hyperlink is the device used to transfer an individual using tax preparation software from a tax return preparer's webpage to a webpage operated by another person without the individual having to separately enter the web address of the destination page.

(7) Request for consent. A request for consent includes any effort by a tax return preparer to obtain the taxpayer's consent to use or disclose the taxpayer's tax return information. The act of supplying a taxpayer with a paper or electronic form that meets the requirements of a revenue procedure published pursuant to §301.7216-3(a) is a request for a consent. When a tax return preparer requests a taxpayer's consent, any associated efforts of the tax return preparer, including, but not limited to, verbal or written explanations of the form, are part of the request for consent.

(c) Gramm-Leach-Bliley Act. Any applicable requirements of the Gramm-Leach-Bliley Act, Public Law 106-102 (113 Stat. 1338), do not supersede, alter, or affect the requirements of section 7216 and §§301.7216-1 through 301.7216-3. Similarly, the requirements of section 7216 and §§301.7216-1 through 301.7216-3 do not override any requirements or restrictions of the Gramm-Leach-Bliley Act, which are in addition to the requirements or restrictions of section 7216 and §§301.7216-1 through 301.7216-3.

(d) Effective/applicability date. This section applies to disclosures or uses of tax return information occurring on or after January 1, 2009.

Par. 4. Section 301.7216-2 is revised to read as follows:

**§301.7216-2 Permissible disclosures or uses without consent of the taxpayer.**

(a) Disclosure pursuant to other provisions of Internal Revenue Code. The provisions of section 7216(a) and §301.7216-1 shall not apply to any disclosure of tax return information if the disclosure is made pursuant to any other provision of the Internal Revenue Code or the regulations thereunder.

(b) Disclosures to the IRS. The provisions to section 7216(s) and §301.7216-1 shall not apply to any disclosure of tax return information to an officer or employee of the IRS.

(c) Disclosures or uses for preparation of a taxpayer's return –

(1) Updating Taxpayers' Tax Return Preparation Software. If a tax return preparer provides software to a taxpayer that is used in connection with the preparation or filing of a tax return, the tax return preparer may use the taxpayer's tax return information to update the taxpayer's software for the purpose of addressing changes in IRS forms, e-file specifications and administrative, regulatory and legislative guidance or to test and ensure the software's technical capabilities without the taxpayer's consent under §301.7216-3.

(2) Tax return preparers located within the same firm in the United States. If a taxpayer furnishes tax return information to a tax preparer located within the United States, including any territory or possession of the United States, an officer, employee, or member of a tax return preparer may use the tax return information, or disclose the tax return information to another officer, employee, or member of the same tax return preparer, for the purpose of performing services that assist in the preparation of, or assist in providing auxiliary services in connection with the preparation of, the taxpayer's tax return. If an officer, employee, or member to whom the tax return information is to be disclosed is located outside of the United States or any territory or possession of the United States, the taxpayer's consent under §301.7216-3 prior to any disclosure is required.

(3) Furnishing tax return information to tax return preparers located outside the United States. If a taxpayer initially furnishes tax return information to a tax return preparer located outside of the United States or any territory or possession of the United States, an officer, employee, or member of a tax return preparer may use tax return information, or disclose any tax return information to another officer, employee, or member of the same tax return preparer, for the purpose of performing services that assist in the preparation of, or assist in providing auxiliary services in connection with the preparation of, the tax return of a taxpayer by or for whom the information was furnished without the taxpayer's consent under §301.7216-3.

(4) Examples. The following examples illustrate this paragraph (c):

## Example 1

Preparer P provides tax return preparation software to Taxpayer T for T to use in the preparation of its 2009 income tax return. For the 2009 tax year, and using T's tax return information furnished while registering for the software, P would like to update the tax return preparation software that T is using to account for last minute changes made to the tax laws for the 2009 tax year. P is not required to obtain T's consent to update the tax return preparation software. P may perform a software update regardless of whether the software update will affect T's particular return preparation activities.

## Example 2

T is a client of Firm, which is a tax return preparer. E, an employee at Firm's State A office, receives tax return information from T for use in preparing T's income tax return. E discloses the tax return information to P, an employee in Firm's State B office; P uses the tax return information to process T's income tax return. Firm is not required to receive T's consent under §301.7216-3 prior to E's disclosure of T's tax return information to P, because the tax return information is disclosed to an employee employed by the same tax return preparer located within the United States.

## Example 3

Same facts as Example 2 except T's tax return information is disclosed to FE who is located in Firm's Country F office. FE uses the tax return information to process T's income tax return. After processing, FE returns the processed tax return information to E in Firm's State A office. Because FE is outside of the United States, Firm is required to obtain T's consent under §301.7216-3 prior to E's disclosure of T's tax return information to FE.

## Example 4

T, Firm's client, is temporarily located in Country F. She initially furnishes her tax return information to employee FE in Firm's Country F office for the purpose of having Firm prepare her U.S. income tax return. FE makes the substantive determinations concerning T's tax liability and forwards T's tax return information to FP, an employee in Firm's Country P office, for the purpose of processing T's tax return information. FP processes the return information and forwards it to Partner at Firm's State A office in the United States for review and delivery to T. Because T initially furnished the tax return information to a tax return preparer outside of the United States, T's prior consent for use or disclosure under §301.7216-3 was not required. An officer, employee, or member of Firm in the United States may use T's tax return information or disclose the tax return information to another officer, employee, or member of Firm without T's prior consent under §301.7216-3 as long as any use or disclosure of T's tax return information is within the United States. Firm is required to receive T's consent under §301.7216-3 prior to any subsequent disclosure of T's tax return information to a tax return preparer located outside of the United States.

(d) Disclosures to other tax return preparers –

(1) Preparer-to-preparer disclosures. Except as limited in paragraph (d)(2) of this section, an officer, employee, or member of a tax return preparer may disclose tax return information of a taxpayer to another tax return preparer located in the United States (including any territory or possession of the United States) for the purpose of preparing, or assisting in preparing a tax return, or obtaining or providing auxiliary services in connection with the preparation of any tax return so long as the services provided are not substantive determinations or advice affecting the tax liability reported by taxpayers. A substantive determination involves an analysis, interpretation, or application of the law. The authorized disclosures permitted under this paragraph (d)(1) include one tax return preparer disclosing tax return information to another tax return preparer for the purpose of having the second tax return preparer transfer that information to, and compute the tax liability on, a tax return of the taxpayer by means of electronic, mechanical, or other form of tax return processing service. The authorized disclosures permitted under this paragraph (d)(1) also include disclosures by a tax return preparer to an Authorized IRS e-file Provider for the purpose of electronically filing the return with the IRS. Authorized disclosures also include disclosures by a tax return preparer to a second tax return preparer for the purpose of making information concerning the return available to the taxpayer. This would include, for example, whether the return has been accepted or rejected by the IRS, or the status of the taxpayer's refund. Except as provided in paragraph (c) of this section, a tax return preparer may not disclose tax return information to another tax return preparer for the purpose of the second tax return preparer providing

substantive determinations without first receiving the taxpayer's consent in accordance with the rules under §301.7216-3.

(2) Disclosures to contractors. A tax return preparer may disclose tax return information to a person under contract with the tax return preparer in connection with the programming, maintenance, repair, testing, or procurement of equipment or software used for purposes of tax return preparation only to the extent necessary for the person to provide the contracted services, and only if the tax return preparer ensures that all individuals who are to receive disclosures of tax return information receive a written notice that informs them of the applicability of sections 6713 and 7216 to them and describes the requirements and penalties of sections 6713 and 7216. Contractors receiving tax return information pursuant to this section are tax return preparers under section 7216 because they are performing auxiliary services in connection with tax return preparation. See §301.7216-1(b)(2)(i)(B) and (D).

(3) Examples. The following examples illustrate this paragraph (d):

## Example 1

E, an employee at Firm's State A office, receives tax return information from T for Firm's use in preparing T's income tax return. E makes substantive determinations and forwards the tax return information to P, an employee at Processor; Processor is located in State B. P places the tax return information on the income tax return and furnishes the finished product to E. E is not required to receive T's prior consent under §301.7216-3 before disclosing T's tax return information to P, because Processor's services are not substantive determinations and the tax return information remained in the United States at Processor's State B office during the entire course of the tax return preparation process.

## Example 2

Firm, a tax return preparer, offers income tax return preparation services. Firm's contract with its software provider, Contractor, requires Firm to periodically randomly select certain taxpayers' tax return information solely for the purpose of testing the reliability of the software sold to Firm. Under its agreement with Contractor, Firm discloses tax return information to Contractor's employee, C, who services Firm's contract without providing Contractor or C with a written notice that describes the requirements of and penalties under sections 7216 and 6713. C uses the tax return information solely for quality assurance purposes. Firm's disclosure of tax return information to C was an impermissible disclosure, because Firm failed to ensure that C received a written notice that describes the requirements and penalties of sections 7216 and 6713.

## Example 3

E, an employee of Firm in State A in the United States, receives tax return information from T for use in preparing T's income tax return. After E enters T's tax return information into Firms' computer, that information is stored on a computer server that is physically located in State A. Firm contracts with Contractor, located in Country F, to prepare its clients' tax returns. FE, an employee of Contractor, uses a computer in Country F and inputs a password to view T's income tax information stored on the computer server in State A to prepare T's tax return. A computer program permits FE to view T's tax return information, but prohibits FE from downloading or printing out T's tax return information from the computer server. Because Firm is disclosing T's tax return information outside of the United States, Firm is required to obtain T's consent under §301.7216-3 prior to the disclosure to FE. As provided in §301.7216-3(b)(5), however, Firm may not obtain consent to disclose T's social security number (SSN) to a tax return preparer located outside the United States or any territory or possession of the United States.

## Example 4

A, an employee at Firm A, receives tax return information from T for Firm's use in preparing T's income tax return. A forwards the tax return information to B, an employee at another firm, Firm B, to obtain advice on the issue of whether T may claim a deduction for a certain business expense. A is required to receive T's prior consent under §301.7216-3 before disclosing T's tax return information to B because B's services involve a substantive determination affecting the tax liability that T will report.

(e) Disclosure or use of information in the case of related taxpayers.

(1) In preparing a tax return of a second taxpayer, a tax return preparer may use, and may disclose to the second taxpayer, in the form in which it appears on the return, any tax return information that the tax return preparer obtained from a first taxpayer if –

(i) The second taxpayer is related to the first taxpayer within the meaning of paragraph (e)(2) of this section;

(ii) The first taxpayer's tax interest in the information is not adverse to the second taxpayer's tax interest in the information; and

(iii) The first taxpayer has not expressly prohibited the disclosure or use.

(2) For purposes of paragraph (e)(1) (i) of this section, a taxpayer is related to another taxpayer if they have any one of the following relationships: husband and wife, child and parent, grandchild and grandparent, partner and partnership, trust or estate and

beneficiary, trust or estate and fiduciary, corporation and shareholder, or members of a controlled group of corporations as defined in section 1563.

(3) See §301.7216-3 for disclosure or use of tax return information of the taxpayer in preparing the tax return of a second taxpayer when the requirements of this paragraph are not satisfied.

(f) Disclosure pursuant to an order of a court, or an administrative order, demand, request, summons or subpoena which is issued in the performance of its duties by a Federal or State agency, the United States Congress, a professional association ethics committee or board, or the Public Company Accounting Oversight Board. The provisions of section 7216(a) and §301.7216-1 will not apply to any disclosure of tax return information if the disclosure is made pursuant to any one of the following documents:

(1) The order of any court of record, Federal, State, or local.

(2) A subpoena issued by a grand jury, Federal or State.

(3) A subpoena issued by the United States Congress.

(4) An administrative order, demand, summons or subpoena that is issued in the performance of its duties by –

(i) Any Federal agency as defined in 5 U.S.C. 551(1) and 5 U.S.C. 552(f), or

(ii) A State agency, body, or commission charged under the laws of the State or a political subdivision of the State with the licensing, registration, or regulation of tax return preparers.

(5) A written request from a professional association ethics committee or board investigating the ethical conduct of the tax return preparer.

(6) A written request from the Public Company Accounting Oversight Board in connection with an inspection under section 104 of the Sarbanes-Oxley Act of 2002 (Act), 15 U.S.C. 7214, or an investigation under section 105 of such Act, 15 U.S.C. 7215, for use in accordance with such Act.

(g) Disclosure for use in securing legal advice, Treasury investigations or court proceedings. A tax return preparer may disclose tax return information –

(1) To an attorney for purposes of securing legal advice;

(2) To an employee of the Treasury Department for use in connection with any investigation of the tax return preparer (including investigations relating to the tax return preparer in its capacity as a practitioner) conducted by the IRS or the Treasury Department; or

(3) To any officer of a court for use in connection with proceedings involving the tax return preparer (including proceedings involving the tax return preparer in its capacity as

a practitioner), or the return preparer's client, before the court or before any grand jury that may be convened by the court.

(h) Certain disclosures by attorneys and accountants. The provisions of section 7216(a) and §301.7216-1 shall not apply to any disclosure of tax return information permitted by this paragraph (h).

(1)

(i) A tax return preparer who is lawfully engaged in the practice of law or accountancy and prepares a tax return for a taxpayer may use the taxpayer's tax return information, or disclose the information to another officer, employee or member of the tax return preparer's law or accounting firm, consistent with applicable legal and ethical responsibilities, who may use the tax return information for the purpose of providing other legal or accounting services to the taxpayer. As an example, a lawyer who prepares a tax return for a taxpayer may use the tax return information of the taxpayer for, or in connection with, rendering legal services, including estate planning or administration, or preparation of trial briefs or trust instruments, for the taxpayer or the estate of the taxpayer. In addition, the lawyer who prepared the tax return may disclose the tax return information to another officer, employee or member of the same firm for the purpose of providing other legal services to the taxpayer. As another example, an accountant who prepares a tax return for a taxpayer may use the tax return information, or disclose it to another officer, employee or member of the firm, for use in connection with the preparation of books and records, working papers, or accounting statements or reports for the taxpayer. In the normal course of rendering the legal or accounting services to the taxpayer, the attorney or accountant may make the tax return information available to third parties, including stockholders, management, suppliers, or lenders, consistent with the applicable legal and ethical responsibilities, unless the taxpayer directs otherwise. For rules regarding disclosing outside of the United States, see §301.7216-2(c) and (d).

(ii) A tax return preparer's law or accounting firm does not include any related or affiliated firms. For example, if law firm A is affiliated with law firm B, officers, employees and members of law firm A must receive a taxpayer's consent under §301.7216-3 before disclosing the taxpayer's tax return information to an officer, employee or member of law firm B.

(2) A tax return preparer who is lawfully engaged in the practice of law or accountancy and prepares a tax return for a taxpayer may, consistent with the applicable legal and ethical responsibilities, take the tax return information into account, and may act upon it, in the course of performing legal or accounting services for a client other than the taxpayer, or disclose the information to another officer, employee or member of the tax

return preparer's law or accounting firm to enable that other officer, employee or member to take the information into account, and act upon it, in the course of performing legal or accounting services for a client other than the taxpayer. This is permissible when the information is, or may be, relevant to the subject matter of the legal or accounting services for the other client, and consideration of the information by those performing the services is necessary for the proper performance of the services. In no event, however, may the tax return information be disclosed to a person who is not an officer, employee or member of the law or accounting firm, unless the disclosure is exempt from the application of section 7216(a) and §301.7216-1 by reason of another provision of §§301.7216-2 or 301.7216-3.

(3) Examples. The application of this paragraph may be illustrated by the following examples:

## Example 1

A, a member of an accounting firm, renders an opinion on a financial statement of M Corporation that is part of a registration statement filed with the Securities and Exchange Commission. After the registration statement is filed, but before its effective date, B, a member of the same accounting firm, prepares an income tax return for N Corporation. In the course of preparing N's income tax return, B discovers that N does business with M and concludes that the information given by N should be considered by A to determine whether the financial statement opined on by A contains an untrue statement of material fact or omits a material fact required to keep the statement from being misleading. B discloses to A the tax return information of N for this purpose. A determines that there is an omission of material fact and that an amended statement should be filed. A so advises M and the Securities and Exchange Commission. A explains that the omission was revealed as a result of confidential information that came to A's attention after the statement was filed, but A does not disclose the identity of the taxpayer or the tax return information itself. Section 7216(a) and §301.7216-1 do not apply to B's disclosure of N's tax return information to A and A's use of the information in advising M and the Securities and Exchange Commission of the necessity for filing an amended statement. Section 7216(a) and §301.7216-1 would apply to a disclosure of N's tax return information to M or to the Securities and Exchange Commission unless the disclosure is exempt from the application of section 7216 (a) and §301.7216-1 by reason of another provision of either this section or §301.7216-3.

## Example 2

A, a member of an accounting firm, is conducting an audit of M Corporation, and B, a member of the same accounting firm, prepares an income tax return for D, an officer of M. In the course of preparing the return, B obtains information from D indicating that D, pursuant to an arrangement with a supplier doing business with M, has been receiving from the supplier a percentage of the amounts that the supplier invoices to M. B discloses this information to A who, acting upon it, searches in the course of the audit for indications of a kickback scheme. As a result, A discovers information from audit sources that independently indicate the existence of a kickback scheme. Without revealing the tax return information, A has received from B, A brings to the attention of officers of M the audit information indicating the existence of the kickback scheme. Section 7216(a) and §301.7216-1 do not apply to B's disclosure of D's tax return information to A, A's use of D's information in the course of the audit, and A's disclosure to M of the audit information indicating the existence of the kickback scheme. Section 7216(a) and §301.7216-1 would apply to a disclosure to M, or to any other person not an employee or member of the accounting firm, of D's tax return information furnished to B.

(i) Corporate fiduciaries. A trust company, trust department of a bank, or other corporate fiduciary that prepares a tax return for a taxpayer for whom it renders fiduciary, investment, or other custodial or management services may, unless the taxpayer directs otherwise –

(1) Disclose or use the taxpayer's tax return information in the ordinary course of rendering such services to or for the taxpayer; or

(2) Make the information available to the taxpayer's attorney, accountant, or investment advisor.

(j) Disclosure to taxpayer's fiduciary. If, after furnishing tax return information to a tax return preparer, the taxpayer dies or becomes incompetent, insolvent, or bankrupt, or the taxpayer's assets are placed in conservatorship or receivership, the tax return preparer may disclose the information to the duly appointed fiduciary of the taxpayer or his estate, or to the duly authorized agent of the fiduciary.

(k) Disclosure or use of information in preparation or audit of State or local tax returns or assisting a taxpayer with foreign country tax obligations. The provisions of paragraphs (c) and (d) of this section shall apply to the disclosure by any tax return preparer of any tax return information in the preparation of, or in connection with the preparation of, any tax return of the taxpayer under the law of any State or political subdivision thereof, of the District of Columbia, of any territory or possession of the United States, or of a country other than the United States. The provisions of section 7216(a) and §301.7216-1 shall not apply to the use by any tax return preparer of any tax return information in the preparation of, or in connection with the preparation of, any tax return of the taxpayer under the law of any State or political

subdivision thereof, of the District of Columbia, of any territory or possession of the United States, or of a country other than the United States. The provisions of section 7216(a) and §301.7216-1 shall not apply to the disclosure or use by any tax return preparer of any tax return information in the audit of, or in connection with the audit of, any tax return of the taxpayer under the law of any State or political subdivision thereof, of the District of Columbia, of any territory or possession of the United States.

(l) Payment for tax preparation services. A tax return preparer may use and disclose, without the taxpayer's written consent, tax return information that the taxpayer provides to the tax return preparer to pay for tax preparation services to the extent necessary to process or collect the payment. For example, if the taxpayer gives the tax return preparer a credit card to pay for tax preparation services, the tax return preparer may disclose the taxpayer's name, credit card number, credit card expiration date, and amount due for tax preparation services to the credit card company, as necessary, to process the payment. Any tax return information that the taxpayer did not give the tax return preparer for the purpose of making payment for tax preparation services may not be used or disclosed by the tax return preparer without the taxpayer's prior written consent, unless otherwise permitted under another provision of this section.

(m) Retention of records. A tax return preparer may retain tax return information of a taxpayer, including copies of tax returns, in paper or electronic format, prepared on the basis of the tax return information, and may use the information in connection with the preparation of other tax returns of the taxpayer or in connection with an examination by the Internal Revenue Service of any tax return or subsequent tax litigation relating to the tax return. The provisions of paragraph (n) of this section regarding the transfer of a taxpayer list also apply to the transfer of any records and related papers to which this paragraph applies.

(n) Lists for solicitation of tax return business. A tax return preparer may compile and maintain a separate list containing solely the names, addresses, e-mail addresses, and phone numbers of taxpayers whose tax returns the tax return preparer has prepared or processed. This list may be used by the compiler solely to contact the taxpayers on the list for the purpose of offering tax information or additional tax return preparation services to such taxpayers. The compiler of the list may not transfer the taxpayer list, or any part thereof, to any other person unless the transfer takes place in conjunction with the sale or other disposition of the compiler's tax return preparation business. A person who acquires a taxpayer list, or a part thereof, in conjunction with a sale or other disposition of a tax return preparation business is subject to the provisions of this paragraph with respect to the list. The term list, as used in this paragraph (n), includes any record or system whereby the names and addresses of taxpayers are retained. The provisions of this paragraph (n) also apply to the transfer of any records and related papers to which this paragraph (n) applies.

(o) Producing statistical information in connection with tax return preparation business. A tax return preparer may use, for the limited purpose specified in this paragraph (o), tax return information to produce a statistical compilation of data described in §301.7216-1(b)(3)(i)(B). The purpose and use of the statistical compilation must relate directly to the internal management or support of the tax return preparer's tax return preparation business. The tax return preparer may not disclose or use the tax return information in connection with, or in support of, businesses other than tax return preparation. The compiler of the statistical compilation may not disclose the compilation, or any part thereof, to any

other person unless disclosure of the statistical compilation is made in order to comply with financial accounting or regulatory reporting requirements or occurs in conjunction with the sale or other disposition of the compiler's tax return preparation business. A person who acquires a compilation, or a part thereof, in conjunction with a sale or other disposition of a tax return preparation business is subject to the provisions of this paragraph with respect to the compilation as if the acquiring person had compiled it.

(p) Disclosure or use of information for quality or peer reviews. The provisions of section 7216(a) and §301.7216-1 shall not apply to any disclosure for the purpose of a quality or peer review to the extent necessary to accomplish the review. A quality or peer review is a review that is undertaken to evaluate, monitor, and improve the quality and accuracy of a tax return preparer's tax preparation, accounting, or auditing services. A quality or peer review may be conducted only by attorneys, certified public accountants, enrolled agents, and enrolled actuaries who are eligible to practice before the Internal Revenue Service. See Department of the Treasury Circular 230, 31 CFR part 10. Tax return information may also be disclosed to persons who provide administrative or support services to an individual who is conducting a quality or peer review under this paragraph (p), but only to the extent necessary for the reviewer to conduct the review. Tax return information gathered in conducting a review may be used only for purposes of a review. No tax return information identifying a taxpayer may be disclosed in any evaluative reports or recommendations that may be accessible to any person other than the reviewer or the tax return preparer being reviewed. The tax return preparer being reviewed will maintain a record of the review including the information reviewed and the identity of the persons conducting the review. After completion of the review, no documents containing information that may identify any taxpayer by name or identification number may be retained by a reviewer or by the reviewer's administrative or support personnel. Any person (including administrative and support personnel) receiving tax return information in connection with a quality or peer review is a tax return preparer for purposes of sections 7216(a) and 6713(a).

(q) Disclosure to report the commission of a crime. The provisions of section 7216(a) and §301.7216-1 shall not apply to the disclosure of any tax return information to the proper Federal, State, or local official in order, and to the extent necessary, to inform the official of activities that may constitute, or may have constituted, a violation of any criminal law or to assist the official in investigating or prosecuting a violation of criminal law. A disclosure made in the bona fide but mistaken belief that the activities constituted a violation of criminal law is not subject to section 7216(a) and §301.7216-1.

(r) Disclosure of tax return information due to a tax return preparer's incapacity or death. In the event of incapacity or death of a tax return preparer, disclosure of tax return information may be made for the purpose of assisting the tax return preparer or his legal representative (or the representative of a deceased tax return preparer's estate) in operating the business. Any person receiving tax return information under the provisions of this paragraph (r) is a tax return preparer for purposes of sections 7216(a) and 6713(a).

(s) Effective/applicability date. This section applies to disclosures or uses of tax return information occurring on or after January 1, 2009.

Par. 5. Section 301.7216-3 is revised to read as follows:

**§301.7216-3 Disclosure or use permitted only with the taxpayer's consent.**

(a) In general –

(1) Taxpayer consent. Unless section 7216 or §301.7216-2 specifically authorizes the disclosure or use of tax return information, a tax return preparer may not disclose or use a taxpayer's tax return information prior to obtaining a written consent from the taxpayer, as described in this section. A tax return preparer may disclose or use tax return information as the taxpayer directs as long as the preparer obtains a written consent from the taxpayer as provided in this section. The consent must be knowing and voluntary. Except as provided in paragraph (a)(2) of this section, conditioning the provision of services on the taxpayer's furnishing consent will make the consent involuntary, and the consent will not satisfy the requirements of this section.

(2) Taxpayer consent to a tax return preparer furnishing tax return information to another tax return preparer.

(i) A tax return preparer may condition its provision of preparation services upon a taxpayer's consenting to disclosure of the taxpayer's tax return information to another tax return preparer for the purpose of performing services that assist in the preparation of, or provide auxiliary services in connection with the preparation of, the tax return of the taxpayer.

(ii) Example. The application of this paragraph (a)(2) may be illustrated by the following example:

## Example

Preparer P, who is located within the United States, is retained by Company C to provide tax return preparation services for employees of Company C. An employee of Company C, Employee E, works for C outside of the United States. To provide tax return preparation services for E, P requires the assistance of and needs to disclose E's tax return information to a tax return preparer who works for P's affiliate located in the country where E works. P may condition its provision of tax return preparation services upon E consenting to the disclosure of E's tax return information to the tax return preparer in the country where E works.

(3) The form and contents of taxpayer consents –

(i) In general. All consents to disclose or use tax return information must satisfy the following requirements –

(A) A taxpayer's consent to a tax return preparer's disclosure or use of tax return information must include the name of the tax return preparer and the name of the taxpayer.

(B) If a taxpayer consents to a disclosure of tax return information, the consent must identify the intended purpose of the disclosure. Except as provided in §301.7216-3(a)(3)(iii), if a taxpayer consents to a disclosure of tax return information, the consent must also identify the specific recipient (or recipients) of the tax return information. If the taxpayer consents to use of tax return information, the consent must describe the particular use authorized. For example, if the tax return preparer intends to use tax return information to generate solicitations for products or services other than tax return preparation, the consent must identify each specific type of product or service for which the tax return preparer may solicit use of the tax return information. Examples of products or services that must be identified include, but are not limited to, balance due loans, mortgage loans, mutual funds, individual retirement accounts, and life insurance.

(C) The consent must specify the tax return information to be disclosed or used by the return preparer.

(D) If a tax return preparer to whom the tax return information is to be disclosed is located outside of the United States, the taxpayer's consent under §301.7216-3 prior to any disclosure is required. See §301.7216-2(c) and (d).

(E) A consent to disclose or use tax return information must be signed and dated by the taxpayer.

(ii) The form and contents of taxpayer consents with respect to taxpayers filing a return in the Form 1040 series – guidance describing additional requirements for taxpayer consents with respect to Form 1040 series filers. The Secretary may issue guidance, by publication in the Internal Revenue Bulletin (see §601.601(d)(2)(ii)(b) of this chapter), describing additional requirements for tax return preparers regarding the format and content of consents to disclose and use tax return information with respect to taxpayers filing a return in the Form 1040 series, e.g., Form 1040, Form 1040NR, Form 1040A, or Form 1040EZ.

(iii) The form and contents of taxpayer consents with respect to all other taxpayers. A consent to disclose or use tax return information with respect to a taxpayer not filing a return in the Form 1040 series may be in any format, including an engagement letter to a client, as long as the consent complies with the requirements of §301.7216-3(a)(3)(i). Additionally, the requirements

of §301.7216-3(c)(1) are inapplicable to consents to disclose or use tax return information with respect to taxpayers not filing a return in the Form 1040 series. Solely for purposes of a consent issued under §301.7216-3(a)(3)(iii), in lieu of identifying specific recipients of an intended disclosure under §301.7216-3(a)(3)(i)(B), a consent may allow disclosure to a descriptive class of entities engaged by a taxpayer or the taxpayer's affiliate for purposes of services in connection with the preparation of tax returns, audited financial statements, or other financial statements or financial information as required by a government authority, municipality or regulatory body.

(iv) Examples. The application of §301.7216-3(a)(3)(iii) may be illustrated by the following examples:

## Example 1

Consistent with applicable legal and ethical responsibilities, Preparer Z sends its client, a corporation, Taxpayer C, an engagement letter. Part of the engagement letter requests the consent of Taxpayer C for the purpose of disclosing tax return information to an investment banking firm to assist the investment banking firm in securing long term financing for Taxpayer C. The engagement letter includes language and information that meets the requirements of §301.7216-3(a)(3)(i), including: (I) Preparer Z's name, Taxpayer C's name, and a signature and date line for Taxpayer C; and (Il) a statement that "Taxpayer C authorizes Preparer Z to disclose the portions of Taxpayer C's 2009 tax return information to the firm retained by Taxpayer C necessary for the purposes of assisting Taxpayer C secure long term financing." The engagement letter satisfies the requirements of §301.7216-3(a)(3) for the disclosure of the information provided therein for the specific purpose stated.

## Example 2

Consistent with applicable legal and ethical responsibilities, Preparer N sends its client, a corporation, Taxpayer D, an engagement letter. Part of the engagement letter requests the consent of Taxpayer D for the purpose of disclosing tax return information to Preparer N's affiliated firms located outside of the United States for the purposes of preparation of Taxpayer D's 2009 tax return. The engagement letter includes language and information that meets the requirements of §301.7216-3(a)(3)(i), including: (I) Preparer N's name, Taxpayer D's name, and a signature and date line for Taxpayer D; (II) a statement that "Taxpayer D authorizes Preparer N to disclose Taxpayer D's 2009 tax return information to Preparer N's affiliates located outside of the United States for the purposes of assisting Preparer N prepare Taxpayer D's 2009 tax return"; and (III) a statement that, in providing consent, Taxpayer D acknowledges that its tax return information for 2009 will be disclosed to tax return preparers located abroad. The engagement letter satisfies the requirements of §301.7216-3(a)(3) for the disclosure of the information provided therein for the specific purpose stated.

(b) Timing requirements and limitations –

(1) No retroactive consent. A taxpayer must provide written consent before a tax return preparer discloses or uses the taxpayer's tax return information.

(2) Time limitations on requesting consent in solicitation context. A tax return preparer may not request a taxpayer's consent to disclose or use tax return information for purposes of solicitation of business unrelated to tax return preparation after the tax return preparer provides a completed tax return to the taxpayer for signature.

(3) No request for consent after an unsuccessful request. With regard to tax return information for each income tax return that a tax return preparer prepares, if a taxpayer declines a request for consent to the disclosure or use of tax return information for purposes of solicitation of business unrelated to tax return preparation, the tax return preparer may not solicit from the taxpayer another consent for a purpose substantially similar to that of the rejected request.

(4) No consent to the disclosure of a taxpayer's social security number to a return preparer outside of the United States. A tax return preparer located within the United States, including any territory or possession of the United States, may not obtain consent to disclose the taxpayer's social security number (SSN) to a tax return preparer located outside of the United States or any territory or possession of the United States. Thus, if a tax return preparer located within the United States (including any territory or possession of the United States) obtains consent from a taxpayer to disclose tax return information to another tax return preparer located outside of the United States, as provided under §§301.7216-2(c) and 301.7216-2(d), the tax return preparer located in the United

States may not disclose the taxpayer's SSN, and the tax return preparer must redact or otherwise mask the taxpayer's SSN before the tax return information is disclosed outside of the United States. If a tax return preparer located within the United States initially receives or obtains a taxpayer's SSN from another tax return preparer located outside of the United States, however, the tax return preparer within the United States may, without consent, retransmit the taxpayer's SSN to the tax return preparer located outside the United States that initially provided the SSN to the tax return preparer located within the United States.

(5) Duration of consent. A consent document may specify the duration of the taxpayer's consent to the disclosure or use of tax return information. If a consent agreed to by the taxpayer does not specify the duration of the consent, the consent to the disclosure or use of tax return information will be effective for a period of one year from the date the taxpayer signed the consent.

(c) Special rules –

(1) Multiple disclosures within a single consent form or multiple uses within a single consent form. A taxpayer may consent to multiple uses within the same written document, or multiple disclosures within the same written document. A single written document, however, cannot authorize both uses and disclosures; rather one written document must authorize the uses and another separate written document must authorize the disclosures. Furthermore, a consent that authorizes multiple disclosures or multiple uses must specifically and separately identify each disclosure or use. See §301.7216-3 (a)(3)(iii) for an exception to this rule for certain taxpayers.

(2) Disclosure of entire return. A consent may authorize the disclosure of all information contained within a return. A consent authorizing the disclosure of an entire return must provide that the taxpayer has the ability to request a more limited disclosure of tax return information as the taxpayer may direct.

(3) Copy of consent must be provided to taxpayer. The tax return preparer must provide a copy of the executed consent to the taxpayer at the time of execution. The requirements of this paragraph (c)(3) may also be satisfied by giving the taxpayer the opportunity, at the time of executing the consent, to print the completed consent or save it in electronic form.

(d) Effective /applicability date. This section applies to disclosures or uses of tax return information occurring on or after January 1, 2009.

**(REVENUE PROCEDURE 26 CFR Part 301)**

**SECTION 1. PURPOSE**

This revenue procedure provides guidance to tax return preparers regarding the format and content of consents to disclose and consents to use tax return information with respect to taxpayers filing a return

in the Form 1040 series, e.g., Form 1040, Form 1040NR, Form 1040A, or Form 1040EZ, under section 301.7216-3 of the Regulations on Procedure and Administration (26 CFR Part 301). This revenue procedure also provides specific requirements for electronic signatures when a taxpayer executes an electronic consent to the disclosure or use of the taxpayer's tax return information. This revenue procedure modifies and supersedes Revenue Procedure 2008-12, 2008-5 I.R.B. 368, to provide guidance pursuant to section 301.7216-3T(b)(4)(ii).

## SECTION 2. BACKGROUND

.01 In general, section 7216(a) of the Internal Revenue Code imposes criminal penalties on tax return preparers who knowingly or recklessly make unauthorized disclosures or uses of information furnished in connection with the preparation of an income tax return. A violation of section 7216 is a misdemeanor, with a maximum penalty of up to one year imprisonment or a fine of not more than $1,000, or both, together with the costs of prosecution. Section 7216(b) establishes exceptions to the general rule in section 7216(a) and also authorizes the Secretary to promulgate regulations prescribing additional permitted disclosures and uses.

.02 Section 6713(a) prescribes a related civil penalty for unauthorized disclosures or uses of information furnished in connection with the preparation of an income tax return. The penalty for violating section 6713 is $250 for each disclosure or use, not to exceed a total of $10,000 for a calendar year. Section 6713(b) provides that the exceptions in section 7216(b) also apply to section 6713.

.03 Section 301.7216-3 provides that, unless section 7216 or §301.7216-2 specifically permits the disclosure or use of tax return information, a tax return preparer may not disclose or use a taxpayer's tax return information prior to obtaining a consent from the taxpayer. Section 301.7216-3(a) provides that consent must be knowing and voluntary. Section 301.7216-3(a)(3)(i) prescribes the form and content requirements that all consents to disclose or use must include. Sections 301.7216-3(b) and 301.7216-3T(b) provide timing requirements and other limitations upon consents to disclose or use tax return information. Section 301.7216-3T(b)(4) provides a limitation upon consents to disclose a taxpayer's social security number to a tax return preparer located outside of the United States.

.04 Section 301.7216-3(a)(3)(ii) provides that the Secretary may, by publication in the Internal Revenue Bulletin, prescribe additional requirements for tax return preparers regarding the format and content of consents to disclose and consents to use tax return information with respect to taxpayers filing a return in the Form 1040 series, as well as the requirements for a valid signature on an electronic consent under section 7216. Section 301.7216-3T(b)(4)(ii) provides that the Secretary may, by publication in the Internal Revenue Bulletin, describe the requirements of an "adequate data protection safeguard" for purposes of removing the limitation upon consents to disclose a taxpayer's social security number to a tax return preparer located outside of the United States. This revenue procedure provides additional consent format and content requirements and defines an "adequate data protection safeguard."

## SECTION 3. SCOPE

This revenue procedure applies to all tax return preparers, as defined in §301.7216-1(b)(2), who seek consent to disclose or use tax return information pursuant to §§301.7216-3 and 301.7216-3T with

respect to taxpayers who file a return in the Form 1040 series, e.g., Form 1040, Form 1040NR, Form 1040A, or Form 1040EZ.

## SECTION 4. FORM AND CONTENT OF A CONSENT TO DISCLOSE OR A CONSENT TO USE FORM 1040 TAX RETURN INFORMATION

.01 Separate Written Document. Except as provided by §301.7216-3(c)(1) (special rule for multiple disclosures or uses within a single consent form), and described in section 4.05, below, a taxpayer's consent to each separate disclosure or use of tax return information must be contained on a separate written document, which can be furnished on paper or electronically. For example, the separate written document may be provided as an attachment to an engagement letter furnished to the taxpayer.

.02 A consent furnished to the taxpayer on paper must be provided on one or more sheets of 8½ inch by 11 inch or larger paper. All of the text on each sheet of paper must pertain solely to the disclosure or use the consent authorizes, and the sheet or sheets, together, must contain all the elements described in section 4.04 and, if applicable, comply with section 4.06. All of the text on each sheet of paper must also be in at least 12-point type (no more than 12 characters per inch).

.03 An electronic consent must be provided on one or more computer screens. All of the text placed by the preparer on each screen must pertain solely to the disclosure or use of tax return information authorized by the consent, except for computer navigation tools. The text of the consent must meet the following specifications: the size of the text must be at least the same size as, or larger than, the normal or standard body text used by the website or software package for direction, communications or instructions and there must be sufficient contrast between the text and background colors. In addition, each screen or, together, the screens must—

(1) Contain all the elements described in section 4.04 and, if applicable, comply with section 4.06,

(2) Be able to be signed as required by section 5 and dated by the taxpayer,

(3) Be able to be formatted in a readable and printer-friendly manner.

.04 Requirements for Every Consent. In addition to the requirements provided in §301.7216-3, consents to disclose or use Form 1040 series tax return information must satisfy the following requirements—

(1) Mandatory statements in the consent. The following statements must be included in a consent under the circumstances described below, except that a tax return preparer may substitute the preparer's name where "we" or "our" is used.

(a) Consent to disclose tax return information in context other than tax preparation or auxiliary services. Unless a tax return preparer is obtaining a taxpayer's consent to disclose the taxpayer's tax return information to another tax return preparer for the purpose of performing services that assist in the preparation of, or provide auxiliary services (as defined in §301.7216-1(b)(2)(ii)) in connection with the preparation of, the tax return of the taxpayer,

any consent to disclose tax return information must contain the following statements in the following sequence:

Federal law requires this consent form be provided to you. Unless authorized by law, we cannot disclose, without your consent, your tax return information to third parties for purposes other than the preparation and filing of your tax return. If you consent to the disclosure of your tax return information, Federal law may not protect your tax return information from further use or distribution.

You are not required to complete this form. If we obtain your signature on this form by conditioning our services on your consent, your consent will not be valid. If you agree to the disclosure of your tax return information, your consent is valid for the amount of time that you specify. If you do not specify the duration of your consent, your consent is valid for one year.

(b) Consent to disclose tax return information in tax preparation or auxiliary services context. If a tax return preparer is otherwise required to obtain a taxpayer's consent to disclose the taxpayer's tax return information to another tax return preparer for the purpose of performing services that assist in the preparation of, or provide auxiliary services (as defined in §301.7216-1(b)(2)(ii)) in connection with the preparation of, the tax return of the taxpayer, any consent to disclose tax return information must contain the following statements in the following sequence:

Federal law requires this consent form be provided to you. Unless authorized by law, we cannot disclose, without your consent, your tax return information to third parties for purposes other than the preparation and filing of your tax return and, in certain limited circumstances, for purposes involving tax return preparation. If you consent to the disclosure of your tax return information, Federal law may not protect your tax return information from further use or distribution.

You are not required to complete this form. Because our ability to disclose your tax return information to another tax return preparer affects the service that we provide to you and its cost, we may decline to provide you with service or change the terms of service that we provide to you if you do not sign this form. If you agree to the disclosure of your tax return information, your consent is valid for the amount of time that you specify. If you do not specify the duration of your consent, your consent is valid for one year.

(c) Consent to use. All consents to use tax return information must contain the following statements in the following sequence:

Federal law requires this consent form be provided to you. Unless authorized by law, we cannot use, without your consent, your tax return information for purposes other than the preparation and filing of your tax return.

You are not required to complete this form. If we obtain your signature on this form by conditioning our services on your consent, your consent will not be valid. Your consent is valid for the amount of time that you specify. If you do not specify the duration of your consent, your consent is valid for one year.

(d) All consents must contain the following statement:

If you believe your tax return information has been disclosed or used improperly in a manner unauthorized by law or without your permission, you may contact the Treasury Inspector General for Tax Administration (TIGTA) by telephone at 1-800-366-4484, or by email at complaints@tigta.treas.gov.

(e) Mandatory statement in any consent to disclose tax return information to a tax return preparer located outside of the United States. If a tax return preparer to whom the tax return information is to be disclosed is located outside of the United States, the taxpayer's consent under §301.7216-3 prior to any disclosure is required. See §§ 301.7216-3(a)(3)(i)(D), 301.7216-2(c) and (d).

> (i) If the tax return information to be disclosed does not include the taxpayer's social security number, or if the social security number is fully masked or otherwise redacted, consents for disclosure of tax return information to a tax return preparer outside of the United States must contain the following statement:
>
> This consent to disclose may result in your tax return information being disclosed to a tax return preparer located outside the United States.
>
> (ii) If the tax return information to be disclosed includes the taxpayer's social security number, or if the social security number is not fully masked or otherwise redacted, pursuant to the limitations of §301.7216-3T(b)(4) and section 4.07, consents for disclosure of the taxpayer's tax return information including a social security number to a tax return preparer outside of the United States must contain the following statement:
>
> This consent to disclose may result in your tax return information being disclosed to a tax return preparer located outside the United States, including your personally identifiable information such as your Social Security Number ("SSN"). Both the tax return preparer in the United States that will disclose your SSN and the tax return preparer located outside the United States which will receive your SSN maintain an

adequate data protection safeguard (as required by the regulations under 26 U.S.C. Section 7216) to protect privacy and prevent unauthorized access of tax return information. If you consent to the disclosure of your tax return information, Federal agencies may not be able to enforce US laws that protect the privacy of your tax return information against a tax return preparer located outside of the US to which the information is disclosed.

(2) Affirmative consent. All consents must require the taxpayer's affirmative consent to a tax return preparer's disclosure or use of tax return information. A consent that requires the taxpayer to remove or "deselect" disclosures or uses that the taxpayer does not wish to be made, i.e., an "opt-out" consent, is not permitted.

(3) Signature. All consents to disclose or use tax return information must be signed by the taxpayer.

(a) For consents on paper, the taxpayer's consent to a disclosure or use must contain the taxpayer's signature.

(b) For electronic consents, a taxpayer must sign the consent by any method prescribed in section 5, below.

(4) Incomplete consents. A tax return preparer shall not present a consent form with blank spaces related to the purpose of the consent to the taxpayer for signature.

.05 Special rule for multiple disclosures within a single consent form or multiple uses within a single consent form. Section 301.7216-3(c)(1) provides that a taxpayer may consent to multiple uses within the same written document, or multiple disclosures within the same written document. Multiple disclosure consents and multiple use consents must provide the taxpayer with the opportunity, within the separate written document, to affirmatively select each separate disclosure or use. Further, the taxpayer must be provided the information in section 4.04 for each separate disclosure or use. The mandatory statements required in section 4.04(1) relating to use or disclosure need only be stated once in a multiple disclosure or multiple use consent.

.06 Disclosure of entire return. If, under §301.7216-3(c)(2), a consent authorizes the disclosure of a copy of the taxpayer's entire tax return or all information contained within a return, the consent must provide that the taxpayer has the ability to request a more limited disclosure of tax return information as the taxpayer may direct.

.07 Adequate data protection safeguard. Pursuant to §301.7216-3T(b)(4), a tax return preparer located within the United States, including any territory or possession of the United States, may disclose a taxpayer's SSN to a tax return preparer located outside of the United States or any territory or possession of the United States with the taxpayer's consent only when both the tax return preparer located within the United States and the tax return preparer located outside of the United States maintain an adequate data protection safeguard at the time the taxpayer's consent is obtained and when making the disclosure. An "adequate data protection safeguard" is a security program, policy and practice that has been approved

by management and implemented that includes administrative, technical and physical safeguards to protect tax return information from misuse or unauthorized access or disclosure and that meets or conforms to one of the following privacy or data security frameworks:

(1) The United States Department of Commerce "safe harbor" framework for data protection (or successor program);

(2) A foreign law data protection safeguard that includes a security component, e.g., the European Commission's Directive on Data Protection;

(3) A framework that complies with the requirements of a financial or similar industry-specific standard that is generally accepted as best practices for technology and security related to that industry, e.g., the BITS (Financial Services Roundtable) Financial Institution Shared Assessment Program;

(4) The requirements of the AICPA/CICA Privacy Framework;

(5) The requirements of the most recent version of IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities; or

(6) Any other data security framework that provides the same level of privacy protection as contemplated by one or more of the frameworks described in (1) through (5).

## SECTION 5. ELECTRONIC SIGNATURES

.01 If a taxpayer furnishes consent to disclose or use tax return information electronically, the taxpayer must furnish the tax return preparer with an electronic signature that will verify that the taxpayer consented to the disclosure or use. The regulations under §301.7216-3(a) require that the consent be knowing and voluntary. Therefore, for an electronic consent to be valid, it must be furnished in a manner that ensures affirmative, knowing consent to each disclosure or use.

.02 A tax return preparer seeking to obtain a taxpayer's consent to the disclosure or use of tax return information electronically must obtain the taxpayer's signature on the consent in one of the following manners:

(a) Assign a personal identification number (PIN) that is at least 5 characters long to the taxpayer. To consent to the disclosure or use of the taxpayer's tax return information, the taxpayer may type in the pre-assigned PIN as the taxpayer's signature authorizing the disclosure or use. A PIN may not be automatically furnished by the software so that the taxpayer only has to click a button for consent to be furnished. The taxpayer must affirmatively enter the PIN for the electronic signature to be valid;

(b) Have the taxpayer type in the taxpayer's name and then hit "enter" to authorize the consent. The software must not automatically furnish the taxpayer's name so that the taxpayer only has to click a button to consent. The taxpayer must affirmatively type the taxpayer's name for the electronic consent to be valid; or

(c) Any other manner in which the taxpayer affirmatively enters 5 or more characters that are unique to that taxpayer that are used by the tax return preparer to verify the taxpayer's identity. For example, entry of a response to a question regarding a shared secret could be the type of information by which the taxpayer authorizes disclosure or use of tax return information.

## SECTION 6. EXAMPLES

.01 The application of this revenue procedure is illustrated by the following examples:

(1) Example 1. Preparer P offers tax preparation services over the Internet. P wishes to use information the taxpayer provides during tax preparation of the taxpayer's Form 1040 to generate targeted banner advertisements (i.e., electronic advertisements appearing on the computer screen based on the taxpayer's tax return information). In the course of advertising services and products, P wishes also to disclose to other third parties information that the taxpayer provides.

(a) P posts, in pertinent part, the following consent on the computer screen for taxpayers to indicate approval. If a taxpayer does not indicate approval, the tax return preparation software does not permit the taxpayer to use the software.

**PRIVACY STATEMENT**

Your privacy is very important to us at P. We are providing this statement to inform you about the types of information we collect from you, and how we may disclose or use that information in connection with the services we provide. This Privacy Statement describes the privacy practices of our company as required by applicable laws. . . . During the course of providing our services to you, we may offer you various other services that may be of interest to you based on our determination of your needs through analysis of your data. Your use of the services we offer constitutes a consent to our disclosure of tax information to the service providers. If at any time you wish to limit your receipt of promotional offers based upon information you provide, you may call us at the following. . . .

(b) Beneath this Privacy Statement, the following acknowledgment line appears next to two button images stating "yes" and "no:"

"I have read the Privacy Statement and agree to it by clicking here."

(c) If the taxpayer clicks "no," a message appears on the screen informing the taxpayer that tax return preparation will not proceed without the taxpayer agreeing to the company's Privacy Statement.

(d) P has failed to comply with the requirements of §301.7216-3 and this revenue procedure. P has attempted to obtain consent from the taxpayer by making the use of the program contingent on the taxpayer's consent to P's disclosure and use of the taxpayer's tax return information for purposes other than tax preparation (e.g., for use in displaying targeted banner advertisement). Thus, the consent is not voluntary, as required by §301.7216-3(a). P has also failed to identify the tax return information that it will disclose or use, as required by §301.7216-3(a)(3)(C), to identify the purposes of the disclosures and uses, as required by section §301.7216-3(a)(3)(B), and to the extent that P intends to disclose the entire return based on the consent, P's consent has not provided that the taxpayer has the ability to request a more limited disclosure of tax return information as the taxpayer may direct as required by section 4.06. The single document attempts to have the taxpayer consent to both disclosures and uses, in violation of section 4.05. P has not used the mandatory statements required by section 4.04(1). The consent is not signed by the taxpayer because P has not provided a means for the taxpayer to electronically sign the consent in a form authorized by section 5. Finally, the consent is not dated as required by section 4.03(2).

(2) Example 2. Preparer Q offers tax preparation services over the Internet and wishes to use targeted banner advertisements during tax return preparation. Q contracts with Bank A regarding the advertisement of Individual Retirement Accounts (IRAs). Preparer Q displays advertisements to the taxpayer only if the taxpayer's tax return information indicates that the services are relevant to the taxpayer (i.e., they are targeted banner advertisements). A taxpayer using Q's software must enter a password to begin the process of preparing a return.

(a) Before the taxpayer starts providing tax return information, the following screen appears on Q's tax preparation program.

**CONSENT TO USE OF TAX RETURN INFORMATION**

Federal law requires this consent form be provided to you. Unless authorized by law, we cannot use, without your consent, your tax return information for purposes other than the preparation and filing of your tax return.

You are not required to complete this form. If we obtain your signature on this form by conditioning our services on your consent, your consent will not be valid. Your consent is valid for the amount of time that you specify. If you do not specify the duration of your consent, your consent is valid for one year.

For your convenience, Q has entered into arrangements with certain banks regarding the provision of Individual Retirement Accounts (IRAs). To determine whether this service may be of interest to you, Q will need to use your tax return information.

If you would like Q to use your tax return information to determine whether this service is relevant to you while we are preparing your return, please check the corresponding box if you are interested, provide the information requested below, and sign and date this consent to the use of your tax return information.

I, [INSERT NAME] authorize Q to use the information I provide to Q during the preparation of my tax return for 2006 to determine whether to offer me an opportunity to invest in an IRA.

Signature: [INSERT SIGNATURE AS PRESCRIBED UNDER SECTION 5]

Date: [INSERT DATE]

If you believe your tax return information has been disclosed or used improperly in a manner unauthorized by law or without your permission, you may contact the Treasury Inspector General for Tax Administration (TIGTA) by telephone at 1-800-366-4484, or by email at complaints@tigta.treas.gov.

(b) If the taxpayer selects the consent above, the taxpayer is directed to print the screen. Later, after the taxpayer has entered data to prepare his or her 2006 tax return, the following screen is displayed:

**CONSENT TO DISCLOSURE OF TAX RETURN INFORMATION**

Federal law requires this consent form be provided to you. Unless authorized by law, we cannot disclose, without your consent, your tax return information to third parties for purposes other than the preparation and filing of your tax return. If you consent to the disclosure of your tax return information, Federal law may not protect your tax return information from further use or distribution.

You are not required to complete this form. If we obtain your signature on this form by conditioning our services on your consent, your consent will not be valid. If you agree to the disclosure of your tax return information, your consent is valid for the amount of time that you specify. If you do not specify the duration of your consent, your consent is valid for one year.

You have indicated that you are interested in obtaining information on IRAs. To provide you with this information, Q must forward your tax return information, as indicated below, to the bank that provides this service.

If you would like Q to disclose your tax return information to the bank providing this service, please check the corresponding box for the service in which you are interested, provide the information requested below, and sign and date your consent to the disclosure of your tax return information.

I, [INSERT NAME], authorize Q to disclose to Bank A that portion of my tax return information for 2006 that is necessary for Bank A to contact me and provide information on obtaining an IRA or altering my contribution to an IRA for 2006.

Signature: [INSERT SIGNATURE AS PRESCRIBED UNDER SECTION 5]

Date: [INSERT DATE]

If you believe your tax return information has been disclosed or used improperly in a manner unauthorized by law or without your permission, you may contact the Treasury Inspector General for Tax Administration (TIGTA) by telephone at 1-800-366-4484, or by email at complaints@tigta.treas.gov.

If the taxpayer consents to the disclosure of the tax return information using the screen above, the taxpayer is directed to print the screen. Q will then transmit only that portion of the taxpayer's tax return information for 2006 that is necessary for the bank authorized in the consent, Bank A, to provide the service.

(c) These two consent documents, above, satisfy the requirements of §301.7216-3(c) and this revenue procedure for the disclosure or use of the information provided therein for the specific purposes stated.

(3) Example 3. Large corporation C employs 200 expatriated employees who work in Belgium. Preparer R, located in the United States, prepares individual income tax returns for C's expatriated workers pursuant to a corporate plan for executive tax return preparation. Preparer R is affiliated with Preparer F, located in Belgium. Pursuant to the corporate plan for executive tax return preparation, Preparer R plans to provide the expatriated employee's tax return information, including the expatriated employee's SSNs, located on Preparer R's US based data servers to Preparer F who then plans to meet with the expatriated employees to prepare those employees' 2008 individual income tax returns. Preparer R obtains information electronically from various sources

in anticipation of providing the information to Preparer F. Preparer R developed, adopted and incorporated into its operations a data privacy program which meets the requirements of the AICPA/CICA Privacy Framework. Preparer F also developed, adopted and incorporated into its operations a data privacy program and Preparer F's data privacy program is subject to the European Commission's Directive on Data Protection. The data privacy programs adopted by Preparer R and Preparer F are in operation at the time all consents to disclose are obtained by Preparer R and disclosures are made by Preparer R to Preparer F.

(a) Before transmitting or sending any expatriated employee's SSN to Preparer F, Preparer R provides the expatriated employee (taxpayer) with the following document.

**CONSENT TO DISCLOSURE OF TAX RETURN INFORMATION**

Federal law requires this consent form be provided to you. Unless authorized by law, we cannot disclose, without your consent, your tax return information to third parties for purposes other than the preparation and filing of your tax return and, in certain limited circumstances, for purposes involving tax return preparation. If you consent to the disclosure of your tax return information, Federal law may not protect your tax return information from further use or distribution.

You are not required to complete this form. Because our ability to disclose your tax return information to another tax return preparer affects the service that we provide to you and its cost, we may decline to provide you with service or change the terms of service that we provide to you if you do not sign this form. If you agree to the disclosure of your tax return information, your consent is valid for the amount of time that you specify. If you do not specify the duration of your consent, your consent is valid for one year.

This consent to disclose may result in your tax return information being disclosed to a tax return preparer located outside the United States, including your personally identifiable information such as your Social Security Number ("SSN"). Both the tax return preparer in the United States that will disclose your SSN and the tax return preparer located outside the United States which will receive your SSN maintain an adequate data protection safeguard (as required by the regulations under 26 U.S.C. Section 7216) to protect privacy and prevent unauthorized access of tax return information. If you consent to the disclosure of your tax return information, Federal agencies may not be able to enforce US laws that protect the privacy of your tax return information against a tax return preparer located outside of the US to which the information is disclosed.

If you agree to allow Preparer R to disclose your tax return information, including your SSN, to Preparer F for purposes of providing assistance in the preparation of your 2008 individual income tax return, please check the box below, provide the information requested below, and sign and date your consent to the disclosure of your tax return information.

I, [INSERT NAME], authorize Preparer R to disclose to Preparer F my tax return information including my SSN to allow Preparer F to assist in the preparation of my 2008 individual income tax return.

Signature:

Date: [INSERT DATE]

If you believe your tax return information has been disclosed or used improperly in a manner unauthorized by law or without your permission, you may contact the Treasury Inspector General for Tax Administration (TIGTA) by telephone at 1-800-366-4484, or by email at complaints@tigta.treas.gov.

The taxpayer provides consent by checking the box and signing and dating the consent form. Preparer R then provides a copy of the signed and dated consent form to the taxpayer, and then transmits the taxpayer's tax return information to Preparer F for processing of taxpayer's 2008 individual income tax return.

(b) The consent above satisfies the requirements of 301.7216-3, 301.7216-3T and this revenue procedure for the disclosure of the information provided therein for the specific purpose stated.

## SECTION 7. EFFECT ON OTHER DOCUMENTS

.01 Rev. Proc. 2008-12, 2008-5 I.R.B. 368, is modified and superseded.

## SECTION 8. EFFECTIVE DATE

This revenue procedure is effective on January 1, 2009.

## SECTION 9. DRAFTING INFORMATION

The principal author of this revenue procedure is Lawrence Mack of the Office of Associate Chief Counsel (Procedure & Administration). For further information regarding this revenue procedure contact Lawrence Mack at (202) 622-4940 (not a toll free call).

# GLOSSARY

**Active Duty Fraud Alerts –** Members of the military who are away from their usual duty station may place an active duty alert on their credit reports by contacting any one of the three major consumer-reporting companies. Active duty alerts can help minimize the risk of identity theft while an individual is deployed.

**Consumer –** For purposes of the Gramm-Leach-Bliley Act, a "consumer" is an individual who obtains or has obtained a financial product or service from a financial institution for personal, family or household reasons.

**Customer –** For purposes of the Gramm-Leach-Bliley Act, a "customer" is a consumer with a continuing relationship with a financial institution. Generally, if the relationship between the financial institution and the individual is significant and/or long-term, the individual is a customer of the institution.

**Disposal Rule –** The disposal rule is a part of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which calls for the proper disposal of information in consumer reports and records to protect against "unauthorized access to or use of the information."

**"E" Money –** An electronic payment system – sometimes referred to as "electronic money" – which is becoming common. Their goal is to make purchasing simpler. For example, "stored-value" cards let you transfer cash value to a card. They are commonly used for public transportation, at colleges and universities, at gas stations, and for prepaid telephone use.

**Fair Credit Reporting Act –** Federal law which establishes procedures for correcting fraudulent information on an individual's credit report and requires that their report be made available only for certain legitimate business needs.

**Fair Debt Collection Practices Act –** Federal law that prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection, even if those bills do not result from identity theft.

**Federal Trade Commission –** The federal agency charged with investigating complaints of identity theft, preparing materials for public education on the subject and maintaining a data base of reported incidents, among other responsibilities.

**Financial Institution –** For purposes of the Gramm-Leach-Bliley Act, companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance.

**Fraud Alert –** A "red flag" that individuals who fear they have been victimized by identity theft – or who know they have – can place on their consumer credit reports to help prevent identity thieves from obtaining credit under the victim's name.

**Freedom of Information Act –** This federal law establishes a presumption that records in the possession of agencies and departments of the executive branch of the federal government are accessible to the people.

**Gramm-Leach-Bliley Act –** Enacted in 1999, this federal law prohibits the making of false or fraudulent statements or representations to an officer, employee or agent of a financial institution, or to a customer of a financial institution, in order to obtain consumer information. The Act also prohibits anyone from requesting a person to obtain customer information of a financial institution, knowing that the person will use fraudulent methods to obtain information from the institution. The Act also imposes criminal sanctions for knowing and intentional violations of these provisions.

**Identity Theft and Assumption Deterrence Act –** This Act enacted by Congress in October 1998 (and codified, in part, at 18 U.S.C. §1028) made identity theft a federal crime for the first time.

**Non-Public Personal Information (NPI) –** For purposes of the Gramm-Leach-Bliley Act, NPI is any "personally identifiable financial information" that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise "publicly available."

**Phishing –** A general term for criminals' creation and use of e-mails and websites – designed to look like e-mails and websites of well-known legitimate businesses, financial institutions, and government agencies – in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords. The "phishers" then take that information and use it for criminal purposes, such as identity theft and fraud.

**Pretexing –** The practice of getting an individual's personal information under false pretenses. Pretexters typically sell this information to people who may use it to obtain credit under the victim's name, steal assets or even sue the victim of pretexting. Pretexting is a violation of federal law.

**Privacy Act of 1974 –** This Act regulates federal government agencies' collection, maintenance, use and disclosure of personal information maintained by agencies in a system of records. The Act prohibits the disclosure of any record contained in a system of records unless the disclosure is made on the basis of a written request or prior written consent of the person to whom the records pertain, or is otherwise authorized by law.

**Red Flags Rule –** The Red Flags Rule was created by the Federal Trade Commission (FTC), along with other government agencies such as the National Credit Union Administration (NCUA), to help prevent identity theft. It sets out how certain businesses and organizations must develop, implement, and administer their Identity Theft Prevention Programs.

**Safeguards Rule –** Federal law that requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions "such as credit reporting agencies" that receive customer information from other financial institutions.

**Skimming –** The practice of stealing a victim's credit or debit card numbers by capturing the information in a data storage device.

**Smishing –** The texting equivalent to phishing. Smishing is the act of attempting to acquire personal information such as passwords and credit card details by masquerading as a trustworthy entity by sending consumers text messages containing a link to a fraudulent website or a phone number in an attempt to collect personal information.

**Social Security Act Amendments of 1990 –** A provision of the social security Act that bars disclosure by federal, state and local governments of social security numbers collected pursuant to laws enacted on or after October 1, 1990.

**Vishing –** The telephone equivalent of phishing. Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

# INDEX

# THE BASICS OF IDENTITY THEFT (COURSE #7050D) – FINAL EXAM COPY

**The following exam will not be graded. It is attached only for your convenience while you read the course text. To access the exam to be submitted for grading, go to your account and select Take Exam.**

1. **According to research, what are the two most common reasons offenders turn to identity theft:**

   **A.** boredom and a desire to get caught
   **B.** financial gain and concealment
   **C.** loss of a job and being in debt
   **D.** pressure from others and fear of government

2. **When did identity theft become a federal crime:**

   **A.** 1933
   **B.** 1968
   **C.** 1998
   **D.** 2010

3. **Other than financial loss, what is the most common harm reported by victims of identity theft:**

   **A.** job loss
   **B.** damage to their credit report
   **C.** loss of their home
   **D.** harassing calls from bill collectors

4. **How often is each nationwide consumer reporting company required to provide individuals with a free copy of their credit report:**

   **A.** upon request, once every month
   **B.** upon request, once every quarter
   **C.** upon request, once every year
   **D.** upon request, once every two years

5. **What is the term for the scheme that involves attaching a device to money machines that reads the information on your debit and credit cards when you swipe them:**

   **A.** vishing
   **B.** card skimming
   **C.** pretexting
   **D.** smishing

6. **Which of the following industries has been subject to FTC enforcement actions due to privacy issues:**

   **A.** social media
   **B.** ad tech
   **C.** mobile apps
   **D.** all of the above

7. **How long does an initial fraud alert stay on an individual's consumer credit report:**

   **A.** for at least 30 days
   **B.** for at least 90 days
   **C.** for at least one year
   **D.** for at least seven years

8. **When an individual places an extended alert on his or her credit report, he or she is entitled to how many free credit report(s) from each of the three nationwide consumer-reporting companies within 12 months:**

   **A.** one
   **B.** two
   **C.** three
   **D.** unlimited

9. **Under the Identity Theft and Assumption Deterrence Act, which of the following agencies is responsible for receiving and processing complaints from victims of identity theft:**

   **A.** Federal Bureau of Investigation
   **B.** Department of Justice
   **C.** Federal Trade Commission
   **D.** Department of Homeland Security

10. **Federal law limits an individual's liability for unauthorized credit card charges for each card to how much:**

   **A.** $50
   **B.** $100
   **C.** $500
   **D.** $1,000

11. **How long are active duty alerts in effect on the requester's report:**

   **A.** 6 months
   **B.** 1 year
   **C.** 2 years
   **D.** 5 years

12. **How often does the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule allow individuals to order one free copy of the accounting from each of their medical providers:**

   **A.** every 30 days
   **B.** every 6 months
   **C.** every 12 months
   **D.** every 2 years

13. **Which of the following is true regarding child identity theft statistics:**

   **A.** social security numbers are the most commonly used piece of information by thieves
   **B.** victims will find out immediately if they have been targeted by an identity thief
   **C.** rarely does the victim know the individual who is responsible for the crime
   **D.** as the family income decreases, the risk of child identity fraud decreases

14. **Which of the following protects the privacy of student records and gives parents the right to opt-out of sharing contact or other directory information with third parties:**

   **A.** Family Education Rights and Privacy Act
   **B.** Identity Theft and Deterrence Assumption Act
   **C.** Freedom of Information Act
   **D.** Gramm-Leach-Bliley Act

15. **Which of the following is true regarding the process of clearing one's name after becoming a victim of criminal identity theft:**

   **A.** the victim's name will be completely taken off the official records
   **B.** the whole process is quick and simple
   **C.** there are no laws to enable victims to clear their names in the court records
   **D.** victims should receive "certificates of clearance" that should be kept on hand at all times

16. **Which of the following is true regarding mobile apps:**

   **A.** they only access data that is related to the purpose of the app
   **B.** they cannot share your data with other companies
   **C.** they can access your location until you change the setting on your phone
   **D.** it is easy to know what data a specific app will access

17. **To determine if a website is encrypted, the beginning of the web address should begin with which of the following:**

    **A.** http
    **B.** https
    **C.** www
    **D.** none of the above

18. **Which of the following is correct regarding the use of encryption on a wireless network:**

    **A.** it protects against all hackers
    **B.** it is the most effective way to secure your network from intruders
    **C.** it is unnecessary for home use computers
    **D.** it is only useful in hotspots

19. **Each of the following is a recommended tip for protecting yourself when using public Wi-Fi <u>except</u>:**

    **A.** stay permanently signed into accounts
    **B.** install browser add-ons or plug-ins that force the browser to use encryption on popular websites
    **C.** use a virtual private network (VPN)
    **D.** keep your browser and security software up-to-date

20. **Which of the following is true regarding peer-to-peer (P2P) sharing:**

    **A.** files can be permanently deleted or retrieved once another user on the P2P network has downloaded your files
    **B.** there is no need for concern if a P2P program asks you to disable or change the settings of your firewall
    **C.** closing the file-sharing program window (clicking the x) will always close your connection to the network
    **D.** some P2P programs open automatically every time you turn on your computer

21. **Which form of personal identification listed below plays the most significant role in people's lives:**

    **A.** driver's license number
    **B.** social security number
    **C.** library card
    **D.** passport

22. **Which of the following laws regulates the federal government's collection, maintenance, and use of personal information:**

    **A.** Freedom of Information Act
    **B.** Privacy Act of 1974
    **C.** Personal Information Security Act of 1978
    **D.** Identity Theft and Assumption Deterrence Act of 1998

23. **Which of the following is <u>not</u> one of the practices recommended for controlling access to social security numbers in business:**

    **A.** limit access to records containing social security numbers only to those who need to see the numbers for the performance of their duties
    **B.** generally share social security numbers with other businesses that request them
    **C.** use logs or electronic audit trails to monitor employees' access to records with social security numbers
    **D.** refrain from storing records containing social security numbers on computers or other electronic devices that are not secured against unauthorized access

**24. Which of the following is <u>not</u> a recommended practice for businesses to help prevent identity theft:**

- **A.** require employees to use passwords for access to databases containing personal information
- **B.** utilize faxes, e-mail, or voice mail to send messages containing sensitive personal data
- **C.** train employees about their responsibilities to protect client information from unauthorized access
- **D.** use a cross-cut shredder to destroy paper customer records containing personal information

**25. According to business espionage professionals, what is the single most available source of competitive and private information from the average business:**

- **A.** customers
- **B.** the trash
- **C.** computers
- **D.** employees

**26. Which of the following statements about a business's response to identity theft is correct:**

- **A.** a business should never contact law enforcement because such a practice may scare away customers
- **B.** a business should contact law enforcement, but only after waiting a reasonable period of time to see if it can fix the problem itself
- **C.** a business is advised to contact their local law enforcement agency immediately and report the situation
- **D.** identity theft is the customer's problem so the business should do nothing

**27. The Gramm-Leach-Bliley Financial Modernization Act of 1999 applies to which of the following:**

- **A.** companies that offer financial products or services to individuals
- **B.** accountants only
- **C.** all businesses that have annual gross sales of $100,000 or more
- **D.** banks only

**28. What type of information does the Gramm-Leach-Bliley Act require financial institutions to protect:**

- **A.** information collected about individuals only
- **B.** information collected in business activities only
- **C.** information collected in commercial activities only
- **D.** information collected about individuals and in business and commercial activities

**29. What does the Financial Privacy Rule govern:**

- **A.** the collection and disclosure of customers' personal financial information by financial institutions
- **B.** the collection of personal and financial information by the Internal Revenue Service and other federal agencies
- **C.** the collection and disclosure of personal information held by employers
- **D.** all of the above

**30. Which of the following is <u>not</u> an example of a customer relationship between an individual and a financial institution:**

- **A.** cashing a check with a check cashing company
- **B.** opening a credit card account with a bank
- **C.** leasing an automobile from an auto dealer
- **D.** obtaining the services of a tax preparer

**31. The Financial Privacy Rule requires covered entities to provide their customers with which of the following:**

- **A.** suggestions for safeguarding their personal financial information
- **B.** the responsibilities of the Federal Trade Commission in investigating identity theft
- **C.** a clear and conspicuous written notice describing its privacy policies and practices
- **D.** a list of agencies to contact in the event of a dispute

**32. How often must covered financial institutions provide their customers with the privacy notice mandated by the Financial Privacy Rule:**

- **A.** only before entering into a customer relationship
- **B.** at least once every quarter
- **C.** at least once in any period of 12 consecutive months
- **D.** every other year

**33. The Safeguards Rule applies to which of the following:**

- **A.** tax preparers
- **B.** mortgage brokers
- **C.** retailers that issue credit cards
- **D.** all of the above

**34. Which of the following is true regarding the written plan mandated by the Safeguards Rule:**

- **A.** it should be appropriate to the financial institution's size and complexity
- **B.** it should be designated to a single person
- **C.** it should be described in a single document
- **D.** it should be the same for all financial institutions

**35. Regarding the Safeguards Rule, each of the following are suggestions for maintaining security throughout the life cycle of customer or client information <u>except</u>:**

- **A.** store sensitive customer data on a machine with an Internet connection
- **B.** maintain secure backup media and keep archived data secure
- **C.** ensure that storage areas are protected against destruction or potential damage from natural hazards
- **D.** store paper records in a room, cabinet, or other container that is locked when unattended

**36. Federal regulations require banks to report all known or suspected criminal violations to law enforcement and which of the following by the use of the Suspicious Activity Report ("SAR"):**

- **A.** the Federal Trade Commission
- **B.** the Office of the Controller of the Currency
- **C.** the Internal Revenue Service
- **D.** the Securities and Exchange Commission

**37. Which businesses are subject to the federal Disposal Rule:**

- **A.** all financial institutions, regardless of type
- **B.** all businesses that extend credit
- **C.** any business that uses a consumer report for a business purpose
- **D.** all retail establishments

**38. Which of the following is true regarding disposal practices under the disposal rule:**

- **A.** they must be reasonable and appropriate to prevent the unauthorized access to, or use of, information in a consumer report
- **B.** they are guaranteed to prevent the unauthorized access to information in a consumer report
- **C.** they are expressly mandated by the Federal Trade Commission
- **D.** they must be approved by the entity's board of directors

**39. Which of the following must comply with the Red Flags Rule:**

**A.** banks
**B.** CPAs
**C.** lawyers
**D.** all of the above

**40. How often should the person responsible for the red flags program report to the board of directors or a designated senior manager:**

**A.** at least once a month
**B.** at least semiannually
**C.** at least annually
**D.** at least every other year