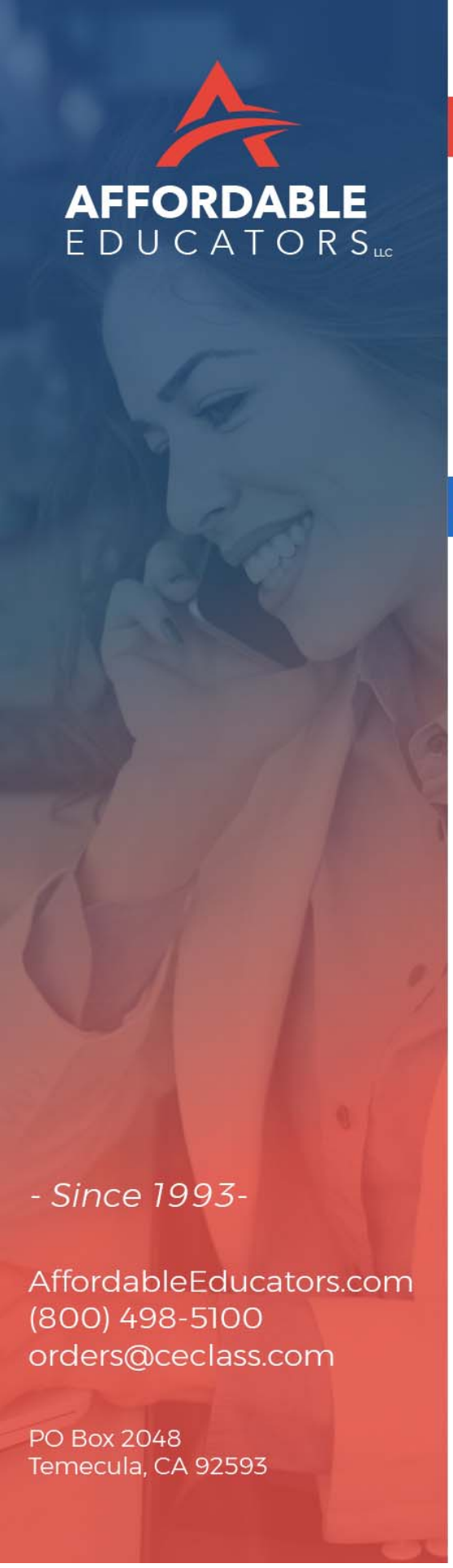


AFFORDABLE EDUCATORS LLC

- Since 1993-

AffordableEducators.com
(800) 498-5100
orders@ceclass.com

PO Box 2048
Temecula, CA 92593

182

AGENTS AND IDENTITY THEFT

COURSE INSTRUCTIONS

You are on Page 1 of this book.

Use your "Page Down", "Arrow Down" or scroll, to start reading.

How to Search Book?

Use ***CTRL+F*** (Command F for Mac) or ***Go to INDEX*** on next page.

Course Contents

iPad and Tablet Users See DEMO & Links Above

Index

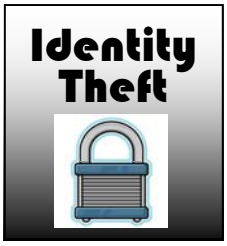
AFFORDABLE EDUCATORS

NEED HELP OR HAVE LICENSING QUESTIONS?

Insurance licensing and choosing proper / required CE courses can be tricky. A mistake can cost you a delay in commissions and license penalties.

We've provided excellent CE advice for 25 years! We know the rules and we're only a phone call away.

Call us
(800) 498-5100



Section1: What Is Identity Theft

Identity theft has become a rampant crime. The ability of computers to store large amounts of data, the value of this data for servicing and sales, and the ease of transmitting this information from one location to another, has led to the accumulation of thousands of pieces of personal data in thousands of locations. The knowledge and technological explosions that digital information makes possible also makes it possible for dishonest individuals to take information and steal the financial reputations of others, for a profit.

Identity theft costs financial institutions and other businesses hundreds of thousands of dollars annually. It creates a living nightmare for the individual whose identity has been stolen, who suddenly receives bills for items never charged, non-stop creditor calls, and perhaps is even arrested for crimes committed by the thief. Trying to protect the privacy and identity of customers has created a bureaucratic maze for any business that uses personal information. These businesses are required to issue myriad notices and disclosures, obtain authorizations for information release and set up systems to check and double-check the security. The presence of identity theft causes everyday citizens to make daily trips to the post office to safely mail bills, and to purchase shredders for the home office.

Types of Identity Theft

Financial Identity Theft

The perpetrator pretends to be an existing account holder in order to ***obtain funds*** from the legitimate bank account of the victim. This involves obtaining one or more identity token (plastic card, paper check, deposit slip, PIN code, card number, identifying personal data, etc.) then using the ID token to access funds via victim by presenting an accurate name, address, birth date, or other information that the lender requires as a means of establishing identity. Even if this information is checked against the data at a national consumer reporting agency, the lender will encounter no concerns, as all of the victim's information matches the records. The lender has no easy way to discover that the person is pretending to be the victim, especially if an original, government-issued id can't be verified (as is the case in online, mail, telephone, and fax-based transactions). This kind of crime is considered non-self-revealing, although authorities may be able to track down the criminal if the funds for the loan were mailed to them. The criminal keeps the money from the loan, the financial institution is never repaid, and the victim is wrongly blamed for defaulting on a loan he/she never authorized.

An account established by a perpetrator can be abused by passing bad checks, and "busting out" a checking or credit account with bad checks, counterfeit money orders, or empty ATM envelope deposits. If checks are written against fraudulently opened checking accounts, the person receiving the checks will suffer the financial loss. However, the recipient might attempt to retrieve money from the impersonated person by using a collection agency. This action would appear in the victim's credit history until it was shown to be fraud.

In most cases the financial identity theft will be reported to the national Consumer credit reporting agency or Credit bureaus (U.S.) as a collection or bad loan under the impersonated person's record. The victim may discover the incident by being denied a loan, by seeing the

accounts or complaints when they view their own credit history, or by being contacted by creditors or collection agencies. The victim's credit score, which affects one's ability to acquire new loans or credit lines, will be adversely affected until they are able to successfully dispute the fraudulent accounts and have them removed from their record.

Identity Cloning and Concealment

In this situation, a criminal acquires personal identifiers, and then ***impersonates*** someone for the purpose of concealment from authorities. This may be done by a person who wants to avoid arrest for crimes, by a person who is working illegally in a foreign country, or by a person who is hiding from creditors or other individuals. Unlike credit-dependent financial crimes, concealment can continue for an indeterminate amount of time without ever being detected. Additionally, the criminal might attempt to obtained fraudulent documents or IDs consistent with the cloned identity to make the impersonation even more convincing and concealed.

Criminal Identity Theft

When a criminal identifies himself to police as another individual it is sometimes referred to as "Criminal Identity Theft." In some cases the criminal will obtain a state issued ID using stolen documents or personal information belonging to another person, or they might simply use a fake ID. When the criminal is arrested for a crime, they present the ID to authorities, who place charges under the identity theft victim's name and release the criminal. When the criminal fails to appear for his court hearing, a warrant would be issued under the assumed name. The victim might learn of the incident if the state suspends their own drivers license, or through a background check performed for employment or other purposes, or in rare cases could be arrested when stopped for a minor traffic violation.

It can be difficult for a criminal identity theft victim to clear their record. The steps required to clear the victim's incorrect criminal record depend on what jurisdiction the crime occurred in and whether the true identity of the criminal can be determined. The victim might need to locate the original arresting officers, or be fingerprinted to prove their own identity, and may need to go to a court hearing to be cleared of the charges. Obtaining an expungement of court records may also be required. Authorities might permanently maintain the victim's name as an alias for the criminal's true identity in their criminal records databases. One problem that victims of criminal identity theft may encounter is that various data aggregators might still have the incorrect criminal records in their databases even after court and police records are corrected. Thus it is possible that a future background check will return the incorrect criminal records.

Synthetic Identity Theft

A variation of identity theft which has recently become more common is *synthetic identity theft*, in which identities are completely or partially fabricated. The most common technique is combining a real social security number with a name and birthdate other than the ones associated with the number. Synthetic identity theft is ***more difficult to track***, as it doesn't show on either person's credit report directly, but ***may appear as an entirely new file in the credit bureau*** or as a subfile on one of the victim's credit reports. Synthetic identity theft primarily harms the creditors that unwittingly grant the fraudsters credit. Consumers can be affected if their names become confused with the synthetic identities, or if negative information in their subfiles impacts their credit.

Medical Identity Theft

Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity—such as insurance information—without the person's knowledge or consent to ***obtain medical services or goods***, or uses the person's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name.

Common Methods Used To Steal Identities

Identity theft is not always a hi-tech exercise. Some of the methods below are alarmingly simple, preying on the complacency of people and companies.

Identity may be stolen by someone hacking into a computer, gaining access to an employer's records, or gaining information illegally through means of bribes or extortion. Thieves also trick people into revealing credit information, by watching over people's shoulder while they use ATM machines, or pretending to be someone with a valid need to know personal identification information.

Many people have the opportunity to gain access to pertinent personal information that is not properly secured or destroyed. Thieves hack into computers, dive into dumpsters, rifle through trash, steal wallets, scam information by posing as legitimate government offices or organizations, divert mail, or scan files from an employer to gain information that is lucrative to them and damaging to the victim.

Thieves damage the credit ratings of victims, before the victims have any idea that fraud has occurred.

- Stealing mail or rummaging through rubbish containing personal information (dumpster diving)
- Retrieving information from redundant equipment, like computer servers that have been disposed of carelessly, e.g. at public dump sites, given away without proper sanitizing etc.
- Researching about the victim in government registers, internet search engines, or public records search services.
- Stealing payment or identification cards, either by pickpocketing or surreptitiously by skimming through a compromised card reader
- Remotely reading information from an RFID chip on a smart card, RFID-enabled credit card, or passport
- Eavesdropping on public transactions to obtain personal data (shoulder surfing)
- Stealing personal information from computers and computer databases (Trojan horses, hacking and Zero day attacks)

- Data breach that results in the public (i.e. posted on the internet) or easily-obtainable (i.e. printed on a mailing label) display of sensitive information such as a Social Security number or credit card number.
- ***Advertising bogus job offers*** (either full-time or work from home based) to which the victims will reply with their full name, address, curriculum vitae, telephone numbers, and banking details
- Infiltration of organizations that store large amounts of personal information
- Impersonating a trusted company/institution/organization in an electronic communication to promote revealing of personal information (phishing)
- Obtaining castings of fingers for falsifying fingerprint identification.
- Browsing social network (MySpace, Facebook, Bebo etc) sites, online for personal details that have been posted by users
- Changing your address thereby diverting billing statements to another location to either get current legitimate account info or to delay discovery of fraudulent accounts.
- Using false pretenses to trick a business (usually through a customer service representative) into disclosing customer information (***pretexting***)
- Use of *'contactless' credit card skimming technology to acquire data recorded on special enabled cards*
- Stealing checks to acquire banking information, including account numbers and bank routing numbers.

A First Hand Account

Following is an account before Congress that illustrates the impact identity theft has on consumers as well as the need to better understand the fixes.

WEDNESDAY, SEPTEMBER 13, 2000
U.S. House of Representatives,
Committee on Banking and Financial Services, Washington, DC.

STATEMENT OF HON. STEVEN C. LaTOURETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Mr. LATOURETTE.

I thought I would, by way of illustration, share with the Committee a story as to how I became intimately involved with the issue of identity theft. Last year, a couple from my hometown, Ray and Maureen Mitchell, came into my district office.

And I have a special affection for the Mitchells, because when I was first running in 1994, their son, who goes to Madison High School with my daughter Sarah, was the only boy who would show up to be in my television commercials, so the Mitchells have been long-time favorites of mine.

They told me a numbing story of how they became involved in identity theft and how they had been involved now in "identity theft hell."

There are a half-a-million people a year out there just like them—victims of crimes that largely go unreported and widely misunderstood.

In many ways, being the victim of this crime can be far more devastating than being the victim of a typical crime. Once you are exposed to this crime, you never feel totally safe. As a matter of fact, now the Mitchells drive around with a signed affidavit in their car, fearing that when they make a purchase they will be confused for the bogus Mitchells, and this is not a way for innocent people to live.

The Mitchells' daughter just graduated from high school this year, and like a lot of parents, they wanted to buy her a car. They purchased the car with cash, however, because they were afraid they could not get a loan as a result of their once perfect credit now being shattered.

It started about a year ago. The Mitchells' bank noticed $2,100 worth of unusual charges on their credit card, and it has been downhill ever since. The thieves used the Mitchells' personal information to open new credit cards, buy cell phones, take out two huge personal loans, and purchase not one, but two $40,000 SUVs. One was a Ford Expedition. They are probably having some problems with their tires now.
[Laughter.]

Mr. LATOURETTE. And the other one was a Lincoln Navigator.

All told, Ray and Maureen have been victimized to the tune of $110,000. The Secret Service is involved, the Postal Inspector is involved, Illinois authorities are involved.

But last November 19th, Mr. Chairman, three days after the fraud alerts were placed on their credit report, a man went into three different Chicago banks, and in a two-hour period applied for $45,000 worth of personal loans in Ray Mitchell's name. Each time the bogus Ray Mitchell presented a valid Illinois driver's license, an Illinois State identification card, and all of the real Ray Mitchell's personal information.

The Mitchells never engaged in so-called risky behavior or behavior that is, quite frankly, typical for millions of American families. They did not put shopping receipts or preapproved credit card offers in the trash. They did not buy things online. They did not do catalogue shopping or pay for credit card purchases over the telephone. There was no stolen wallet or credit cards. Still, someone was able to re-create Ray Mitchell's identity with ease. Because the Mitchells had a history of always paying their bills on time and had a blemish-free credit report, they were a perfect target.

The good news, Mr. Chairman, is that the guy that applied for the loans was arrested the same afternoon. Police arrested him as he tried to leave Bank One in Chicago, after securing a $15,000 loan. He had $5,000 in cash and $10,000 in bank checks payable to "Raymond Mitchell".

The bad news is that the judge freed him two days later on a personalrecognizance bond, even though he has a criminal record dating back to 1977 and has used seventeen different aliases. Suffice to say that the guy was not shaking in his boots when he was arrested. He told the detective, "I did not use a gun. I did not use a knife. Call my lawyer and I will plead guilty and they will put me on probation."

The Mitchells are angry, Mr. Chairman. They agree with the purposes of this bill. There were red flags that should have been noticed by someone, like the thirty inquiries in the Mitchell's credit card report in just sixty days or the numerous change-of-address requests.

This testimony reflects just one of thousands of cases of identity theft that occur each year. It is a crime that is cutting a deep swathe throughout American society, changing the ways business is being done and people view their personal information.

Identity theft occurs when someone uses an individual's name, social security number, credit cards, or banking information without that individual's permission, for profit or other unauthorized use.

A New Crime

Identity theft started to occur in earnest in the 1990's, and the rate of this activity has grown substantially over the years. Because personal information is shared many times daily -- information that includes social security numbers, credit card, checking account numbers, and drivers license numbers – more and more people are vulnerable to this theft. Talking on cell phones, using credit cards in person and over the internet, writing checks and paying with them over the phone, and sharing addresses and phone numbers with unknown people each day gives identity thieves many opportunities to prey on unknowing victims. Each piece of information that is shared can potentially be used to commit a crime.

FTC Examples

The Federal Trade Commission (FTC), which is responsible for several identity theft victim services as well as consumer education about identity theft, recently released figures showing that 27.3 million Americans have been victims of such theft in the last five years. In 2003 alone, 9.9 million people were victims. According to this survey, victims paid over 5 billion dollars in out of pocket expenses, and financial institution losses totaled nearly 48 billion dollars. Here are just a few accounts from identity theft victims, compiled by the FTC:

From a consumer complaint to the FTC, January 2, 2001:

My purse was stolen in December 1990. In February 1991, I started getting notices of bounced checks. About a year later, I received information that someone using my identity had defaulted

on a number of lease agreements and bought a car. In 1997, I learned that someone had been working under my Social Security number for a number of years. A man had been arrested and used my SSN on his arrest sheet. There's a hit in the FBI computers for my SSN with a different name and gender. I can't get credit because of this situation. I was denied a mortgage loan, employment, credit cards, and medical care for my children. I've even had auto insurance denied, medical insurance and tuition assistance denied.

From a consumer complaint to the FTC, February 22, 2001:

My wallet was stolen in December 1998. There's been no end to the problems I've faced since then. The thieves used my identity to write checks, use a debit card, open a bank account with a line of credit, open credit accounts with several stores, obtain cell phones and run up huge bills, print fraudulent checks on a personal computer bearing my name, and more. I've spent the last two years trying to repair my credit report (a very frustrating process) and have suffered the ill effects of having a marred credit history. I've recently been denied a student loan because of inaccurate information on my credit report.

From a consumer complaint to the FTC, April 3, 2001:

In November 2000, I found out that someone used my information to obtain a cell phone. Since then, I've been living a nightmare. My credit report is a mess. It's a full-time job to investigate and correct the information.

The Workplace

The workplace is an identity thief's favorite hunting ground. Thieves gain access to records through employers, when personal financial information is left on desks, or thrown into wastebaskets or dumpsters. The company credit card is another source of information for identity thieves, especially dishonest employees of the card vendor. Unlocked employee personnel paper and computerized files provide all the details an identity thief needs to open credit card accounts, establish a checking account, rent an apartment, buy a car, or even get a new job, all using the employee's identity.

The FTC reported in 2003 that ***the biggest source of identity fraud is employer records*** and other records from businesses. The FTC states that 90% of business records theft involves payroll and employment records, and customer lists account for about 10%.

Identity thieves use a number of methods to gain access to employer and business records. Some have taken jobs as temporary workers with the express intent of gaining access to company files. Others work as janitors, and scour the company's location after-business hours for records in wastebaskets and in unlocked files and computers. Sometimes, fellow employees are the culprits, and rifle through desks, purses and the coatroom for personal data.

"Friends" and Relatives

Today, home is not a haven of safety from identity theft. Another source of identity theft are "friends," relatives and acquaintances. Friends and relatives know the victim's address, birth date, employer, and other key information that can be used in identity theft. They may gain

access to personal data kept at the victim's home, or thrown away as trash. A credit card statement left on a table may be stuffed into the thief's pocket and used to make unauthorized purchases. An insurance policy filed in the home office may be taken and the social security number within it used to open new credit cards, sent to the thief's address.

Passersby

Many people also have had their identity stolen when they failed to shred credit card statements before disposing of them. The information is fished from a curbside garbage can. Thieves then proceed to empty bank accounts, purchase small and large ticket items, and open credit accounts of every kind.

Mail Theft

Mail theft is a common way to gain access to personal information. Thieves have been known to divert mail by filling out change of address forms. They then have access to the bills, bank statements and credit card applications of the prior addressee. Plus, any new checks or newly issued or renewed credit cards will all conveniently be mailed right to the thief's doorstep – or more likely to his or her locked post office box.

Or, the thieves steal outgoing or incoming mail in order to compile the data they need to assume a victim's identity. Apartment and condominium complexes are favorite mail theft targets. The thieves can break one lock, and have access to the contents of dozens of mailboxes.

Individual mailbox holders are not free from the threat of mail theft. Identity thieves roll down suburban streets, where many people are absent from home during the day, emptying one mailbox after another.

Impact of Identity Theft

Identity theft is hard on the individual whose name is used without permission. It leaves victims feeling not only vulnerable, but also alone.

It is sometimes hard to get police officers to pay attention to this crime, when violent and drug related crimes need their time.

Creditors who contact the victim to collect funds are often more interested in getting the money than in listening to the victim's claim that the charges are unauthorized. Calmly working with the identity theft victim to straighten out their credit mess is not traditionally part of a bill collector's job description. There are many people who just don't want to pay the bills they rightly should, and the identity theft victim has to work hard to prove to creditors that they aren't just another "deadbeat."

Slow Wheels of Justice

Traditionally, little has been done to ***prosecute the identity theft offender***. The cost of prosecuting such cases is high, and the prosecution often has a ***difficult case to prove***, so law enforcement agencies are often reticent to do much about the crimes. Also, since may credit card companies do not hold the credit card holder responsible for most of the unauthorized charges incurred by the thief, law enforcement agencies traditionally have not looked at the individual against whom the identity theft occurred as the victim of the crime. Rather, they consider the credit card companies as the victims, and require that the credit card companies file charges against the thief. Changes have been made at the federal level to help make the prosecuting of identity thieves more likely.

Lost Time

A single victim may spend hours, weeks, or months trying to put back the order that a thief has unraveled. On average, according to the FTC, a victim spends 175 hours straightening out credit reports and picking up the pieces left by the crime. Credit bureaus must be notified, police reports must be filed, and creditors must be contacted. In many cases, supplemental affidavits and other proofs must be written or collected and sent to these entities. Sometimes, creditors have to contacted again and again to ensure accounts are closed and the creditor stops accepting additional charges to the account.

Lost Credit

Years of good credit habits, diligence and hard work in paying bills on time can be lost for victims of identity theft. They may be denied loans, housing, or education. In some cases, they may even be arrested for crimes they did not commit. Victims are commonly contacted and harassed by collection agencies seeking payment.

Tax Liens

Some identity theft involves the IRS. If someone else uses the victim's name and social security number for employment purposes, and does not file an income tax return, it appears that the identity theft victim is not properly claiming income for tax purposes. The IRS then tries to collect back taxes from the victim.

Increased Expenses

Victims of identity theft incur expenses when trying to clean up their credit or medical mess. They have to communicate with law enforcement agencies that may be far from their homes, causing them to pay for long-distance and mailing charges. They may have to engage legal counsel, creating expenses for legal services. They may also have to miss work, reducing their income.

The victims of these crimes have their lives turned upside down, and it takes much time and effort to regain their good credit reputation, and right the wrongs that they did not commit.

Why Is Identity Theft Important Today?

There are many reasons. First and foremost is the fact that the ***sharing of information has become complicated***. The United States is in the midst of a revolution in information technology. Gone are days of a customer's financial and health records being locked in a file room at the rear of the office. New electronic distribution channels of providing and servicing insurance products and health care have created exposure of personal financial information and health histories. And, the way we get our health care is changing from one-on-one, patient/doctor relationships, to large, integrated health networks where many levels of employees have access to records. In a sense, a new by-product of trying to control health-care and insurance costs using technology and centralization has resulted in a profound potential for abuse of privacy.

In a nutshell, today, entire networks distribute and / or disclose the data you collect on your clients with a variety of affiliates and third parties; all the while, putting you and other agents in the path of tighter and more responsible privacy rules.

Information Sharing Problems

Some have a problem understanding why the sharing of client information is a problem. After all, wouldn't it be to the client's benefit for a central database to itemize a history of medications and comprehensive medical records? For example, what if you were involved in a car accident far from home and unconscious by the time you arrived at the local hospital? The emergency room doctor might conceivably access a special computer link; plug-in your social security number and instantly learn about your specific allergies, medical conditions and medications. Life-saving therapies might be administered faster and costly re-testing for certain information might be avoided. Sounds great, right?

Unfortunately, not everyone will use this kind of information as it was intended. For example, what if the same medical records were retrieved by a prospective employer. Could he use the health and financial information in making a decision <u>not</u> to hire you? Insurers themselves have been accused of privacy invasion when they use personal financial information, like FICO scores (a system to determine a consumer's credit worthiness), to raise insurance premiums or rank insurability based on the types of credit cards, catalogs or cars a prospect owns and uses.

Also, consider cases where records have fallen into the wrong hands. Are the consequences of exploiting personal information sufficient to deter someone from the temptation? Think it doesn't happen? Think again. In Nevada, for example, a woman purchased a used computer and discovered that it still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy database included names, addresses, social security numbers, and a list of all the medicines the customers had purchased. What happens to the data on your old computers? In another case, a 30-year FBI veteran was put on administrative leave when, without his permission, his pharmacy released information about his

treatment for depression. Or, how about a 1999 incident in which the health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut.

The Importance of Privacy

The reasoning behind the ***enacting of state and national privacy rules*** includes the assertion that ***privacy is a fundamental right of the citizenry***. It is considered as essential to individual and collective freedom. All fifty states recognize a common law or statutory right to privacy. A few states include the right to privacy in their respective constitutions.

From the founding of the United States, privacy has played a fundamental role in the structure and content of America's laws. As stated in the Federal Register: December 28, 2000, Volume 65, Number 250:

"Throughout our nation's history, we have placed the rights of the individual at the forefront of our democracy. In the Declaration of Independence, we asserted the "unalienable right" to "life, liberty and the pursuit of happiness." Many of the most basic protections in the Constitution of the United States are imbued with an attempt to protect individual privacy while balancing it against the larger social purposes of the nation.

To take but one example, the Fourth Amendment to the United States Constitution guarantees that "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated." By referring to the need for security of "persons" as well as "papers and effects" the Fourth Amendment suggests enduring values in American law that relate to privacy. The need for security of "persons" is consistent with obtaining patient consent before performing invasive medical procedures. The need for security in "papers and effects" underscores the importance of protecting information about the person, contained in sources such as personal diaries, medical records, or elsewhere. As is generally true for the right of privacy in information, the right is not absolute. The test instead is what constitutes an "unreasonable" search of the papers and effects."

The United States Supreme Court recognized two different kinds of interests within a constitutionally protected "zone of privacy" in a New York case, Whalen v. Roe, 429 U.S. 589 (1977). In this case, a New York statute that created a database of persons who obtained drugs that were available both lawfully and unlawfully. One of the interests said to be protected in the zone of privacy is "the individual interest in avoiding disclosure of personal matters."

However, an individual's right to privacy in information about himself is not considered an absolute right under United States law. For example, the right to privacy does not prevent the reporting of communicable diseases to public health agencies, or stop law enforcement from obtaining information as long as due process is observed.

It is largely held that each individual has some rights to control personal and sensitive information about himself. In particular, medical and health information may be among the most sensitive type of information. People do not want their medical and health information to be

publicly available, where anyone from neighbors, relatives, employers and the government could review it.

Mental health information may be the most sensitive type of medical or health information. Mental health treatment may include records of reflections of a patient's most intimate thoughts, words and emotions. The Supreme Court held in Jaffee v. Redmond, 116 S. Ct. 1923 (1996), that statements made to a therapist during a counseling sessions were protected against civil discovery under the Federal Rules of Evidence. Within its opinion, the Court noted that some form of psychotherapist-patient privilege has been adopted by all fifty states. The Supreme Court stated that it "serves the public interest by facilitating the appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance."

The Right of Privacy

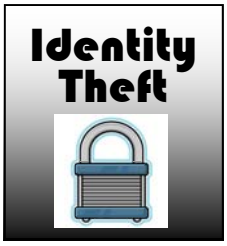
Privacy has become a prominent issue in every part of the American and international economy in the last few years. Legislators have been introducing many privacy bills. Laws already in place are being reinforced with new regulations and deadlines. The process of underwriting and gathering client information go hand in hand. The Internet, consolidation in financial services, and the electronic transfer of medical and financial client data have sparked new privacy concerns. Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age.

Nearly every country in the world recognizes a right of privacy explicitly in their Constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. Most recently written Constitutions such as South Africa and Hungary's include specific rights to access and control one's personal information. In many of the countries where privacy is not explicitly recognized in the Constitution, such as the United States, Ireland and India, the courts have found that right in other provisions. In many countries, international agreements that recognize privacy rights such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights have been adopted into law.

Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define and circumscribe. Privacy has roots deep in history. The Bible has numerous references to privacy. There was also substantive protection of privacy in early Hebrew culture, Classical Greece and ancient China. These protections mostly focused on the right to solitude. Definitions of privacy vary widely according to context and environment. In many countries, the concept has been fused with Data Protection, which interprets privacy in terms of management of personal information. Outside this rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs. It can be divided into the following areas:

- **Information Privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records

- **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches
- **Privacy of communications,** which covers the security and privacy of mail, telephones, email and other forms of communication
- **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.



Section2: Identity Theft & Insurance

What Goes Wrong

The identity theft we hear about most is the credit-style scams in TV commercials or as a spotlight on 60 minutes where some poor sole has had his life turned upside down when his credit identity was stolen?

But identity theft can also affect insurance agents and their clients viciously and directly. Most insurance identity theft breaches come from four primary directions:

Employee Mistakes: An employees seals or somehow causes by his mistake a customer's personal information to be exposed, stolen or viewed. This can be as quick and dirty as opening an email attachment with a virus that invades the agency's computer system.

Physical Loss: Perhaps a computer hard drive with customer information gets stolen, sold or recycled or client files get disposed in a dumpster before getting shredded.

Password Breaches: Theft or loss of a password that allows unauthorized individuals access to computer files and a customer's personal information.

Work In Progress Exposures: Applications for insurance contain all kinds of personal information and these documents, both paper and digital, can get passed around quite a bit. For example, a single app might be submitted to three different carriers for quotes and underwriting appraisal. And, all the employees of these three companies now have access to this information that you sent. These apps can further be sent to data warehouses, the Medical Information Bureau, etc.

Identity Theft Insurance Scams

Clearly, there are a lot of opportunities for a customer's personal identity information to be exposed and abused. What can someone do with it? Well, beyond the normal credit scams, you will soon read about some insurance scams de jour . . . what happened to the agent . . . . what happened to the customer. It's a sad commentary that needs your attention.

Stolen Insurance Info: Stolen basic member ID and group policy number founds on insurance cards can be used to impersonate one of your clients. The perpetrator can receive everything from routine physicals to major surgery under your client's coverage. This is surprisingly easy to do because many doctors and hospitals do not ask for identification beyond an insurance card.

Agent Records Hijacked: Social Security Numbers and driver license numbers were stolen from an insurance agent's office. The agent was responsible for notifying two-thousand customers that their private identities may have been compromised.

Reselling Stolen Indo: Medical information is stolen by insiders at a medical or insurance office. Thieves download vital personal insurance data and related information from the operation's computerized records, then sell it on the black market or use it themselves to make fraudulent billing claims.

Medical Records Disaster: A retired school teacher was harassed by a bill collector for a medical bill for the amputation of her foot. The problem was: she still had two feet. The amputation was performed on a scammer who also had diabetes. Months later, the school teacher suffered a heart attack. When she awoke in the hospital the nurse asked her what type of drug she was taking for her diabetes. Has she underwent heart surgery as a diabetic, the mistreatment could have been life threatening.

Dropped Coverage: A healthy female received a disturbing "Notice To Cancel" her health insurance. When she inquired why, the company told her she was suspected of fraud for not disclosing "pre-existing cancer" on her application. After investigation, she learned that someone had stolen her identity and was attempting to use her coverage in addition to applying for thousands od dollars worth of credit cards.

Medical Identity Theft: A perfectly healthy man was blocked from buying a home when $66,000 of outstanding medical bills surfaced on his credit report, including $19,000 for medical transportation. The debt was incurred by a medical identity thief.

Child Identities: More and more, children are becoming the target of identity theft. Worse yet, the crime is likely to go undetected for years because kids are not attempting to apply for loans or credit cards. In a really pathetic case, a father deliberately ran up his son's credit and failed to make good on the debt. It took the son (who happened to have the same name as his father) 10 years to clean up his reputation.

Medicare Patients Exposed: Thousands of files listing unpaid Medicare bills for patients in eight states were stolen from 10 computers protected by passwords, video cameras and locks. Data on the records includes Social Security numbers.

Veterans Data At Risk: A computer containing personal information on thousands of veterans turned up missing. The computer contained names, address, Social Security numbers, dates of birth, claims data and more for at least 5,000 veterans, possibly more.

Agent Victims: Recent scams have even targeted insurance agents where savvy thieves pretend to be state insurance department officials informing an agent that their insurance license is about to be revoked because of some "outstanding paperwork" or fines unless they provide a payment using a credit card as well as other personal information like birthdates, Social Security numbers, etc. ***State Insurance Departments DO NOT ask for this information over the phone.***

Medical Record Lockout: Some medical identity theft victims found that scams in hospitals and doctor offices are so convincing that these same medical professionals feel that revealing bogus treatments would actually compromise the privacy of the imposter who infiltrated them. Therefore, the victim could be "locked-out" of his own medical records!

Agent Scammers: Some less-than-ethical insurance agents with unfettered access to private client files, have used this information to file false claims or creating fake client accounts to earn extra commissions and bonuses or cash in on a bogus settlement (more on these agents later).

Insurance Risk Appraisal

Risk appraisal helps an insurance company determine the appropriate cost to cover one's ***risk profile***—or one's "fair share." It prevents one from having to pay the same as someone with a less favorable risk profile. Risk appraisal is necessary to allow the carrier to offer coverage at an affordable price, and in some cases, to offer coverage at all. What does this have to do with identity theft? Well, nothing can be accomplished in the risk appraisal arena without the use of personal financial and health information supplied by consumers. It is to the advantage of BOTH that this information be collected with as little restriction as possible and protected with best efforts. A breach of this personal information jeopardizes the entire risk appraisal process.

Think about it. A world without risk appraisal would mean everyone would pay the same price. Even if a consumer would be considered a "good risk," he would end up paying more than the appropriate amount for his risk level. That is because he and every other policy owner would have to absorb the extra risk and costs associated with those who have less favorable risk profiles. These extra costs would drive up the cost of insurance for everyone. Risk appraisal is especially important to the policy owner because it protects the value of his insurance. It ensures that the underwriter will only issue appropriate amounts of insurance, at the appropriate price, to people who fall within established guidelines. It also ensures that the underwriter's risk appraisal guidelines and goals remain consistent over time. Risk appraisal safeguards against compromising the value of customers' insurance and the financial stability of the company. A thorough risk appraisal process helps the consumer in several ways.

- **Lower Cost** – He is often able to purchase a policy as a member of the most favorable risk group, which means the best price—he pays only his fair share.
- **Locked-in Risk Classification** - Once the risk classification has been determined for one's policy, it cannot be changed due to deterioration in his health.
- **Quality Coverage** - A thorough risk appraisal process is a hallmark of a strong company. One can be confident he is receiving the finest-quality coverage for his money.
- **Non-Cancelable Coverage** - Once a policy is issued, the company cannot cancel it due to a deterioration of your health. By participating in the risk appraisal process, and supplying accurate information, he can secure insurance coverage that can be with him for the rest of his life.
- **Early Warning** - The risk appraisal process might alert one to potential or existing health problems that he otherwise may not have known about.

The risk appraisal process allows the underwriter to determine the state of the client's health, his financial situation and, if necessary, whether his job and hobbies impact his application. It is

critical for insurers to ask for and collect information from the client about himself. The underwriter treats all of this information as personal and sensitive. And, just as the client has a responsibility to provide the underwriter with this information, the underwriter also has a responsibility to ensure that it is handled carefully and with confidentiality. The professional underwriter has established procedures in every step of the application and risk appraisal processes to help maintain the consumer's privacy. He is committed to maintaining the confidentiality of all of the information that he receives from his clients. Agents must do the same.

Understanding Consumer Concerns

The most important compliance issue for the insurance industry over the next ten years will most likely be privacy. The quest for greater privacy is a natural reaction to the information age. Privacy is a basic human right that is being reasserted. Consumers are demanding a choice in how information is used. The National Association of Insurance Commissioners believes that consumers are concerned about all types of marketing activities. They are concerned about activities related to their financial or health information.

The Internet holds tremendous potential for reducing healthcare costs and opening the door for patients to take a more active role in the administration of their healthcare. The same systems, which streamline the processing of healthcare information and afford easy, timely access to personal health information, also open new doors to the misuse of sensitive information. It is not hard to see how personal health information given to a physician or other healthcare provider, would be sought by insurers, employers or even advertisers. It is the doctor and patient's fears of this potential misuse that is the Achilles Heel of online healthcare services. Unfortunately, countless abuses of personal information by e-commerce companies have created an environment of open distrust of online services.

Privacy advocates' numbers have exploded in the past two years in response to corporate abuses. The fact that corporate America openly spends hundreds of millions to lobby against new privacy legislation adds to consumer distrust. But, privacy concerns in the world of e-commerce pale in comparison to a patient's perception that his or her personal health information could be revealed to someone without consent. The damage that could occur from misuse could be devastating to an individual, causing great personal harm. No wonder indeed, that doctor and patient acceptance of Internet technologies will depend on the perception that information that is entrusted to the healthcare system will be protected by stringent standards.

A report by the American Medical Association says the majority of today's health information web sites do not comply with their own stated privacy standards, and fail to protect personal health information of their visitors. As eHealth moves beyond information sites to more direct healthcare functions, privacy will become even more important. Building confidence in the online experience is critical to the future success of eHealth. Privacy failures will stifle physician and patient enthusiasm for the online health industry.

Personal Health Information

Even though the consumer is concerned about activities related to both his health and financial information, he desires a greater level of protection for his personal health information. Health records are among the most sensitive data that are acquired, used, and disclosed by the government and the private sector. Health information reveals a great deal of personal facts about individuals which may lead to stigma and discrimination when possessed and misused by government officials, employers, insurers, and by friends and family. The increasing potential for disclosure of this information within a rapidly developing national health information infrastructure, facilitated by massive computerization of records and other technological developments, presents significant risks to individual privacy.

Despite the highly sensitive nature of individual health information, protecting the privacy and security of these records has been historically de-emphasized when compared with statutory protections allotted to other types of personal information such as banking and investment records, consumer spending information, tax information, and video rental records. There are many reasons for the de-emphasis of health information privacy, including economic and political theories. However, modern legal developments are likely to improve privacy and security protection. As we develop a national health information infrastructure, the importance of privacy and security become crucial.

Health information privacy, of course, is a two-edged sword. While it is important in respecting the autonomy and dignity of individuals, excessive amounts of privacy can impede many of the goals of the health care system. Health information creates unprecedented opportunities to benefit individuals and communities. Health care professionals can use computerized data to improve clinical care for patients. Health service researchers can better assess the quality of services. Government and health service managers can gain administrative efficiencies. Health insurers, including Medicare and Medicaid, can prevent fraud and abuse. Public health authorities can improve surveillance and epidemiological investigations within the community.

In each of these areas, overly restrictive health information privacy and security protections may thwart legitimate and important uses of identifiable health data that benefit society. Though privacy is certainly necessary, legal protection should strike a reasonable balance between individual rights and the collective goods of health information. Today, society is witnessing tremendous changes in both the collection and use of health information and in the environment in which it resides. The transition from fee-for-service health care to managed care has led to a demand for an unprecedented depth and breadth of personal information by a growing number of players. At the same time, the environment for information is moving rapidly from paper forms and files to electronic media, giving organizations a greater ability to tie formerly distinct information together and send it easily through different sources.

Personal health information can be used to hurt consumers in various ways. Consumers realize that their health information can be used against them when they are trying to qualify for a loan or mortgage. It can also be used against one when he is applying for a job, or cause termination of employment. An individual with a medical condition requires treatment with a very high-priced prescription drug. After his insurance company receives the claim for reimbursement, his doctor receives numerous calls from pharmaceutical companies trying to convince him to change the

medication to a drug that their company produces. Other patients have received marketing calls for products related to their illness, even though they had not disclosed this information to anyone other than their insurance company.

Because of these consumer concerns, the National Association of Insurance Commissioners (NAIC) has decided to treat health information differently from financial information. This will be done by using an “opt-in” standard for individually identifiable health information, and by enforcing marketing restrictions. It is critical for underwriters to be thinking about the future, and making privacy compliance a significant factor in planning for the future. It is also important for them to begin developing a privacy compliance program.

Studies have shown that health web sites understand the consumer’s concern about the privacy of their personal health information. These web sites have tried to establish privacy policies, but there is inconsistency between the privacy policies, and they fall short of truly safeguarding consumers. Visitors to health web sites are seeking to manage their health better. The risks of doing this, however, are that they are not anonymous, even if they think they are, and their personal health information is probably not adequately protected. To make matters worse, health web sites disclaim liability for the actions of third parties, which negates the privacy policies.

Personal Financial Information

Banks, insurance companies, and brokerage firms operating as one are known as financial institutions. They offer benefits such as consolidated account statements and lower fees. At the same time, the ability of these companies to merge customer data from several sources and even sell it to third parties represents a real risk to one’s privacy. Consumer information kept in the files of financial institutions is some of the most sensitive, personal information imaginable. In the past, there were few restrictions on a financial institution's ability to share or even sell one’s personal information. Title V of GLBA gives the consumer some minimal rights to protect his financial privacy.

The GBLA requires that a financial institution give the consumer notice of three things:

- **Privacy Policy:** The financial institution must tell one the kinds of information it collects about him and how it uses that information.
- **Right to Opt-Out:** The financial institution must explain one’s ability to prevent the sale of his customer data to third parties.
- **Safeguards**: Financial institutions are required to develop policies to prevent fraudulent access to confidential financial information. These policies must be disclosed to the consumer.

The deadline for financial institutions to comply with new privacy regulations under Title V of the Gramm-Leach-Bliley Act was July 1, 2001. Financial services professionals spend hours attending seminars, pouring over the legislation and reading clarifications from the office of the Comptroller of the Currency. The law contains extensive federal requirements governing the

disclosure of consumer information by banks and other private entities. Differing requirements created some confusion because satisfying one set of requirements does not necessarily amount to compliance with another.

Consumers continue to express concern over the availability and distribution of their personal financial information. Relieving their concerns may not be as simple as complying with the letter of the law. While consumers may have been only vaguely aware of debate in Washington leading up to the new legislation, they find it impossible to ignore one of its by-products. A typical consumer's home mailbox has been stuffed with privacy notices from banks, credit card companies, brokerage and investment firms, and other finance companies. While financial institutions have notified consumers, it's ongoing communication and education that are the key to long-term consumer confidence. Effective communication requires a certain amount of empathy, and the ability to see a situation from another point of view. Financial service companies must continue to develop their privacy policies keeping their customers at the forefront. Financial service companies should ask themselves how their customers might react to the following issue:

- The quantity of a customer's personal financial information the business collects
- How the business uses the information
- Whether that information is transferred to affiliates or other parties
- Which other entities receive that information
- What happens to the information once it is handed over to another party

Financial service companies that deal with a customer's nonpublic financial information should make every effort to explain their privacy policy in plain language. Failing to understand the volatility of sentiment surrounding privacy may endanger the public trust that financial institutions have worked diligently to earn and maintain. Eroding consumer trust could constrict the flow of vital credit information, and this in turn would have a negative impact, not only on financial institutions, but also on consumers. When lending institutions have an accurate and complete picture of creditworthiness, they reduce their risk in lending, which ultimately reduces the cost of credit. Consumers can shop for the best rates among many lenders who can quickly access the applicant's financial information. This increases competition among lenders and also helps to drive rates down for consumers. The ability to monitor information also helps financial institutions spot fraudulent activity, and identify unusual transactions or unacceptable risks. When fraud does occur, immediate access to information helps investigators limit loss and apprehend criminals.

Availability of consistent and accurate information has enabled investors to buy loans of similar credit quality that are packaged and sold as asset-backed securities. Access to this information allows investors to judge with more confidence the risks and potential return of their investment. The secondary mortgage market is one example of successful secondary markets that provide liquidity, spread the risk among a large pool of investors, and lower the price of loans. According to at least one estimate, the secondary loan market has lowered the price of mortgages in the U.S. by a full two percentage points in comparison to other countries.

Secondary markets for automobile loans and credit card receivables are producing similar results. Investors in pools of security backed assets hold more than 50% of all revolving credit and over 30% of all non-mortgage consumer credit, currently totaling approximately $436 billion.

The advent of online financial transactions heightened consumer demands that financial service companies handle and exchange nonpublic financial information responsibly. Technology has opened the door for new, more specialized financial products and services, but in order to successfully take advantage of those opportunities, banks must reassure consumers that the bank-customer relationship -- and the expectation of privacy that is an essential part of that relationship -- will be honored as much on the Internet as it is in the branch office.

Customers enjoy the benefits and convenience that an information-based marketplace makes possible, such as fast credit approval or financial products tailored to their specific needs. In the past, consumers may have enjoyed these benefits without understanding what is required to handle nonpublic financial information responsibly. The new privacy regulations may prompt consumers to make more informed choices about how their personal financial information is used. At the same time, the rules are moving financial institutions to demonstrate they take privacy protection seriously. Education and privacy protection are both vital because consumers and financial service companies have too much to gain from a marketplace where information can be exchanged quickly, accurately and securely.

Steps to Take When Identity Theft Occurs

If an individual is concerned that credit theft has occurred, it is important that he or she contact the three major credit bureaus and place a fraud alert on the credit file held at each credit reporting bureau. The three major credit bureaus are Equifax, Experian, and TransUnion. (Their phone numbers and addresses may be found in the “ID Theft Affidavit,” later in this chapter.)

Fraud Alert

In theory, the victim should be able to contact just one of the credit bureaus, and that bureau should pass on the fraud alert to the other bureaus. However, those with experience in trying to clear up credit problems strongly suggest that each bureau be contacted individually to help ensure that the information is properly included in the report generated from each bureau. Newly enacted legislation, that will be discussed later in the course, is putting into place a centralized system that may make these multiple contacts unnecessary. The fraud alert requests creditors to contact the individual before opening any new accounts or making changes , such as increasing the credit line, to existing accounts.

In certain state laws, an agent may be responsible to contact customers and credit bureaus if an identity breach has occurred. This could involve embarrassing mailings and a major expense in credit bureau fees.

Examine Credit Reports

Once the bureaus have been notified, they are to send credit reports free of charge to the victim. The victim must then examine the reports carefully, looking for inaccurate account information.

An important part of the credit report that should be scrutinized is the “inquiries” information. The “inquiries” portion of the report lists creditors who have recently pulled a credit report on the victim. For example, the victim may see that several creditors have pulled his or her credit report in the past six months, and the victim had not given any of them permission. This may mean that new false accounts are pending with these creditors. They should be contacted ASAP, to stop more credit being racked up under the victim’s name. When the credit bureaus are notified, the victim should also require that all the unauthorized inquiries be removed from the reports.

Police Report

Any fraudulent accounts must be closed, and a police report filed as soon as possible after the identity theft has been discovered. The victim may also need to close all bank accounts, since fraudulent checks could be written under his or her name.

It is also important to obtain a copy of the police report and send it to all creditors and others who require proof of the crime***. Without the police report***, some ***creditors will not stop contacting the victim***, demanding payment. If there are disputed amounts, experts tell victims that the amounts should not be paid, even if a creditor is persistent. Instead, victims should remain firm with the creditors, stating that the victim did not incur the charges, but that they were incurred by the thief.

The victim should also file a complaint at the Federal Trade Commission. The FTC will file a record of the crime. Law enforcement agencies may then use FTC information to investigate and prosecute criminals. The FTC’s Identity Theft Hotline is 1-877-IDTHEFT (438-4338). In addition, the FTC has an “ID Theft Affidavit,” which can be used to report the theft information to many organizations, including creditors. A copy of this affidavit is on the following pages.

FTC ID Theft Affidavit

Instructions for Completing the ID Theft Affidavit

To make certain that you do not become responsible for the debts incurred by the identity thief, you must provide proof that you didn't create the debt to each of the companies where accounts where opened or used in your name.

A working group composed of credit grant- ors, consumer advocates and the Federal Trade Commission (FTC) developed this ID Theft Affidavit to help you report information to many companies using just one standard form. Use of this affidavit is optional for companies. While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it.

You can use this affidavit where a **new** account was opened in your name. The information will enable the companies to investigate the fraud and decide the outcome of your claim. (If someone made unauthorized charges to an existing account, call the company to find out what to do.)

This affidavit has two parts:

- ID Theft Affidavit is where you report general information about yourself and the theft.
- Fraudulent Account Statement is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (for example, drivers license, police report) you have. Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks of receiving it. Delaying could slow the investigation.

Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Please print clearly.

When you have finished completing the affidavit, mail a copy to each creditor, bank or company that provided the thief with the unauthorized credit, goods or services you describe. Attach to each affidavit a copy of the Fraudulent Account Statement with information only on accounts opened at the institution receiving the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. **Keep a copy of everything you submit for your records**.

If you cannot complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party.

Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

If you haven't already done so, report the fraud to the following organizations:

1. Each of the three **national consumer reporting agencies**. Ask each agency to place a .fraud alert. on your credit report, and send you a copy of your credit file. When you have completed your affidavit packet, you may want to send them a copy to help them investigate the disputed accounts.

Equifax Credit Information Services, Inc.
(800) 525-6285/ TDD 1-800-255-0056 and ask the operator to call the Auto Disclosure Line at 1-800-685-1111 to obtain a copy of your report.
P.O. Box 740241, Atlanta, GA 30374-0241 www.equifax.com

Experian Information Solutions, Inc. (888) 397-3742/ TDD (800) 972-0322 P.O. Box 9532, Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289/ TDD (877) 553-7803 Fraud Victim Assistance Division P.O. Box 6790, Fullerton, CA 92834-6790
www.transunion.com

2. The **fraud department at each creditor, bank, or utility/service** that provided the identity thief with unauthorized credit, goods or services. This would be a good time to find out if the company accepts this affidavit, and whether they require notarization or a copy of the police report.

3. Your local **police department**. Ask the officer to take a report and give you a copy of the report. Sending a copy of your police report to financial institutions can speed up the process of absolving you of wrongful debts or removing inaccurate information from your credit reports. If you can't get a copy, at least get the number of the report.

4. The FTC, which maintains the Identity
Theft Data Clearinghouse . the federal government's centralized identity theft complaint database . and provides information to identity theft victims. You can visit www.consumer.gov/idtheft or call toll-free 1-877-ID-THEFT (1-877-438-4338).

The FTC collects complaints from identity theft victims and shares their information with law enforcement agencies nationwide. This information also may be shared with other government agencies, consumer reporting agencies, and companies where the fraud was perpetrated to help resolve identity theft-related problems.

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Name _____ Phone Number _____ Page 1

ID Theft Affidavit

Victim Information

(1) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)

(2) (If different from above) When the events described in this affidavit took place, I was known as

_____
(First) (Middle) (Last) (Jr., Sr., III)

(3) My date of birth is _____
(day/month/year)

(4) My Social Security number is_____

(5) My driver's license or identification card state and number are_____

(6) My current address is _____

City _____ State _____ Zip Code _____

(7) I have lived at this address since _____
(month/year)

(8) (If different from above) When the events described in this affidavit took place, my address was

_____

City _____ State _____ Zip Code _____

(9) I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)

(10) My daytime telephone number is (____)_____

My evening telephone number is (____)_____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Name _____ *Phone number* _____ *Page 2*

How the Fraud Occurred

Check all that apply for items 11 - 17:

(11) . I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

(12) I did not receive any benefit, money, goods or services as a result of the events described in this report.

(13) My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were stolen lost on or about _____.
(day/month/year)

(14) To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

_____	_____
Name (if known)	Name (if known)
_____	_____
Address (if known)	Address (if known)
_____	_____
Phone number(s) (if known)	Phone number(s) (if known)
_____	_____
Additional information (if known)	Additional information (if known)

(15) I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16) Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

_____

_____

Name _____ *Phone number* _____ *Page 3*

Victim's Law Enforcement Actions

(17) (check one) I am am not willing to assist in the prosecution of the person(s) who committed this fraud.
(18) (check one) I am am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.
(19) (check all that apply) I have have not reported the events described in this affidavit to the police or other law enforcement agency. The police did did not write a report. *In the event you have contacted the police or other law enforcement agency, please complete the following:*

_____ _____
(Agency #1) (Officer/Agency personnel taking report)

_____ _____
(Date of report) (Report number, if any)

_____ _____
(Phone number) (email address, if any)

_____ _____
(Agency #2) (Officer/Agency personnel taking report)

_____ _____
(Date of report) (Report number, if any)

_____ _____
(Phone number) (email address, if any)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

(20) A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

(21) Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Name _____ *Phone number* _____ *Page 4*

(22) A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

I declare under penalty of perjury that the information I have provided in this affidavit is true and correct to the best of my knowledge.

_____ _____

(signature) (date signed)

Knowingly submitting false information on this form could subject you to criminal prosecution for perjury.

_____

(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

_____ _____

(signature) (printed name)

_____ _____

(date) (telephone number)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Fraudulent Account Statement

- Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company.** Include a copy of your signed affidavit
- List only the account(s) you're disputing with the company receiving this form. **See the example below.**
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original)

I declare (check all that apply):

As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

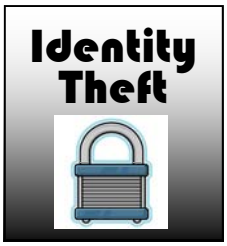
Creditor Name/Address *(the company that opened the account or provided the goods or services)*	**Account Number**	**Type of unauthorized credit/goods/services provided by creditor** *(if known)*	**Date issued or opened** *(if known)*	**Amount/Value provided** *(the amount charged or the cost of the goods/services)*
Example Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	Auto loan	01/05/2002	$25,500.00

. During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address_____

Account number _____



Section 2: Agents & Identity Theft

Always consult proper counsel such as an attorney or your carrier before using any course information in personal or client matters.

Agent Responsibilities

Agents are involved in the identity theft debate because under the definition of privacy legislation, you are referred to as a "financial institution" or "covered entity". As such, you must comply with sweeping and complex rules and standards under HIPAA, the Gramm-Leach-Bliley Act, the Federal Medical Privacy Rule, and possibly the new Patriot Act.

In addition, as a California agent you also must comply with the California Insurance Information and Privacy Protection Act (California Insurance Code Sections 791-791.27. So, you fall under "double" standards. For example, the privacy rules under HIPAA state that items such as a person's name, address, social security number and payment history are protected "health information" subject to an ***opt-in standard***. Therefore, HIPAA would prohibit any sharing of this information with a third party unless an express release is signed by your client. Many states, however, would consider these same items as "financial information" subject to ***opt-out standards*** where the sharing of client information is allowed until he "opts-out".

Can you see where disputes might surface? And, the penalties for a mistake or not complying can be stiff, ranging from $100 to $25,000 per incident; and, even prison terms of up to one year. Failure to provide a required notice is also a violation of agency rules subject to enforcement by your State Department of Insurance, and enforcement action under federal and state unfair trade practices rules. In addition, an individual whose information has been shared in violation of the rules may bring their own, private civil action against you.

For these reasons and more, this course will attempt to provide as much information as possible to help you comply with the many client privacy requirements

Keep in mind when reading this course, that even though you see a lot of legislative activity today, privacy laws in the United States are truly in their infancy. Experts say we are years behind most European countries. More rules can be expected.

The Biggest Threats & What To Do About Them

While a security breach can come at an agency or agent form many directions, the biggest threats occur from employee theft or mistakes, physical loss of a computer or back-up drive and loss or theft of a password. Some common sense precautions to consider to mitigate these security threats include the following:

PC's & Passwords

Implement firewall technology to protect your online access form unauthorized persons or viruses. Monitor systems traffic for unusual activity that indicates a breach might have occurred.

Implement the latest versions of anti-virus, anti-SPAM and intrusion software. Continually update them and activate updates wherever possible.

If your agency system is accessed wirelessly at remote locations be sure to be connected via a secure virtual private network (VPN). Do not use WEP (Wired Equivalent Privacy) encryption. It can be more easily hacked than the preferred WPA (Wi-Fi Protected Access) which is much more secure. Also, understand that when you access wireless you always run the risk of unauthorized people breaching your security.

Passwords need to be hidden and kept private. Avoid simple or obvious passwords or the practice of communicating them on a sticky note. ***Note:*** *Typical agency agreements make the* ***agent responsible*** *if an unauthorized individual gains access to the carrier's only system using an agent's password.*

Back-up

Decide whether you should host your own back-up system or rely on a more secure hosted (third party) data center employing 24-hour security, anti-spam, anti-virus and traffic monitoring.

Implement specific procedures for back-up, portable devices and removable media. Keep non-public customer information data and policy information off these devices wherever possible or encrypt them when they contain sensitive data.

Emails

Unsecured email, including policy forms and attachments, is very dangerous. A ***better choice is real-time interface*** where you are sending data via a secured server that is password protected.

Visitors

In this day and age, it's probably not a good idea to let customers roam through your office. Escort visitors throughout the office and know your night-time cleaning crew.

Office Security

Are your office doors and files secure? Add tamper-proof locks and dead-bolts where necessary

The Agent Employer

Many insurance agents run their own offices, and employ others to assist them. There are special privacy regulations that apply to the financial information collected by insurers and their agents, which are discussed later in this chapter. For now, we will look at some simple steps an agent who is also an employer can take to help prevent identity theft from occurring in his or her office. These tips can also be passed on to employers who ask the agent with help with identity theft risks:

Establish A Privacy Policy

The employer should write and implement a privacy policy. Doing this may help prevent fraud from occurring in the first place. First, the ways information is currently used in the workplace must be identified. Then, the employer must decide if any changes are needed in the way that information is handled.

A privacy policy generally includes: 1) what personal information is collected by the business, 2) how the information is used and disclosed, 3) how employees and clients are able to receive information about themselves that the business has, 4) what security measures are in place to protect personal information.

Agents may have to write and implement an "information security program," under the laws of the Financial Modernization Act. If the agent is exempt from this requirement because he or she does not supervise the office in which the agent works, the agent should strictly adhere to the privacy policy or information security program that applies to the agent's workplace.

Keep Personal Information Secure

Employers should keep filing cabinets locked that contain client records, employee personnel files and other sensitive information. Putting client and employee files away as soon as staff is finished with them, rather than stacking them in a "to be filed" pile, should be a rule that is enforced in the office. No one in the office should leave sensitive files out overnight when the office is closed.

Computer files should be password-protected, and access to computer and paper files with personal information should be limited. Only those in the office who have a reasonable business purpose for access to these files should be allowed to access them. Installing firewall software can protect computer files from being hacked into by an outsider

All social security numbers should be especially protected. It used to be that many businesses, including insurers, felt that social security numbers were the best identifier, since every individual's social security number is unique. This attitude and practice has been all but eliminated by legislation and public awareness of the risks involved in using social security numbers. In California, for example, recent legislation requires the elimination of public use of social security numbers in the workplace. However, social security numbers are still on most insurance applications, and many health insurers nationwide still use social security numbers to

identify a policy or certificate holder. So, businesses still have many records that include social security numbers, and need to make sure records with social security numbers are secure.

Employee information should be kept off of the business' website as well. Employees must also be prohibited from sharing sensitive information about the company or its clients over the Internet, such as in a chat room.

Shred Documents

Shredding documents containing personal information should be a normal corporate practice. Many businesses have made the mistake of thinking that taking these documents to the dumpster is enough protection from identity theft, and customers have suffered the consequences.

Be Careful Who Is Hired

Employers must check backgrounds of potential employees thoroughly. If using temporary help, the employer should talk to the temp agency about the procedures it uses to check out the people it sends out on jobs. If the employer doesn't feel comfortable with the agency's level of care, he or she should hire temps from an agency that he or she does feel comfortable with.

Make A Secure Place Where Employees Can Keep Personal Items

Employees should be encouraged to place purses or other items containing personal information in a locked drawer in their desk, or some other secure location.

Train Agent Employees

Training employees in all facets of the privacy procedures of the office must be a top priority of employers. Employees must be taught to ***keep files locked or password protected***. They must make sure to ***shred all appropriate documents***. Performing regular ***privacy policy training sessions*** to remind staff of the importance of privacy procedures is one method of helping employees to continually remember these responsibilities. If possible, limit employee access so that they can only view the information they need to do their job.

Protect Personal Information

It is important to keep personal information safe for many reasons, including regulatory responsibilities and care for the well-being and safety of employees. There is also a liability motivation: if an employee's or client's personal information is stolen from the workplace, the employer may be held responsible for the lost information.

If an employee is granted access to customer information from home using a home computer, make sure the entry of an individual password is required to gain access. Wherever possible, all online transmissions should be encrypted and secure.

Employees should be trained to log off their computer systems when they go to lunch, attend a meeting or leave in the evening. ***Terminated employees*** need to be cut-off from data access by ***using new passwords or authentication***.

An employer may be called upon to prove that he or she had reasonable safeguards in place to protect all personal information.

Identity Theft Occurrence Plan

It is also important for employers to have a plan set up in case ***workplace identity theft*** does occur. If fraud occurs, the plan can be used to quickly take the steps needed to prevent more fraud. For example, in California thieves broke into a state government computer database and proceeded to steal social security numbers, addresses, names, etc. However, the situation was dealt with efficiently and in a timely manner. The state's department of Consumer Affairs' Office of Privacy Protection quickly set up a toll free line for state employees so that they could directly contact the three major credit bureaus and post fraud alerts. Employees also received packets in the mail detailing ways to fight fraud. Such prompt action helped keep losses to a minimum.

Client Employees

Identity theft at work is becoming an increasingly common problem. Agents can pass on these tips to clients who are employees, as well as apply these tips for their own use in the workplace.

Employees should take the following steps:

- Make sure personal data is not left in the open. Lock up purses and remove bills that are to be mailed at lunch hour from the coat hanging on the back of the office chair or in the hallway. Clear desks of personal data and lock it when leaving.
- Be careful who accesses their computer.
- Not give out personal passwords.
- If the company computers do not have password protection, save vital information to disks and keep them in a safe place.
- Encrypt computer files.
- Leave all unnecessary credit cards at home.
- If co-workers ask questions about personal information, ask them why they need it.
- If there is a shredder available, use it. Personal information and sensitive information should be shredded.
- Ask to be allowed to use an alternative number to their social security numbers on as many records as possible.

Identity Theft at Home

So far, we've discussed how to help prevent identity theft as an employer and as an employee. We have also examined the responsibilities of insurance companies and agents in protecting the privacy of customers. Now let's turn to the steps that can be taken to prevent identity theft in the home. The agent who offers identity theft insurance should be familiar with these tips to help clients reduce the risk of being victimized.

File or Destroy Records

Sometimes people are not as careful as they should be with their personal records in the home. This can make them more vulnerable to identity theft. Unfortunately, even at home, personal records should be secured, and not left in the open, where unscrupulous visitors, repairpersons or contractors may find them.

Just as in the office, a shredder should be purchased, and all documents containing personal information shredded before disposing of them.

Limit Access

In protecting against identity theft, it also helps to limit access to personal information in as many ways as possible. Passwords should be used on computers and on other devices such as personal digital assistants to protect the information within them. Installing "firewall" software helps to protect data from Internet hackers and burglars. Using filing cabinets with locks to store personal files is also highly recommended.

Reducing the number of credit cards a person utilizes helps to reduce the amount of account information that can be accessed by thieves. Many people have more credit cards than they need, and may also save annual fees by getting rid of some of them. Using credit cards that include photos also provides protection from identity theft.

Pin numbers and other access codes should be memorized and not carried with a person. Memorizing these codes reduces the risk a thief will gain access to them. Another method that can be used to protect pin numbers is to simply put one's other hand up to obscure the view of anyone watching the numbers being entered. Using common names or numbers, such as the last four digits of a social security number or a mother's maiden name, as a pin code should be avoided. In addition, the longer the pin code, the more unlikely it is that a thief will hit on the right combination of letters and/or numbers if the thief tries to figure out the code.

Making sure to take all credit card slips and receipts and shredding them before they are disposed of also provides some protection from identity theft.

Mail should be sent from and delivered to a secure mailbox to keep it from being stolen. These days, many people drop mail to be sent directly at the post office, and use a locked mailbox at their home for mail delivery. Others rent a post office box and have mail delivered there for pickup. One bonus to this method is that mail may be available a day earlier than if it were

delivered to the home. If checks are being mailed, they can often be delivered to the local bank branch, where the owner can pick them up.

Paying bills at home instead of doing them at work and storing personal financial information on the company computer also helps to keep identity thieves from gaining access to an individual's information.

Pay Attention

Individuals can limit identity theft losses by staying alert. If statements do not arrive on time or are skipped completely, the individual should contact the creditor or bank as soon as the statement is missed. It is possible that someone has taken or redirected the individual's mail.

Credit reports should be ordered and reviewed at least once a year. This enables the individual to look over all credit accounts and catch unlawful behavior in a timely manner.

Bank statements should be opened as soon as they are delivered and examined for discrepancies.

Protect Social Security Numbers

If an individual's drivers license number and social security number are one and the same, he or she may be able to change the drivers license number. Some states have enacted privacy provisions that allow replacing the social security number on a license with a different number. The individual should check with the department of motor vehicles to see if this kind of change may be made.

Social security numbers should not be printed or written on checks. Social security cards should be kept at home, not carried in purses or wallets.

Credit Issuers' Role in Protecting Against ID Theft

More and more, credit issuers are being called upon to implement additional safeguards against identity theft. Consumer groups and regulators are focusing on practices such as issuing instant loan and credit card checks that have not been requested by the person to whom they are sent. Identity thieves can take these checks and cash them without the payee even knowing they were issued, until the payee starts receiving the bill.

Pre-approved credit card offers are also used as an avenue for identity thieves. The thief fills out the credit card application using all of the individual's information except the address, and receives the credit card. Again in this scenario, the victim does not even know the pre-approved offer has been made, since the credit issuer sent the pre-approval without the victim's request.

Although not all yet passed into law, several bills have come before Congress addressing the responsibilities of credit issuers in helping to protect against identity theft. It is likely that some of the requirements in these bills will be put into practice by credit issuers, even if the requirements do not become law, due to public pressure and increased theft losses incurred by issuers. Let's

look at some of the steps credit card issuers can take to help reduce the occurrence of identity theft:

Verify Address Changes

Since address changes are a popular method for identity thieves to gain access to personal information, credit card issuers are putting into place more steps for verifying address changes. A provision in a bill proposed in the Senate states that the credit card issuer should have to send verification of address changes to both the new and old address. The FACT Act, discussed in the next chapter, requires creditors to notify a consumer at both old and new addresses if a new credit card is issued or a credit limit increased within thirty days of an address change.

Paying Attention to Fraud Alerts

As mentioned earlier, some creditors do not check for or pay attention to the fraud alerts placed on credit reports. Recently enacted legislation calls for a penalty to be levied on credit issuers who extend credit after the victim has placed a fraud alert on a credit file.

Free Credit Reports

Several states have passed laws that allow consumers to receive one credit report from each bureau annually for free. Federal legislation now also requires this, making it easier for consumers to check their credit reports for evidence of fraud.

Freezing Reports

It has been proposed that consumers be allowed to stop all credit reports from being issued without their authorization. Some states have passed provisions that provide for this action under certain circumstances. The FACT Act allows for specific information on a credit report that is related to the identity theft to be blocked from a consumer report.

Removing Social Security Numbers

Because social security numbers are the key to gaining access to a person's identity, it has been proposed that the use of social security numbers be completed eliminated in the private sector. This step has not yet been taken at the federal level.

Verification of Identity

Another provision in legislation proposed before Congress requires that credit issuers use at least four pieces of information to verify identity as compared to that on the credit report. The FACT Act requires that creditors take reasonable steps to verify identity.

It can be expected that credit issuers will be more and more vigilant in extending credit, since the costs they are bearing because of identity fraud are increasing. However, each individual consumer should still take the steps necessary to protect themselves from this crime.

Agent Ethics & Integrity

Beyond your legal responsibilities, you have an ethical duty to protect your client's private information. You might take a keener interest in this issue if you knew how you could be effected when a transaction goes bad or client conflict arise.

Doing the right thing in the insurance industry comes under the banner of market conduct and fiduciary responsibility. A few years ago, no one knew what ***market conduct*** meant in the insurance industry. ***Fiduciary violations*** were something bad that happened . . . usually to the other guy . . . when he got caught doing what everybody else was doing anyway. And, the consequence was typically a slap on the wrist or a license suspension for a few months.

Today, however, the stakes are higher. There are class action suits and negligence and fiduciary ethics claims filed against insurers and agents alike amounting to millions of dollars for a variety of legal conduct and ethical violations.

Of course, lawsuits involving agents is nothing new. You can find court cases dating back to the early 1800's. What is different nowadays is the trend toward fiduciary responsibility. In essence, the courts and clients are viewing agents as ***more than mere salesmen***. Recent cases, for example, lean toward the legal theory that agents, as insurance professionals, ***should have known*** something was wrong compared to years ago where agent liability was generally limited to issues of ***outright negligence***. Back then you had to do something really wrong like forgetting to submit an application or back-dating a policy to file a claim to land yourself in court.

Consider two examples: In Southwest v Binsfield (1995), the agent was sued because he ***should have known*** that a specific coverage option was important to the business he insured. In Brill v Guardian Life (1995) the agent ***breached his fiduciary duty*** by not using an ***optional*** conditional receipt. Would you consider these to be breaches of ethical duty or malpractice? In today's litigious society they are nearly one and the same. Can you imagine the consequences of a wide-scale identity theft traced to your office?

What has happened is an expansion of a decision by some judge 30 or 40 years ago. Dozens of cases have twisted and distorted the original intent of the law to the point where the level of agent duty has notched higher and higher. This is known as the ***legal precedent theory***. In a nutshell, because our legal system makes legal decisions based on precedents, it is destined to constantly expand. Each decision in the chain sets the stage for the next step of expansion and attorneys get better at convincing juries that agents should be held more accountable.

Agent Misconduct & Identity Theft

Identity theft in the insurance arena is relatively new. However, this fact does not preclude agents form taking advantage of their position to marshal personal, financial and medical information. In other words, some of the problem stems form the agents themselves. The agents in the following examples breached their ethical and conduct duties to their clients and carriers: It is hard to imagine how they believed they would escape detection and the small

amount of money they risked everything to make. All were caught and are paying a heavy toll for their actions.

Drugs Lies and Life Insurance

This is a bizarre case involving an insurance agent and criminal drug traffickers. Dozens of conspirators got "victims" hooked on cocaine, crack and heroin. Stealing their personal identity information, they proceeded to take out life insurance policies, through a less-than-ethical agent, paying the premiums with drug sale money and making themselves beneficiaries. Given their circumstances, many of the unfortunate victims had low life expectancies yielding many settlements for the perpetrators. Federal prosecutors are on the case.

Nursing Home Victims

A licensed agent somehow retrieved / stole identity information from several elderly nursing home patients. He applied for additional coverages in their name without their knowledge and permission to reap insurance commissions. One of the victims was deceased, yet the unscrupulous agent applied for additional health coverage in his name anyway. Local authorities are doing their thing to bring him to justice.

Secret Policies For Commissions & Bonuses

The secret of how a top-selling agent maintained her elite standing is out. She purchased secret policies on 52 different people. Most she did not know, but she was someone able to access enough personal identity info (names, Social Security Numbers, driver license numbers, etc) to apply for policies in their name. She paid premiums for many policies out of her own pocket. Commissions and bonuses, however, totaled more than the premiums netting a small profit. It also netted her 52 counts of identity theft and 52 counts of forgery. There have been other twists on this scam where agents have purchased policies and found holes in the system that allowed policies to go unpaid for years while still collecting commissions.

Supplemental Policy Scam

An agent earned advanced commissions from 18 bogus supplemental medical policies by forging signatures and personal information for people he did not know. Using his own bank account for automatic premium withdrawal, the carrier noticed a high number of his applications were being cancelled for non-payment of premium. Criminal charges are pending.

Low Income Victims

An agent targeted low-income individuals convincing them he had a plan to lower their monthly mortgage payments. After gaining their confidence, he secured a voided check and personal information to buy high-commission life insurance policies in their name without their knowledge. In many cases, monies deducted from the victims' accounts was used to pay premiums and NOT to reduce their mortgage payments. The insurance commissioner has fined the agent $40,000 and local district attorney secured a five-year prison sentence.

Senior Victims

An agent stole identities of more than 100 seniors to collect commissions on bogus Medicare-advantage policies. Her profit? Just $7,000 for a lot of work and certain prison sentence. It doesn't make sense. Why not invest the same time to farm new clients and sign real people?

Dumpster Records

This agent discarded more than 1,000 insurance business records and other insurance transaction documents into an unlocked garbage dumpster. The documents contained clients' personal information, including client names, Social Security Numbers, driver license numbers, bank account numbers, credit card numbers and credit card expiration dates. Fortunately, alert citizens alerted authorities before any known identity theft occurred. The agent, however, was served with a cease and desist order and fined $11,000 for violating the state's Identity Theft Protection Act guidelines for businesses and organizations that collect personal data.

Other Court Cases

Agent accountability can come with a hefty price tag. Consider the following court cases where the actual dollar losses incurred by client victims was extremely low compared to the ***high punitive damages*** levied against agents and their insurers:

State Farm v Grimes	*$1,900 Actual losses*	*$1.25 Million Punitive Award*
Independent v Peavy	*$412 Actual losses*	*$250,000 Punitive damages*
National Life v Miller	*$258 Actual losses*	*$350,000 Punitive damages*

As you read these amounts you may be thinking that the damages were high because insurance companies have ***deep pockets***. They can afford to pay these sums of money, which is why juries awarded them. That's true, but, you must also keep in mind that virtually every agency agreement in existence, including the one you signed, has some kind of ***indemnification clause*** or wording that entitles the insurer to demand reimbursement from you, the agent, for malpractice, negligence or action leading to a jury award, including identity theft you exposed. In other words, if you have a contributing exposure to a problem that caused the insurer to pay-out big bucks, you probably have the same exposure when the ***insurer*** comes after you personally!

Courts make decisions about your behavior based on past court cases. So, as you read through this course and see an old court case, don't be fooled into thinking it can't apply to you. In Daniel v. Brickman (1998), for example, a court made a decision that effected an insurance agent based on a trial decision made in 1917!

Also, don't assume that a ***casualty*** court case has no application to you if you sell ***life insurance*** and vica versa. In fact, in National v. Valley Forge Life (2002), the actions of a ***real estate agent*** were analyzed in a decision against an ***insurance agent***! So, many legal matters concerning duties or negligence are fully portable and transferable between classes of agent.

You may also read about cases where the agent "won" the case. Well, don't forget, he may have escaped the huge cost of a trial or punitive damages, but attorney fees alone cold amount to the same you might pay for your kid's entire college education.

Finally, be aware that some court decisions appear to “clear” the agent of wrongdoing. These decisions can result from issues extraneous to the case or a technicality. But, there is always the possibility of an *appeal*. In fact, many of the cases we researched were appeal cases that initially dismissed the agent of any wrongdoing. A different judge and jury can reverse these decisions and find you liable even if you prevailed at the original trial.

Being Ethical

Being ethical is indeed professional but the gesture goes beyond the mere compliance with law. It ***means*** being completely honest concerning ALL FACTS. It means more than merely NOT telling lies because an incomplete answer can be more deceptive than a lie. It means more than being silent when something needs to be said, because saying nothing can be the same as a lie. Take the case of Bell v. O’Leary - 1984). An agent took an application for flood insurance but failed to notify the client that his mobile home was located in unincorporated areas that were ineligible for any coverage under the National Flood Insurance Plan. A loss occurred and the agent was sued. The courts determined that the agent had superior knowledge and failure to give the client a complete answer about the unavailability of coverage took precedence over the fact that coverage for the property was not available from anyone.

Someday, it may be real important for a court and jury to hear that you have a history of serving clients without consideration for how much commission you made or how busy you were, i.e., you are a person with good ethics. In Grace v. Interstate Life - 1996, an agent sold his client a health insurance policy while in her 50's. After the client reached 65 he continued to collect premiums despite the fact that Medicare would have replaced most of the benefits of her policy. The court considered the agent’s lack of duty to notify his client a serious breach of ethics.

Perhaps this whole issue of ethics can be summed up in the very codes of conduct now in place for members of organizations like Registered Preferred AgentsJ, The American Society of CLU and ChFC, Chartered Property and Casualty Underwriters the International Association of Financial Planning and the Million Dollar Round Table. We summarized many of these in the box on the next page titled simply . . . ***An Agent’s Code of Ethics***

Ethics From The Start

Instilling ethics is a process that must start ***long before*** a person chooses insurance as a career. It is probably part of the very fiber that is rooted in lessons parents teach their children. So, preaching ethics in a forum like this course of study may not be incentive enough to sway agents to stay on track. It may be easier to explain that honesty and fair play could mean greater sales and lessen the possibility of lawsuits.

Perhaps part of the blame for modern-day ethical indiscretions is the complexity of financial products and the intense competition among sellers and agents. Both make it harder for consumers to understand what they want or need and easier for an aggressive salesperson to mislead them. Consider Cunningham v. PFL Life - 1999. Agents, who promoted themselves

as “experts” with superior knowledge, misrepresented the life insurance policies they were selling as investment vehicles. Consumers were easily convinced that the papers they held were investment contracts. The courts found the insurer liable for reckless and wanton failure to train and supervise its agents. The case did not disclose if any suits against individual agents were launched by the insurer.

Some believe that the ethics problem reflects our current culture that glorifies short-term success at all costs. This includes awards for the most sales in a given period of time as well as “golden boy” stories of the entrepreneur who goes from lonely computer geek to multi-millionaire from a single idea. Neither of these events is meant to say that these individuals accomplished their feats in an unethical manner. It simply ***raises the bar*** for those who follow them. If those who follow have inadequate skills and work habits, they could employ less than ethical means to reach the same goals.

Ethics For Life

The insurance industry can do a lot more to promote ethics-building habits. At the MONY Group, for instance, building a relationship in sales and marketing is emphasized with a program called ***Client for Life***. Its premise, “When you constantly exceed the needs and expectations of your clients, you’re doing the right thing“. Sales tools such as reports and newsletters are used to educate clients in a non-threatening and highly personalized manner. ***Long-term success*** is closely associated with building ***long-term relationships*** with clients rather than a quick sale. The results may vary from agent to agent, but a surprising benefit seems to be a ***loyalty factor*** where more than 70 percent of sales comes from existing policyholders or their referrals.

Ethics Defined

Just what is ethics? A simplified definition of ethics is a ***set of values*** that constantly guides our values. These values are typically ***aligned*** with what society considers correct and positive behavior within legal boundaries. Ethics is also the ***balancing*** of an individual's good with the good of the whole. Let's say you develop a seminar series on "asset protection". At the event, you have a person pass around a clipboard asking people if they would like to be informed of future seminars. The real purpose of this exercise, however, is to create a mailing list to market insurance products. Smart marketing? Or, breach of ethics? Are you really concerned with your clients education (the whole) or only what you will get out of their business (the one)?

Balancing the good of the one with the good of the whole is not as easy any more. The whole that we have to consider is everybody, not just a competing agent down the street or in the next town. Survival is important, but not at any cost. True survival requires long-term, successful relationships with customers and companies, as well a co-workers and competitors. When people do not understand their role in the "whole" and are completely self and survival oriented, it throws the ethical system we once knew out of whack.

How can you stay on track? Most important is that you know your personal core values and the values that your company or agency stands for and then live and work congruently and consistently with those values. The people will know you as a person of integrity. And, with integrity comes trust.

The authentically ethical person in our seminar example would have simply disclosed the purpose of the clipboard or simply buy a mailing list from someone else. Respect for privacy would be honored and remembered.

How can agents develop a sense for long-term ethics? The best way is to fully understand what ethics is and the many levels it plays in your career. Following are some special areas of interest you should know about ethics:

Shades of Grey

One of the problems with ethics today is that we have so many different mores or values that guide our society. The values that guide each individual and/or company can vary tremendously, therefore an individual or company may be ***ethical*** according to their values and not to yours or the definition above. Several major shifts in right or wrong standards means that we are faced with more and more gray areas in our personal and professional lives. The shifts are occurring at such a pace that they may even hinder our ability to cope and process the changes.

Take the example of two agents who met with numerous company officials at Universal Manufacturing Company ("Universal") for the purpose of securing permission to offer interested Universal employees a "unique," "local" product. The agents explained that purchasers of the product would receive allegedly ***better coverage*** than that provided by their current insurer which issued the policies then-held by many employees.

More specifically, the agents explained that what they were offering was not an ordinary life insurance policy; rather, it was a ***supplemental retirement program with a death benefit*** and

AN AGENT CODE OF ETHICS

In all my professional relationships, I pledge myself to the following rules of ethical conduct:

- I will make every conscious effort to help my clients in a manner in which I would want to be helped myself.
- I will maintain the highest standards of professional competence and integrity and give the best possible advice to clients.
- I will offer advice only in the areas I have competence and within the scope of my licensing.
- In a conflict of interest situation, the interest of the client shall be paramount. I will always place the interest of clients above my own.
- I will take responsibility for knowledge of the various laws and regulations affecting my services.
- When approaching prospective clients, I will immediately identify myself (verbally or in writing) as an insurance agent / company and disclose the product I am selling.
- I will avoid sensational, exaggerated and unwarranted statements. My proposals and quotes will be clear so clients may know exactly what is being offered and the extent of their commitment they are considering.
- I will make full and adequate disclosure of all facts necessary to enable clients to make informed decisions.
- I will constantly improve my professional knowledge, skills and competence.
- I will be truthful about client testimonials and endorsements.
- I will hold all business and personal information pertaining to my clients in the strictest confidence.
- I will maintain a professional level of conduct in association and when referring to peers and others in my industry. And I will be fair in any product or company comparisons.
- I will conduct my business in a way that my example might help raise the professional standards of insurance agents everywhere.
- I will cooperate with others whose services are constructively related to meeting the needs of my clients.

an "immediate cash benefit plan" containing a $ 1,000 "check" which, in the event of an insured's death, could be cashed immediately to pay for such burdensome expenses as funeral arrangements. Of critical significance, the agents assured that employees who decide to enroll in this "retirement program": (1) could allow their current policies to lapse, and (2) would be covered (insured) "immediately" and unconditionally upon completing an application and "upon signing . . . the[ir] payroll deduction card."

In essence, the agents guaranteed all-important ***risk aversion*** and ***peace of mind***. This was critical to those who were currently insured and were concerned about being without coverage once they allowed their policies to lapse. The so-called $ 1,000 "check" was not actually a check which can be taken to a bank and cashed. The only purpose it seems to serve is as a misleading gimmick to promote sales of the policies.

Clearly this is a ***shade of grey*** bordering legal issues like misrepresentation and fraud. The practice, ***unfortunately***, is widespread.

Moral and Market Values

The American economy depends on ethical standards upheld by responsible business leaders. Unfortunately, this unwritten rule was violated in recent ethics scandals occurring in many corporate boardrooms. Respected companies lost credibility and innocent investors lost millions in the late 1990's and early 2000's. Cheating became rampant because it was the norm. It was no longer seen as wrong. In fact, at the peak of the problem, much of our economy resembled a giant pyramid scheme, taking in money from new suckers to pay those who invested earlier. A so-called ***bubble economy*** developed where businessmen willing to gamble with other people's money were rewarded handsomely. Stock prices were rising so fast that if you cut corners to meet projected numbers, you probably thought you were doing your shareholders a favor. And, there was always new money pouring in to make up the difference.

The insurance industry is not without its own horror stories. Take the case of Joseph and Annette Cooper. They purchased a "vanishing premium" life insurance policy insuring the lives of himself and his wife Annette Cooper.

Agents Steinhardt and Fish , whom Cooper had known for many years, and considered to be trustworthy friends, told Cooper that they were ***highly skilled insurance experts*** who understood complex insurance projects, and encouraged him ***to rely on their expertise and prior relationship of trust in choosing a policy***. Steinhardt and Fish recommended a $ 1 million Berkshire "disappearing premium" policy, and told Cooper he would have to pay the annual $ 9,000 premium for nine years. "Neither Steinhardt nor Fish showed him a 'Supplemental Footnote Page' or anything else that indicated the disappear-year was not guaranteed." To the contrary, they specifically told him that he would ***not have to pay any premiums beyond the illustrated disappear-year***.

Even though Cooper thought it was ***too good to be true***, he decided to buy two policies, one for the Trust, with a $1.5 million death benefit, and a second, with a $1 million death benefit for the Associated to endow a charitable fund.

About six years later, the Coopers learned for the first time that they would have to pay premiums for many years longer than the insurance agents originally represented. Fish disclosed this to Cooper during presentation of a "Life Insurance Policy Reprojection" as part of a meeting that he scheduled to sell them additional financial products.

The Coopers asserted that the ***assumptions*** underlying Berkshire's illustrations of the premiums that the Coopers would have to pay were inconsistent with Berkshire's own internal forecasts and estimates, and were based on abnormally high dividends that, to the defendants' knowledge, Berkshire could not sustain. If the illustration had been based on Berkshire's real investment earnings rate, the Coopers claim, it would have shown the "disappear year" to be ***later than*** the ten years represented to Cooper.

An "expert in the field of life insurance and actuarial science was brought in to testify to this conclusion. His opinion was that the ten year premium illustration was ***materially misleading*** at the time it was used to sell the policy to the Coopers because, contrary to Berkshire's claim, the illustration ***did not accurately reflect current company experience***. He also stated that the agents should have known that the ***disappear date*** portrayed in its sales illustrations were ***false*** and that the actual "disappear date" would be later. . . . Based Berkshire's Net Investment Yield during the five years before the Coopers purchased their policies (i.e., 1985-89). In fact, it was steadily declining. Thus, it was not realistically possible for Berkshire to continue paying dividends as represented in the illustrations while increasing their book of business. In short, Berkshire and the agents knew or should have known in 1990 that the Coopers would have to pay more premiums than illustrated.

The court agreed that a reasonable jury could find that the illustration constituted a materially misleading and inaccurate representation regarding the prospect of a ten year "disappear date" for the Coopers, and that the Coopers ***reasonably relied*** on that misleading illustration in deciding to purchase the Berkshire policy.

In insurance as well as the corporate world, people who rely on your word can be sucked in during times of market sensitivity. When interest rates are crashing down, for example, people will be intently interested in your interest rate programs. Some agents could take advantage of this enthusiasm. What about hard markets where a certain sectors of the industry refuse to insure. Insurers often play the game by offering higher commissions on the less attractive programs. The hope is that it does not get out of hand. During the bubble period, for instance, the economy resembled a giant pyramid scheme, taking in money from suckers to pay those who invested earlier.

Will tougher laws and longer prison sentences be a deterrent. It can't hurt. But, the fact is bubbles burst quicker than a business climate can change. If a crooked practice doesn't pay off, a lot fewer people will take the risk of using them. So, the real challenge is to create a new business culture that matches the market. Think about a system that rewards and reinforces the honest and careful agents and businessmen just like the bubble economies made heroes out of the gamblers.

Moral Compass

During times of fundamental change, values that were previously taken for granted may be strongly questioned. These are the times when the attention to business ethics is critical. Leaders, workers and agents must sensitize their actions -- they must maintain a strong moral compass.

John Kennedy Jr's last flight went wrong because he lost sight of land. In the growing dark around him, the horizon line became blurred and he became disoriented eventually flying his place right into the ocean. When nothing is stable or dependable, you also can lose your own sense of moral direction. When it happens, you start accepting ambiguity as real. You begin making up your own rules. You cut corners. This is exactly how things started going bad at Enron. Accountants simply made-up their own accounting standards. They lied, cheated and waffled because it was to their economic advantage. Over time, they began justifying their unethical behavior as acceptable.

How can you keep this from happening to you? You can have a strong, unfailing sense of what is right and stay focused on it at all times. It's called ***integrity***. When you have it, it allows others to trust you, even when things go bad.

Kim Cameron, Professor of Organizational Behavior at the University of Michigan, says that it is not enough to simply encourage ethical behavior, honesty and integrity because these concepts in themselves imply an ***absence of harm***. A ***strong moral compass*** means that you strive for ***virtuousness*** where your actions rise to doing good, honoring others, taking a positive stance -- i.e., . . . "***behaving in ways where self-interest is not the driving motivation***."

Too soft and fuzzy for you? Well take note, Kim's research proved that businesses with high scores on virtuousness significantly outperformed those with low scores. ***It pays to have a strong moral compass!***

Example: You investigate two proposal quotes for a client. Proposal A is the least expensive policy, but it meets the client's needs. Proposal B also meets the client's needs with a few bells and whistles added at a much higher premium. And, because it includes significant exit penalties, it also pays a much higher commissions. The client relies entirely on your recommendation and doesn't have a clue what a competitive premium might be for a comparable policy. What do you do? As an agent with a strong moral compass, you present Policy A, but explain the options available on Policy B and the fact that premiums and commissions are higher. If the client wants Policy B the honest response is that it is not the one you want him to buy as long as Policy A meets his protection needs.

This is a simplified example for sure, but you get the idea. You are legally able to sell either policy but what is the fairest deal for the client? Truly honest and ethical people live by the choice to do what is right, even when it is not pleasurable. This is how reputations are built. And, regarding reputations, ***Alan Greenspan*** summed it up quite nicely . . "Your reputation is your stock and trade. If you do something to undermine that, then you very well may not have a company any more."

Moral Distress

Have you ever thought about why people make bad decisions? One reason is dissatisfaction with your work or how about near impossible objections. When either one of these occurs, a person experiences growing pressure to engage in unethical behavior. You are left in a situation where every decision must weigh your own survival against the care and attention you give your client. The end results is that shortcuts will be taken or you become frustrated, resentful, angry or guilty about your bad decisions.

What can you do?

Stakeholders: Experts suggest that, among other things, you adopt a long-term stakeholder mentality, and, to be ethical under social justice theories you should be fair to all ***stakeholders***. What does this mean? A stakeholder is anybody that can be affected by your actions. Your client is a stakeholder in that he depends on you and your insurance products to protect is economic well-being. Your insurer is a stakeholder in you representing product fairly and within the scope of the law. The shareholders who have invested in the insurance company are also stakeholders and when it comes down to it, you are a stakeholder yourself. That's right! You owe it to yourself to survive in your chosen field. And, as we have already described, the best way to do this is long-term, with integrity and respect for others and all stakeholders.

Remember, customers ultimately pay your commissions and insurers enable you to make a living. That's something that should be important to you. So, how could you be a bystander and watch either of them be injured in any way by your actions?

Pace Yourself: Another way to reduce moral distress is to operate at a reasonable pace. We have already explained that when you cut corners it promotes unethical practices. For instance, if you fail to budget time to read a client's policy, they go out without being reviewed raising ethical questions and moral distress. What about when you forgot to get a client's initial on an application. It's awful tempting to sign it yourself when you know the client will approve it anyway rather than drive 30 miles back out to meet the client a second time. Again, moral distress raises its ugly head. Of course, the solution is to allow more time the first time out. But, this will mean less production which creates economic stress. At times like this, you have to assure yourself that you are in this for the long-term. Being genuine and ethical means that you live by the choice to do what is right, even when it is not pleasurable. You could also look at it in more positive terms. Why not make a ***client for life*** by taking that 30 mile drive and explaining why you did it!

A Tolerance For Problems: When you succeed at something, it's normally because you are doing something that other people do not want to do. In a sense, you have to "tune-up" your instincts to be ***satisfied*** at meeting objectives that others find hard to take or when people don't want you to succeed. What does this have to do with moral distress. A lot, because you can reduce your level of moral distress by increasing your tolerance for problems. Think about it. You can convince yourself that external forces are never-ending anyway, so there is no reasons to sweat it so much. The fact is, you're in the problem solving business and you're a pro! Just remember the immortal words of Saturday Night Live's Rosanna Rosanna Danna -- "It's always something!"

Loss Control

Being ethical does not mean you have to be the town's whipping boy. Use some of your own sales logic to understand this one. You've probably said this to a client or two . . . "People don't buy insurance and pay premiums so they can run in to every station wagon simply because they hate station wagons. In fact, if they own a small car, they are likely to ***avoid*** station wagons".

In a similar vein, you need to avoid problems that could cause major financial havoc to you and other stakeholders. When you do, your levels of moral distress will be lower. Of course, this is easier said than done, since there is NO foolproof method to avoid a conflict. There are, however, some steps that agents can use to help reduce the possibility of liability developing.

- Know your basic ***legal responsibilities*** as an agent and only exceed them when you are absolutely sure what you're doing. Then, pull out your agency agreement and ***read it . . . right now***!!! And, when you decide that you want to be more than an agent, i.e., ***a specialist or expert***, understand that it comes with a high price tag -- ***added liability***. Also, make sure you are complying with basic license responsibilities to keep you and your company from becoming a commissioner's target for suspension or revocation.

- Learn from other agent mistakes. The best school in town is the one taught by agents who have already had a problem. Study their errors, learn from them and make sure you don't repeat them. Countless lawsuits, for instance, surface due to something an agent wrote down in an application causing the policy to void or a claim denied. The insured typically denies they responded in that manner. If applications were made out in an insured's own handwriting, however, there is little they can say.

- Be aware of and avoid current industry conflicts that could develop into problems for your agency, e.g., mold prevention, viatical settlements, life insurance acting as retirement plans, etc. There are hundreds of professional industry publications and online sources that will help you keep abreast. Once you are aware of a potential problem, take action to make sure it doesn't end up at your doorstep.

- Maintain a strong code of ethics. As you will see from our discussion of ethics, you don't need a list of degrees or designations to be ethical. Simply be as honest and responsible as possible.

- Be consistent in your level of "due care". Adopt a code of procedures and create an operations manual that forces you to treat client situations the same way every time. Courts and attorneys alike are quick to point out any inconsistency or lack of standard operating procedures where the client with a problem was handled different than another client.

- Know every trade practice and consumer protection rule you can and act within standards of other agents. The violation of "unfair practice rules" is a really big deal to lawyers. They will portray you as something short of a "master criminal" for the smallest of violations, especially if they are outside the standards of others working in your same profession.

- Use client disclosures whenever possible. There is nothing more convincing than a client's own signature witnessing his knowledge of the situation or a note in an application offering an explanation. And while we're on the subject, ***spend more time with client applications***. The information provided in an application is serious business. Mistakes, whether intentional or not, can void a policy or reduce benefits and lead to a lot of trouble for your client and you. Use mini-disclosures to evidence a position and reasoning. For instance, assuming your state regulator and company approve, the applicant could be asked to write "I have read everything on this page. The answers are true".

- Get connected to the latest office protocol systems. The ability to access a note concerning a client conversation or the way you "package" correspondence can make a big difference in the outcome of a claim or avoiding one at the outset. You want a system that will produce solid evidence not "hearsay".

- Maintain and understand your errors and omission insurance. This policy is your "first line of defense", but know its limitations and gaps.

Ethics From Education

The customer can't understand what the salesperson can't explain. Further, a customer who understands a product is much less vulnerable to deceptive selling. Both statements stress the importance and need for more education. A recent study by the Insurance Institute found that four out of every five people don't understand their insurance policies. And, if the agent doesn't understand his product the company and client are at risk. Agents end up concentrating on a "comfort zone" product or service B even if it is not the most appropriate one because he is uncertain about newer, more complex products.

Constant training is the answer from the company's perspective, as well as making a long-term effort to ***demystify products***. One solution is the translating of legalese into easily understandable, everyday English. This includes brochures, advertising, applications and the policies themselves.

The process of educating ethics is also the responsibility of our schools. Currently, there is a glaring lack of attention to the selling disciplines. Besides learning the nuances of every product and the marketing behind them, young people could be taught the importance and responsibilities associated with being a salesperson. Like the athlete who trains long hours to prepare for the moment of action, salespeople can be groomed to do the right thing.

Misuse of Position

What are you doing that might ***influence*** people in an unfair or abusive manner. For example, do you represent yourself as an ***insurance expert*** when you are not? Do you claim to have special ***insurance knowledge*** when you don't? The point is, when you ***disguise*** your ***actual position*** you deceive clients with the intention of influencing their purchasing decisions. It is certainly unethical and may be illegal.

Here are examples of several insurance conflicts that developed because of influence.

Campbell v. Valley State Agency

The client was a founder and director of a bank that owned and operated an insurance agency. The agent was also manager of the agency and knew that client was a millionaire. Agent obtained automobile coverage for client in the amount of $100,000 per person and $300,000 per occurrence. A major accident occurred which exceeded the limits of the policy. The client sued agent for these additional damages. Although the case was scheduled for a new trial the original court found that a jury could have found the agent had a duty to advise the client about his liability coverage needs due to the special relationship that existed. Thus, the agent was potentially liable for the damages that exceeded policy limits.

Europeon Bakers v. Holman

After handling the client's insurance needs for approximately six years the agent proposed that the client change its business interruption coverage to a policy that included a coinsurance provision. The insured accepted the proposal but found that it covered only 28 percent of his loss caused by the interruption of business when an oven accidentally exploded. The agent was sued for negligence by the bakery which was seeking the full amount of the lost business production it suffered. The court held that the agent was responsible since he had a duty to advise the client about its business interruption needs, especially since agent held himself to be an "expert" in this area and client had relied on him in the past.

Seascape v. Associated Insurance

Agents held themselves out to be "professional insurance planners". They had served client for several years. Client came to them to get specific advice regarding "seawall insurance". Agents advised client that this type of insurance was NOT available to them. Later, a storm damaged client's seawall and clients learned that seawall insurance could have been purchased. Clients sued agent alleging that their relationship was such that agent owed a duty to exercise reasonable care in rendering advice on insurance matters. The courts agreed.

Sobotor v. Prudential Property & Casualty

Client requested the "best available" auto insurance package from agent. Coverage options for uninsured motorist were NOT discussed and this coverage was NOT included in the policy as issued. Subsequent client losses prompted a lawsuit. The courts sided with the client by determining that even though this was a single insurance transaction between agent and client, a fiduciary relationship existed because the agent held himself out to have special knowledge in insurance and client, who knew nothing about the technical aspects of insurance, placed his faith in agent. Also, by asking agent for the "best available" package client put agent on notice that he was relying on agent's expertise to obtain desired coverage.

Wright Bodyworks v. Columbus Agency

Client requested business interruption insurance from agent. Agent agreed to adequate coverage based on agent's yearly inspection of client's books to determine premium. Coverage was placed but agent calculated premiums based on client's "gross profits" rather than it's "gross earnings". When a major loss occurred the client was underinsured in a big way. The

courts determined that the agent assumed a “dual agency” role because of his special arrangement to audit the books and the fact that agent advertised himself as an expert in this field of insurance. The insurance company paid their limits and the agent was liable for any deficit.

These court cases offer some evidence that many agents might be better off to accept and position themselves as ***insurance agents***, not a “special consultant” or "expert". Customers can learn to accept that ***you are who you are*** without titles that could, influence, mislead or instill false promises.

This is the basic concept behind the ***Preferred Registered Agent™*** proficiency designation. The Preferred Registered Agent is an insurance agent who always practices due care, yet operates within the bounds of agency. They accurately describe policy options that are widely available but refer out if an inquiry is beyond their scope of duties B even if they know the answer. They do not profess to have expert status but know their products as good as they can. Their goal is simply to be the most responsible agent possible. ***Preferred Registered Agents***™ are bound to a strong code of ethics ***and*** a code of procedures.

Ethics Are Not Laws

Many agents believe that ethics and the law are the same. It is important to realize that ***ethics are not laws***, ***yet they can be guided by laws***. Proof of this exists in the fact that you can be unethical yet still operate within limits of the law. A perfect example of this is the insurance client who fears he has physical problem yet he is allowed to withhold disclosing it on an application. He has no duty to disclose his "fears" of a medical condition. It's legal, but not too ethical.

Laws in the United States are abundant, growing in numbers every day. The courts attempt to legislate protections from those without values or with values in opposition to what most of us would consider right and wrong. We have more laws than any one lawyer can ever know. And more and more lawyers seem to be necessary to handle the litigation that results from what seems to be a trend in "making others pay".

Privacy

Protecting a client’s privacy is an ethical responsibility as well as an area of increasing liability for insurance agents. The concern by clients is that highly personal health and financial information you collect in the process of selling insurance will get in the hands of groups who might use this data to exploit them. As a result, new legislation has passed that requires certain disclosures be made to your clients whenever non-public (personal) data is being shared with other parties. Also, they must be given the opportunity to restrict its use.

The following case demonstrates how privacy issues can be violated and taken to the extreme. You won't believe how the sides get whipped into a frenzy with accusations like wiretapping and review board shams.

Richard Fraser joined Nationwide Insurance as an employee in 1986. Fraser later signed the standard Agent's Agreement to become an exclusive career agent with Nationwide.

Fraser also leased computer hardware and software from Nationwide for use in the automation of his office and insurance business. The lease agreement explicitly stated in the Preface that the Agency Office Automation ("AOA") system "will ***remain*** the property of [Nationwide]." Further, anytime someone logged on to the AOA system, a notice appeared on the screen that said:

Please note: for everyone's mutual protection, your AOA SYSTEM, including electronic e-mail, MAY BE MONITORED to protect against unauthorized use.

Problems developed when Fraser and other Nationwide agents met to form a Pennsylvania chapter of the Nationwide Insurance Independent Contractors Association ("NIICA"). NIICA had previously been in existence for some years in other states. Nationwide refused to officially acknowledge NIICA. Fraser was elected to an office of the local chapter. He was also asked to create and write a chapter ***newsletter***, which became known as The Pennsylvania View.

Fraser raised some of the business practices believed to be illegal with Nationwide's Office of Ethics. Thereafter, Fraser initiated a complaint with respect to these practices with the Pennsylvania Insurance Department and the Pennsylvania Legislature. The agents' ongoing efforts to report these practices resulted in media publicity. Nationwide was aware that Fraser and other NIICA members were reporting business practices to state authorities. Nationwide was forced to enter into a series of consent orders with the Pennsylvania Insurance Department, by which Nationwide paid a fine and agreed to cease the business practices about which Fraser had complained. The Pennsylvania View publicized Nationwide's concessions under the consent order.

A short time later, Nationwide drafted a ***warning memo*** headed "Inappropriate Communication" to the entire agency force, including Fraser. The memo stated that Nationwide was aware of communications with the Pennsylvania Insurance Department and the State Attorney General. Citing examples of such communications, the memo asserted that many of these communications included "false statements or unsupported allegations that Nationwide has or intends to violate the law," and that they "have had a damaging effect on the business operations and reputation of Nationwide and its agents." The letter also stated that: *Nationwide recognizes and respects your right as a citizen to communicate with government agencies and the public. However, you do not have the right to make false statements or accuse Nationwide of wrongdoing, unless your allegations are reasonably supported by the facts and the law. Such actions will not be tolerated, and if they occur in the future, Nationwide intends to exercise its legal rights, which could include legal proceedings in addition to canceling your Agent's Agreement.*

At or about the same time, Nationwide implemented a new business policy, to which Fraser and other agents were opposed. The policy changes were related to Nationwide's new publicized growth plan to establish "multiple distribution channels." Under the new plan, policyholders could buy insurance directly, rather than through an agent. The agents feared that the new policies would undermine their work and their independence.

Fraser, through the NIICA decided to make Nationwide's management aware of the agents' opposition to the plan. NIICA members asked Fraser to prepare a letter to competitors of

Nationwide to solicit interest in acquiring the policyholders of the approximately two hundred NIICA members in Pennsylvania. In drafting the letter, the agents' did not intend to actually separate from Nationwide, but to send a warning that they would leave if Nationwide did not cease the objectionable policies. This letter was ultimately sent to at least one competitor.

A top-ranking officer of Nationwide learned of the letter and another "inappropriate communications" memo was soon sent out. Since they were not sure if the letter was actually sent to a competitor, they conducted a ***search of their electronic file server*** for e-mail communication used by all agents, including Fraser. Stored e-mails belonging to Fraser and other agents were opened, including an exchange of e-mails between Fraser and another agent of indicating that the letter had been sent to at least one competitor.

Subsequently, Nationwide ***cancelled*** Fraser's Agent's Agreement and retrieved its computer systems. Fraser immediately appealed the cancellation to an internal Review Board which determined that Nationwide had the right to terminate its relationship with Fraser for any reason or no reason at all, and that, nevertheless, Fraser's breach of loyalty to the company provided them with a good reason to terminate him.

Fraser filed a lawsuit contending his status as an independent contractor was undermined by Nationwide's policy changes as well as federal ***wiretap violations*** resulting from the unlawful interception of Fraser's e-mail communications.

However, the court determined that Nationwide's alleged conduct, although ethically "questionable," ***did not*** constitute an "interception" of an electronic communication under the Wiretap Act or unlawful "access" to an electronic communication under the Stored Communications Act. Why? Because Nationwide retrieved Fraser's e-mail ***from storage after*** the e-mail had already been sent and received by the recipient. Therefore, Nationwide acquired Fraser's e-mail from post transmission storage.

Fraser's second claim involved his right to ***free speech***. The court's decision, however, was that Nationwide is a private corporation and a private actor under the law. Therefore, Nationwide's decision to terminate Fraser's Agent's Agreement is not subject to constitutional requirements of free speech. Further, the court stated that even if it is true that Nationwide terminated Fraser for reporting to government authorities Nationwide's alleged unlawful practices, for drafting the letter to Nationwide's competitors, or for associating with NIICA, Nationwide is not liable under the constitution.

Opt-In / Opt-Out

It is your ethical and legal duty to honor a client's wishes concerning the handling of his personal and financial statistics. ***Opt-out*** is the process of having one's personal information removed from databases and lists that are often sold for marketing purposes. Personal information is collected on individuals in a variety of ways such as when they are applying for a credit card, telephone service, or entering contests. Credit bureaus also sell information for marketing purposes. If the consumer has active accounts with a brokerage house, credit card company, or insurance company, he will receive a privacy notice from these institutions. The term "financial institution" includes companies such as payday loan companies, collection

agencies, and travel agents. For this reason, it is particularly important for the consumer to carefully review all preprinted notices that he receives in the mail or electronic mail messages. Federal law now gives one some minimal rights to protect his personal financial information. The law gives him the right to prevent a company he does business with from sharing or selling certain sensitive information to non-affiliated third parties. The term "opt-out" means that *unless and until* the consumer informs his bank, credit card company, insurance company, or brokerage firm that he does not want them to share or sell his customer data to other companies, they are free to do so.

When this law was debated in Congress, consumer advocates argued unsuccessfully for an **opt-in** provision. This stronger standard would have prevented the sharing or sale of the customer data *unless* the consumer affirmatively consented. The opt-in standard did not prevail. Therefore the *burden is on the consumer* to protect his financial privacy.

Opt-in does not enhance consumer privacy. Since it is the consumer who makes the final and binding decision regarding the use, non-use, or misuse of his personal information under either "opt-in" or "opt-out", there is no privacy advantage to "opt-in". Neither approach provides the consumer with greater or lesser rights than the other. If this argument is valid, and both "opt-in" and "opt-out" fully reflect consumer preferences regarding the use of their personal information, then all the other arguments are invalid – sellers would receive the same amount of information under either approach. Thus, implementing "opt-in" would not impose any additional costs on either producers or consumers, as compared with implementing "opt-out". However, the choice of scheme – "opt-in" or "opt-out" – does distort consumer preferences by imposing transaction costs on one choice or the other. After acknowledging that transaction costs cause both "opt-in" and "opt-out" schemes to reflect imperfectly the "true" privacy preferences of the consumer, the policy debate can move forward and tackle the next question. Does "opt-in" or "opt-out" reflect the true preferences of the consumer better? Presumably, transaction costs under "opt-in" lead consumers to provide less information than their true privacy preferences would suggest; conversely, transaction costs under "opt-out" lead consumers to provide too much information. The structure of the seller-producer relationship suggests one reason why "opt-in" might represent the consumer's true privacy preference better. The seller can adjust the level of transaction costs involved in "opting" in or out, whereas the consumer cannot. Since the seller has an obvious interest in collecting information, it has an incentive to make it easy and simple to opt in, under an "opt-in" system, and an incentive to make it difficult and time-consuming to opt out, under an "opt-out" system. Whatever regulations exist to make opting out easier, the seller has an incentive to push the envelope, to make opting out as difficult as possible within the letter of the law. Thus, transaction costs under an "opt-out" scheme are likely to be higher than under an "opt-in" scheme, and the outcome under "opt-out" is likely to be concomitantly farther away from the correct outcome than under "opt-in".

Opt-in reduces consumer privacy by hampering efforts to fight fraud and identity-theft. Since an "opt-in" approach reduces the amount of information available to sellers regarding the consumer's preferences, spending habits and typical behavior patterns, it hampers sellers' efforts to detect unusual purchases and alert the consumer to possible fraud. This makes it easier for criminals to assume false identities and engage in other fraudulent behavior at the expense of law-abiding consumers. Not only is this an invasion of privacy in itself, but also the rectification of the situation often requires the consumer to provide personal information about himself. This is a valid point, which, under an "opt-in" scheme, producers might wish to present

to consumers in order to convince them to permit use of their personal information. Under an "opt-out" scheme, this point could be presented to consumers to deter them from exercising their "opt-out" option.

Opt-in imposes significant costs on sellers, which are then passed on to consumers. Opt-in increases the costs to a seller of expanding its range of services, because of the necessary expenditure of resources to obtain consumer permission to use the additional personal information that enables the better service. *Opt-in also increases marketing costs* because, instead of sending promotional materials to a neatly identifiable population segment that is likely to find such materials useful, the seller must send the promotional materials blindly to broader population segments. Some believe that in the "distance shopping" market through catalogs and online sales, enforcing an "opt-in" scheme will result in increased costs, which will then be passed on to consumers. The data restrictions inherent in the "opt-in" scheme would affect catalog marketing more than online marketing. This is because the interactive nature of the Internet can counteract the lack of third-party information about prospective customers. To properly understand the aggregate impact of an "opt-in" scheme on sellers, one would need to look at the reliance of other industries on catalogs, as opposed to more interactive means of marketing. One of the factors slowing the growth of e-commerce, though, is consumer hesitation over conducting business online. In a report to Congress on online privacy, the Federal Trade Commission presented surveys showing the extent to which privacy concerns hamper the growth of e-commerce. Recent survey data demonstrate that 92% of consumers are concerned and 67% are **very** concerned about the misuse of their personal information online. Concerns about privacy online reach even those not troubled by threats to privacy in the off-line world. Thus, 76% of consumers who are not generally concerned about the misuse of their personal information, fear privacy intrusions on the Internet. This apprehension likely translates into lost online sales due to lack of confidence in how personal data will be handled. Indeed, surveys show that those consumers most concerned about threats to their privacy online are the least likely to engage in online commerce, and many consumers who have never made an online purchase identify privacy concerns as a key reason for their inaction. There are benefits of adopting and enforcing an "opt-in" scheme, in which consumers are assured that no one will make use of their personal information without their prior and express consent. The resulting burgeoning in e-commerce would reduce sellers' costs, by enabling them to make more extensive use of the efficiency inherent in interactive marketing tools such as the Internet. This effect may offset, and perhaps even outweigh, the increase in costs attributable to the data restriction effect.

Opt-in reduces the amount of competition in the market. By raising costs of operation, "opt-in" will drive marginally profitable companies out of the market altogether. By requiring new entrants to go through a laborious process of obtaining personal data permits from each new consumer, "opt-in" creates a barrier to entry into the market. Market incumbents, on the other hand, will benefit from an established consumer base that has already given permits. Essentially, "opt-in" helps entrench market incumbents. Since consumers are more likely to "opt-in" to companies they know and trust, such a scheme will favor large firms with established brand names over smaller firms. Competition is most reduced in the industries that rely the most on expensive means of obtaining permission, such as telephone or paper-mail, rather than on website-notices and e-mail. As e-commerce continues to grow, and technology becomes more pervasive, there is likely to be a shift from the former to the latter, and a reduction in the height

of the entry barrier. A new entrant, though forced to beseech consumers for information-permission, could do so inexpensively through mass e-mailing.

Opt-in costs to sellers will be passed on disproportionately to less wealthy consumers. A study of distance shopping in the apparel market (catalogs, online purchases) reveals that inner city and rural consumers are significantly more reliant on distance shopping than the average U.S. household. These populations will be hit hardest by increased prices or decreased discounts which will result from implementation of "opt-in", as companies seek to recoup the increased costs of providing the "distance shopping" option. These are also the consumers who can least afford such price hikes.

Confidentiality

Some confuse the confidentiality with privacy. Privacy demotes the right to be left alone and control information about oneself. Confidentiality concerns the communication of private information and personal information form on person to another. If you surreptitiously collect information for marketing purposes, ***you are intruding*** on an individual's privacy***. If you pass on information without permission***, you are ***violating confidentiality***.

The key ingredients of confidentiality are trust and loyalty. As an agent, you gather personal and confidential information from your clients. You must be willing to take responsibility for handling this sensitive information. For instance, do you take measures to secure client data? Do you unknowingly publicize a client's address, phone or e-mail address, exposing them to unwanted mail? Do you forward e-mail messages and attachments without reading them? Share passwords? Neglect to change your own password?

In a nutshell, it takes a combination of legal, technological and individual actions to preserve confidentiality.

Ethical Decision-Making

Before the Enron fiasco, Arthur Anderson had a steadfast reputation. When big organizations wanted him to falsify their accounting he said . . . "No, we'll find other ways to make our money". The point is, to maintain ethical standards, you have to be able to think around problems, cultures and differences. Here are some ways to accomplish this:

Get The Facts: The Makkula Center for Applied Ethics suggests you find the relevant facts about a situation. This means identifying the individuals or groups who have an important stake in the outcome. Some may have a greater stake because they have special needs or because you have a special obligation to them.

An example might be elderly clients. Due to their status or cognition, they may need to rely more on your advice than other clients. Your ethical standards may have to be raised in matters that concern them.

Sizing Up The Problem: Michigan University Business Ethics Professor Tim Fort suggest you ask the following questions when faced with an ethical decision:

What's the moral issue?
Who has been harmed? Or who could be harmed?
In what ways?
What are the alternatives that exist?
What facts need to be known to make a reasoned decision?
What are the personal impacts on the person making the decision?

Working within a format like this helps bring the issues away from your own self-interests over the interests of others.

Pursuasion: If an ethical dilemma arises between you and a peer or client, why not solve the problem with your powers of persuasion. Be convincing. Have convictions. The influence you exert may very well change their mind.

Taking Risks: The more you are paid, the more complex the decisions you must make. Things are rarely "black and white" and a lot of your decisions will challenge your integrity. But, these are the risks you must be prepared to assume in a sometimes difficult world. You must constantly weigh ***short-term results*** with ***long-term consequences***.

Evaluate Alternative Actions: Which option will produce the ***most good*** and do the ***least harm***? Which option respects the rights and dignity of all stakeholders? Will everyone be treated fairly? Which option will promote the ***common good***. Which option will enable the deepening or development of the core values you share with your company? Your profession? Your personal commitment?

Ratification of Misconduct

Ratification generally occurs where, under the particular circumstances, the employer demonstrates an intent to adopt or approve oppressive, fraudulent, or malicious behavior by an employee in the performance of his job duties. The issue commonly arises where the employer or its managing agent is charged with ***failing to intercede in a known pattern of workplace abuse***, or ***failing to investigate or discipline*** the errant employee once such misconduct became known. Corporate ratification in the punitive damages context requires actual knowledge of the conduct and its outrageous nature."

Solicit Client Feedback: Before you make the final decision ask the client if your solution meets with his approval. Always ask these important questions:

- Have I given you all the information you need to make a decision?
- Does this information or policy make sense?
- Is there something else I can answer for you to assure you that this is the right solution based on your needs and objectives?

Reflect on Your Decision: Was you position defensible? Would you do it again? How did it turn out for all concerned? Was your decision successful for both you and your client?

Confronting Unethical Conduct

In a lot of ways, we have become a ***no-fault society***. Popular thinking dictates that as long as you don't own the problem you don't need to get involved. A crucial shift is needed to avoid this bystander mentality. People need to think of themselves as members of a community. And, their life in this community entails ***mutual obligations*** and ***interdependence***. In other words, be part of the solution, not part of the problem.

How can this be accomplished. Well, you can learn to help solve ethical dilemmas rather than walk away or simply ignore them. Here are a few ways to do this:

State Your Position: Ask those who want you to perform an unethical task to ***state their position clearly***. This forces them to make an ethical choice. If your manager wants you to fudge an application, for example, pose the following question: Are you asking me to lie on this application? It is probably a safe bet that he will back away from his unethical request.

Present A Case: Many ethical dilemmas result because someone has taken a short cut. You can sometimes turn their thinking around by presenting things statistically or in an organized manner. Take the manager who wants you to submit an inaccurate application. If you use some of your CE materials, you could easily find a recent court case where an agent did a similar thing and faced a huge penalty and loss of license. When presented this way, it would be hard to ignore the correct path.
Don't Ratify Unethical Actions: One of the easiest ways to become entangled in the wrong deeds of someone else is to ratify their behavior. Not only is it unethical, but it can come back to haunt you in the form of rather large lawsuit. Take the case of Agent Roger McCall, a licensed life insurance agent and/or broker with Alexander Hamilton Life. McCall sold client Richard Barton a life insurance policy. Barton alleges that a number of representations regarding the policy were untrue and fraudulent, that the administration of the policy was fraudulent, and that Mr. McCall had falsified documentation, forged Mr. Barton's signature, and actually took out taken out an unauthorized loan on the policy.

A jury found that Mr. McCall made the intentional and negligent false representations, and the false promises, as an agent of defendant Hamilton. Further, it found that Hamilton had expressly authorized Mr. McCall to make the statements that were found to be misrepresentations or false promises. The court awarded over $850,000 in compensatory damages!

Obviously, Roger McCall did not operate within ethical boundaries. The real question is did his company or anyone in it ***ratify*** or endorse his actions, and in the process, become part of his scheme. Absolutely not! As soon as Hamilton became aware of Mr. Barton's complaint, it terminated Mr. McCall's agent agreement and initiated an investigation. It hired an attorney to interview Mr. McCall and it reported Mr. McCall's conduct to the Department of Insurance and the local Police Department. It contacted policyholders, and it reimbursed them for their losses in the total sum of approximately $1.2 million. In other words, instead of ratifying or approving of Mr. McCall's conduct, it tried to ***solve the problem by restoring the stolen funds***. Hamilton

also offered Mr. Barton the opportunity to rescind the policy and it offered to reimburse him for any money that he was out of pocket as a result of Mr. McCall's acts.

Such conduct, said the court, cannot be considered ratification of Mr. McCall's conduct. Instead, it falls within the established principle that, when the agent exceeds his authority, there is no ratification when the principal ***repudiates*** the agent's actions as soon as the principal learns of them. Despite Mr. Barton's contrary argument, the court did not view Hamilton's conduct as an improper attempt to ratify Mr. McCall's conduct. His misrepresentations were, in fact, not authorized or approved by Hamilton, and they did not provide a basis for an award of punitive damages.

That's how ethics in insurance work!

A Moral Agency Climate

If you ***don't*** create an agency culture that reinforces values and ethics, other agents and employees will only do what is right so many times and then they will either leave or give in to outside pressures to cut corners, lie, fudge, etc.

In order to reinforce this theme, you can't punish people for taking actions they need to take. You have to ***support*** good, moral decisions, even at the ***cost of production***.

What happens if no one else cooperates? You must continue to forge forward, even if you are the only one doing the right thing. Why? It's a fundamental choice you are making to be an ethical leader. And, it will pay off in time.

Integrity

While many agents believe that "integrity" is a characteristic of choice, many state laws set minimum agent standards to follow, such as:

Qualifications

Insurance Commissioners have been known to suspend or revoke an insurance agent's license if it is determined that he or she is not properly qualified to perform the duties of a person holding the license. Qualification may be interpreted to be the meeting of minimum licensing qualifications (age, exam scores, etc) or beyond.

Lack of Business Skills or Reputation

Licenses have been revoked where the agent is NOT of good business reputation, has shown incompetency or untrustworthiness in the conduct of any business, or has exposed the public or those dealing with him or her to danger of loss. In Goldberg v. Barger - 1974, an application for an insurance license was denied by one state on the basis of reports and allegations in other states involving the applicant's violations of laws, misdealing, mismanagement and missing property concerning "non-insurance" companies.

Activities Circumventing Laws

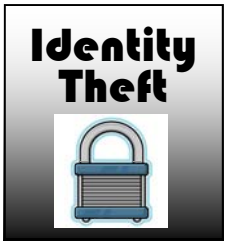
Agent licenses have been revoked or suspended for activities where the licensee (1) did not actively and in good faith carry on as a business the transactions that are permitted by law; (2) avoids or prevents the operation or enforcement of insurance laws; (3) knowingly misrepresents any terms or the effect of a policy or contract; or (4) fails to perform a duty or act expressly required of him or her by the insurance code. In Hohreiter v. Garrison - 1947, the Commissioner revoked a license because the agent misrepresented benefits of policies he was selling and had entered false answers in applications as to the physical condition of the applicants. In Steadman v. McConnell - 1957, a Commissioner found a licensee guilty of making false and fraudulent representations for the purpose of inducing persons to take out insurance by misrepresenting the total cash that would be available from the policies.

Agent Dishonesty

Agents have lost their license because they have engaged in fraudulent practices or conducted any business in a dishonest manner. A licensee is also subject to disciplinary action if he or she has been convicted of a public offense involving a fraudulent act or an act of dishonesty in acceptance of money or property. Furthermore, most Insurance Commissioners will discipline any licensee who aids or abets any person in an act or omission which would be grounds for disciplinary action against the persons he or she aided or abetted. In McConnell v. Ehrlich - 1963, a license was revoked after an agent made a concerted effort to attract "bad risk business" from drivers who licenses had been suspended or revoked. The Commissioner found that the agent had sent out deceptive and misleading solicitation letters and advertising from which it could be inferred that the agents could place automobile insurance at lower rates than could others because of their “volume plan”. If this wasn’t bad enough, the letters appeared to be official correspondence of the Department of Motor Vehicles. Clients would be induced to sign contracts with the agents where the agent would advance the premiums to the insurance company. The prospective insured would agree to repay the agents the amount of the premium plus “charges” amounting to an interest rate of 40 percent per annum. The interest rates charged were usurious and violated state law.

Catchall Category

In addition to the specific violations above, most states establish that agent responsibilities MUST NOT violate the “public interest”. This is obviously a catchall category that has been used where agents have perpetrated acts of mail fraud, securities violations, RICO (Criminal) violations, etc.



Section 4: Identity Theft Insurance for Individuals

The insurance industry has responded to the risk of identity theft by creating new products to protect against the financial risks associated with it. In this chapter, identity theft coverages available for personal lines are examined.

Some insurance companies now offer identity theft insurance to individuals as an endorsement to a homeowners policy, while others offer it as a standalone policy. Such insurance helps pay for the expenses incurred to repair to credit histories. Coverage reimburses policyholders for expenses they incur as a result of their efforts to clear their credit histories and legal and financial records after becoming a victim of identity fraud. Expenses covered include legal expenses, loan re-application fees, telephone and certified mailing charges, notary expenses, and lost wages for time taken off from work to deal with fraud.

Some insurance programs are offered in conjunction with credit monitoring and credit repair services. These bundled services may be available for a monthly or annual fee. These companies may offer insurance that will reimburse up to $10,000 for certain expenses incurred, and include things like personal data organizing software to record confidential information safely in one place, and provide victim assistance in clearing up identity theft records. Legal fees, lost wages, and postage costs may also be included if the coverage.

Identity theft insurance does not cover any financial losses incurred due to unauthorized use of credit cards or stolen checks. These losses are the responsibility of the creditors. This insurance does not repair the victim's credit standing or clean up a criminal record that may be acquired due to identity theft. Instead, it pays for expenses associated with the credit repair process. The insurance covers the time and money it takes victims to process the paperwork necessary to restore credit.

The Homeowners Endorsement Form

One of the methods that can be used to provide identity theft coverage is to add an endorsement form to the client's homeowners insurance form. ISO (the Insurance Services Office) created a Homeowners "Identity Fraud Expense Endorsement" form in 2002, and it has been adopted by many state insurance departments.

The purpose of the coverage is to help homeowners, condominium unit owners and renters pay the necessary costs to repair the individual's credit history due to identity fraud.

The endorsement provides up to $15,000 for the insured's expenses that result from an identity fraud discovered or known during the policy period. Coverage offered by individual insurers may vary in this coverage limit.

Identity Fraud Definition

Under the endorsement, identity fraud is defined as:

The act of knowingly transferring or using, without lawful authority, a means of identification of an "insured" with the intent to commit or to aid or abet another to commit, any unlawful activity that constitutes a violation of federal law or a felony under any applicable state or local law. *Earlier, the definition of identity theft was examined under the Identity Theft Assumption and Deterrence Act. Any of the activities defined as the crime of identity theft under this Act would constitute a triggering event for the identity fraud coverage. Violation of state identity theft laws would also qualify as a triggering event under this type of coverage.*

There are ISO homeowners forms for homeowners, condominium owners and renters. The various types of homeowners forms include:

- HO-1, the basic form for homeowners coverage
- HO-2, the broad form for homeowners coverage
- HO-3, the special form for homeowners coverage that provides open peril coverage on the dwelling,
- HO-4, the contents form used for renters
- HO-5 the comprehensive from for homeowners coverage that provides open peril coverage on the dwelling and personal property
- HO-6, the unit owners form, which is used for condominium unit owners
- HO-8 the modified coverage form used when a home's replacement value is greater than its market value

The definition of "insured" is found in the homeowners form to which the endorsement is attached. . The definition of "insured" is the same in each of the various form types. In these homeowners forms, insured is defined as:

a. *You* (the named insured listed in the policy's declarations) *and residents of your household who are:*
(1) *Your relatives; or*
(2) *Other persons under the age of 21 and in the care of any person named above;*
b. *A student enrolled in school full time, as defined by the school, who was a resident of your household before moving out to attend school, provided the student is under the age of:*
(1) *24 and your relative; or*
(2) *21 and in your care or the care of a person described in* ***a.(1)*** *above;*

Expenses

Most of the endorsement's provisions define the expenses the coverage will pay. These include:

- Costs for notarizing affidavits and similar documents that are required by financial institutions, creditors or credit agencies to attest to fraud
- Costs for certified mail to law enforcement agencies, credit agencies, financial institutions, or other credit grantors
- Lost income due to missing work to complete fraud affidavits, meet or talk with law enforcement agencies, credit agencies or legal counsel. The insurer will pay up to $200 per day, with total lost income payments not to exceed $5000.
- Loan application fees if the insured needs to re-apply for a loan because the loan was rejected solely because the lender received incorrect loan information
- Reasonable attorney fees owed as a result of "identity fraud" to defend lawsuits brought by merchants, financial institutions or their credit agencies, to remove criminal or civil judgments wrongly entered against an insured, or to challenge the accuracy or completeness of any information in a consumer credit report
- Long distance telephone charges incurred for calls to merchants, law enforcement agencies, financial institutions or other creditors, or credit agencies to report or discuss an actual "identity fraud."

Additional Coverage

Under the additional coverage, the insurer pays up to $15,000 for the "expenses" listed in the endorsement as the result of any one "identity fraud" first discovered or learned of during the policy period.

Since it is additional coverage, it is in addition to the coverage limits that normally apply to the policy. So, if the insured has a homeowners policy with a $200,000 limit applicable to the Section I property coverage, the $15,000 in identity fraud expense coverage is in addition to the $200,000 limit. If a windstorm destroys the insured's home, causing $200,000 of damage, and the wind blows the insured's personal records to the home of an identity thief who proceeds to commit identity fraud against the insured, the identity theft coverage would pay up to $15,000 on top of the $200,000 the insurer will pay due to the windstorm.

The ISO homeowners policies provide coverage of up to $500 for the following occurrences that may also be caused by identity fraud:

- The legal obligation of the insured to pay because of the theft or unauthorized use of the insured's credit cards
- Loss resulting from theft or unauthorized use of an insured's electronic fund transfer card or access device used for deposit, withdrawal or transfer of funds
- Loss to an insured due to forgery or alteration of a check or other negotiable instrument

Occurrence Based Coverage

The ***ISO homeowners*** forms and the identity fraud expense coverage endorsement are ***"occurrence" based forms***. This means that an "occurrence", as defined under the homeowners forms, and "identity fraud", as defined under the endorsement, ***must occur during the policy period in order to be covered***. The claim can be made after the policy period, but

must conform to the policy's conditions, including those applicable to the insured's "duties after loss" or "duties after an occurrence."

These duties include:

- Giving prompt notice to the insurer or its agent
- Notifying the police, if loss by theft
- Notifying the credit card company
- Cooperating with the insurer
- Sending the insurer, within 60 days of request, evidence or affidavit to support the claim

Deductible

The identity fraud expense coverage includes a $250 deductible. A deductible is the amount of a covered loss that the insurer will not pay.

Other Identity Theft Insurance Coverages

Besides offering identity theft coverage as an endorsement to a homeowners policy, insurers also offer identity theft insurance through stand-alone policies. These policies also provide coverage for expenses related to attorney and other legal fees, loan expenses and lost wages.

Packaged Identity Theft Services

Some insurers provide insurance as part of a package of services that are meant to combat identity theft. The insurer may partner with security service providers or financial institutions to offer these products. Services may include:

- Credit monitoring services that review the customer's credit report on a regular basis and reports changes and additions to the customer
- Security software that includes firewall protection against hackers attempting to access personal information stored on computers. Some identity theft packages provide the software as part of the service, and others offer a discount on the purchase of such software.
- Identity theft education and alerts about current identity theft threats and scams
- Identity theft resolution services that help customers work with the credit bureaus, creditors, law enforcement agencies, the Social Security Administration, the Postal Service, and so on.
- Identity theft insurance coverage

Employee, Customer or Group Member Benefits

Insurers may also team up with employers, credit issuers or groups to offer identity theft insurance and support services.

Credit issuers can purchase group identity theft insurance and offer it as an optional or free benefit to customers.

Groups or societies can purchase group identity theft insurance and offer it to members.

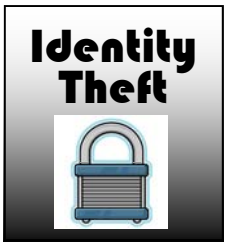
Employers can also offer identity theft insurance as part of an employee benefits package.

These insurance programs may also be packaged with other services, like credit monitoring and victim support services. Legal advisory services are another service included in some employee benefit identity theft programs.

Summary

Identity theft coverage is now available for individuals. The premium may be as low as $25 a year for the homeowners endorsement. Some companies are offering it as a free addition to homeowners policies.

The basic coverages include payment for expenses associated with identity theft, such as costs for notarizing documents, mailing costs, lost income, loan application fees, reasonable attorney fees, and long-distance telephone fees.



Section 5: Identity Theft Insurance In the Workplace

Identity theft is not only a risk to individuals. Businesses need financial protection from its risks.

Risks to Businesses

Businesses can be impacted by identity theft in many ways. Client's and employee's personal information may be stolen by other employees or temporary workers. Carelessness on the part of staff can make it easy for an outsider to gain access to personal information in the office, as can the employer's lack of security measures.

The wealth of information on computer networks and it accessibility over the Internet is another area of risk for employers. Hackers from the inside and the outside of a business can access sensitive information over computer lines.

Thieves, perhaps in the guise of janitors or service contractors, can walk through a business and steal information for identity theft purposes as well.

Businesses who sell items have the threat of identity thieves using stolen checks or credit cards to pay for them. Credit card chargebacks due to fraud are an increasingly big expense for merchants.

Insurance Coverages

Identity theft is a crime that takes advantage of newer technologies that were not in place when many of the commercial insurance policy provisions were developed. This chapter will examine how these standard policy provisions apply in an identity theft situation.

Most businesses have one or more of the following standard business insurance coverages:

- Commercial Property
- Commercial General Liability

In addition, many businesses have standard Crime or Fidelity coverage and Directors & Officers Coverage. They may also have Data Processing Media Coverage.

In this section, these standard coverages are examined in light of their ability to provide protection for the risks associated with identity theft. In addition, new policies and programs specifically designed to cover businesses' identity theft risks are explored.

Commercial Property Coverage

Commercial property coverage protects against loss or damage to a company's real property and its personal property. It covers "first-party" risks – damage and loss to the businesses'

property – and does not cover losses caused by the business to other people's property, known as "third-party" risks.

A businesses' first-party risks related to identity theft include:

- Loss of customer information and transactions that will need to be recovered or restored
- Loss of employee information that will need to be recovered or restored
- Loss of customer records that may involve loss of income, e.g. sales transactions that have not yet been collected or reconciled are taken by the thief
- Loss of property, such as computer terminals or laptops containing customer or employee information
- Loss of goodwill/reputation due to the theft of customer and/or employee records

Loss of Customer or Employee Data

A commercial property policy may not cover the loss of customer or employee information. If the insurer's policy is based on ISO's standard CPP 2000 form, electronic data is excluded from coverage, other than for minimal coverage to replace the material onto which it is stored. The Commercial Property Policy form's electronic data provisions follow:

Covered Property does not include:

n. *The cost to research, replace or restore the information on valuable papers and records, including those which exist on electronic or magnetic media, except as provided in the Coverage Extensions…*

Coverage Extensions

c. Valuable Papers And Records – Cost Of Research
You may extend the insurance that applies to Your Business Personal Property to apply to your costs to research, replace or restore the lost information on lost or damaged valuable papers and records, including those which exist on electronic or magnetic media, for which duplicates do not exist. The most we will pay under this Extension is $2,500 at each described premises, unless a higher limit is shown in the Declarations.

7. Valuation

We will determine the value of Covered Property in the event of loss or damage as follows:
f. *Valuable Papers and Records, including those which exist on electronic or magnetic media (other than prepackaged software programs), at the cost of:*
(1) *Blank materials for reproducing the records; and*
(2) *Labor to transcribe or copy the records when there is a duplicate.*

The standard property form provides limited coverage to replace lost or damaged records.

Another limitation in the use of a commercial property form to cover identity theft occurs if computer data is stolen, destroyed or damaged by a "hacker." The standard policy does not include a computer hacker as a covered cause of loss. So, even if the policy does not exclude electronic data from coverage, loss or damage due to a hacker may not be covered.

Loss of Income

Property policies may include Business Income coverages. Business income coverage can pay for the loss of income if operations must be suspended. The benefit from the policy is based on the "period of restoration." This period begins at a specified length of time after "direct physical loss" occurs, and ends on the date the property can be reasonably repaired, rebuilt or replaced.

Often, business income coverages require that the beginning of the period of restoration start anywhere from 12 to 72 hours after the direct loss occurred. If the identity theft causes loss of computer records and interrupts the computer operations of the business, the business could lose significant income before the period of restoration even begins. In addition, a business that relies on computers to transact must get them up and running again rapidly. Systems may be operational before the 12 – 72 hour waiting period has expired.

Another limitation of the traditional business income policy is that damage done by an identity thief is not normally a covered cause of loss, whether the thief is an outside computer hacker, a dishonest employee, or the janitor.

Businesses may also use outside vendors to store and maintain their computerized files. Standard business income policies require that the loss of income be due to loss or damage that occurs at the business' premises or location. So, loss or damage that occurs at the vendor's location could very well be excluded from coverage.

Loss of Computers and Laptops

The property policy will generally cover the loss or damage of business personal property, but may exclude dishonest or criminal acts of the insured's employees. This depends on the provisions of the causes of loss form used with the commercial property form.

Loss of Reputation/Goodwill

Commercial property policies do not cover intangible losses, such as loss of goodwill.

Commercial General Liability Coverage

The commercial general liability form provides coverage that protects a company against third-party risks. Third-party risks are lawsuits and claims resulting from loss or damage to others caused by the business. Third-party identity theft risks of the business include:

- Lawsuits from customers whose privacy rights are violated
- Lawsuits from employees whose privacy rights are violated
- Lawsuits for resulting loss to customer's or employees whose identity is stolen using records from the business

Most current commercial general liability forms exclude invasion of privacy lawsuits unless the violation occurs in the course of advertising. The older forms did not lay out the intent of the advertising injury coverage as clearly as the newer forms, based on ISO's 1998 CGL form. Under the old from, insureds tried to file claims for defense of invasion of privacy suits based on this definition: *injury arising out of one or more of the following offenses:*

a. *Oral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services;*
b. *Oral or written publication of material that violates a person's right of privacy;*
c. *Misappropriation of advertising ideas or style of doing business; or*
d. *infringement of copyright, title or slogan.*

Since "advertising" was not defined, claimants tried to gain coverage for many different right to privacy lawsuits, based on the advertising injury coverage applying to *oral or written publication of material that violates a person's right of privacy.*

The new form defines "'advertisement" so that it is more clear that right to privacy issues are only covered in they occur in the course of advertising:
a notice that is broadcast or published to the general public or specific market segments about your (the insured's) *goods, products or services for the purpose of attracting customers or supporters.*

Another limitation of the commercial general form is that the standard coverage territory is the United States, Puerto Rico and Canada. If the business has a presence on the Internet, whether for sales or other company services, the policy may not cover liability that arises from a hacker whose location is outside the coverage territory.

Crime Coverage

Crime coverage forms will generally cover identity theft risks such as employee theft and theft of equipment. However, the coverage may be limited in certain ways.

ISO's newest standard crime form, the 2002 version, includes "computer fraud" coverage:

Computer Fraud

We will pay for loss of or damage to "money", "securities" and "other property" resulting directly from the use of any computer to fraudulently
cause a transfer of that property from inside the "premises" or "banking premises":

a. *To a person (other than a "messenger") outside those "premises"; or*
b. *To a place outside those "premises".*

However, the benefit for the cost of reconstructing computer records is limited:

a. Special Limit Of Insurance For Specified Property
b.

We will only pay up to $5,000 for any one "occurrence" of loss of or damage to manuscripts, drawings, or records of any kind or the cost of reconstructing them or reproducing any information contained in them.

In addition, crime forms do not cover indirect or business income losses:

D. Exclusions…
d. Indirect Loss
Loss that is an indirect result of any act or "occurrence" covered by this insurance including, but not limited to, loss resulting from:

(1) *Your inability to realize income that you would have realized had there been no loss of or damage to "money", "securities" or "other property".*
(2) *Payment of damages of any type for which you are legally liable. But, we will pay compensatory damages arising directly from a loss covered under this insurance.*
(3) *Payment of costs, fees or other expenses you incur in establishing either the existence or the amount of loss under this insurance.*

Crime policies also exclude any liability coverages, so do not cover claims or suits against the company for invasion of privacy.

Directors and Officers Insurance

Directors and Officers (D&O) coverage is a form of professional liability insurance that protects directors and officers from personal liability risks occurring through the course of their business responsibilities.

Standard D&O policies often do not explicitly cover computerized or Internet activities, so may not cover them. Invasion of privacy risks are also not generally covered.

In addition, responsibility for invasion of privacy violations may not lay at the feet of directors and officers only, but the business itself may be sued. Broader protection than that provided by standard D&O policies may be needed.

Electronic Data Processing Policy

The Electronic Data Processing (EDP) form is an inland marine policy form that includes property insurance and liability insurance for certain EDP risks.
The property coverage includes protection for loss or damage to computer hardware, computer software and hardware. Business income coverage is also included. The liability coverage applies to liability incurred by the business for handling and storing data for other businesses.

This type of policy may or may not provide sufficient property coverage levels to pay for the cost of restoring or replacing data.

If a ***computer hacker*** is the cause of loss, the business income of the coverage ***may not cover the loss***, if the form includes an indirect loss exclusion.

The liability portion of the coverage may not include coverage for privacy violations.

Filling the Identity Theft Coverage Gaps

As the foregoing discussion demonstrates, standard coverage forms may not cover all of a company's risks associated with identity theft. The agent should review a business client's coverage carefully to determine if new coverages should be added to protect the client from this risk.

Internet or eBusiness Coverage Forms

Internet or eBusiness coverage forms may provide the coverage needed to fill identity theft coverage gaps. Even if a company's primary functions do not involve the Internet, these forms often include the broad computer and electronic media related coverages that today's

businesses often need. In addition, invasion of privacy risks are often specifically covered by Internet liability forms. Businesses who take orders by telephone can also often benefit by the coverages found in Internet Insurance forms.

Endorsements of Stand Alone Policies

Some Internet liability forms can be added as endorsements to the commercial general liability policy. Liability for covered "wrongful acts" in these forms may include:

- Invasion of privacy
- Unauthorized access and hacker attacks
- Infringement of privacy

These endorsements are often known as "multimedia errors & omissions" coverages.

Another coverage available in some internet policies pays for the hiring of a public relations firm to assist the business in repairing its reputation and recapturing its goodwill.

Stand-alone policies or programs are also available. Some insurers offer a suite of coverages and services for companies who specialize in eCommerce. The package may include risk assessment, security services and property and liability coverage.

Amending Current Coverage

Another option for filling coverage gaps for identity theft risks is for the insurer to amend its standards forms, based on the customer's needs. Large companies have risk managers who can identify risk exposures and will work with the insurer to amend coverage to cover these exposures. For example, the valuation provisions related to replacing computer data could be changed to allow for higher limits and broader coverage. Invasion of privacy could be added as a covered wrongful act under existing liability coverage.

However, only a few insurers are likely to be willing to make such changes. Underwriting for individual risks in this manner is not something all insurers feel comfortable doing.

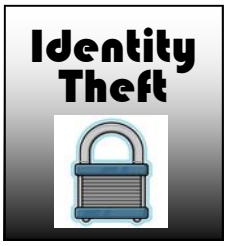
Evaluating Specialized Identity Theft Business Coverages

I

In this section, potential gaps in identity theft coverage in standard forms have been identified. Internet coverage forms should also be evaluated for potential deficiencies.

Some Internet policies cover only property loss and damage. Others cover only liability risks. As has been pointed out, identity theft includes risks to property along with liability risks. Before suggesting an Internet policy as coverage, the agent must help the client identify the types of risks the company has, and make sure the proper coverage is offered.

Liability coverages in this new arena may be "claims made" forms, which means that both the occurrence and the claim must occur during the policy period, plus any extended reporting periods included in the policy. Since identity theft losses may not be discovered immediately, claims made policies may not include all the coverage a client needs.



Section 6: Legislative Action

Insurance Companies and Privacy

Insurance companies are now subject to the **Financial Modernization Act**, also known as the Gramm-Leach-Bliley Act. This Act is broad in scope, regulating affiliations between financially related firms such as banking, securities, and insurance; allowing banks to offer any service of a financial nature. It also protects the Community Reinvestment Act (CRA) while at the same time extending the examination period for banks with satisfactory or outstanding CRA ratings. It restricts the ability of unitary thrift institutions to be sold to commercial firms and protects a bank's ability to sell title insurance and generally insuring healthy competition among financial institutions and more choices at lower prices for consumers. The portion of this Act that we will be reviewing, however, has to do with the privacy of customer financial information.

Insurers are also subject to the **Privacy Rule** that requires, banks, securities, and insurance agencies to protect the privacy of consumers' nonpublic personal health information. The privacy rule is mandated under the Health Insurance Portability and Accountability Act, or HIPAA.

Most state insurance offices have adopted privacy regulations based on these Acts. While each state's law may vary slightly, they have in common that they provide customers with more information about their insurance companies and their affiliate relationships, and include stringent privacy procedures. Under these regulations, customers are given the opportunity to "opt out" of having their personal information shared with other companies. e.g. through marketing lists. The required privacy notices help protect customers from consumer fraud and theft. Most identity theft experts suggest that consumers remove their names from as many marketing lists as possible, so that there are fewer opportunities for a thief to get hold of the individual's information in them.

Requirements Under the Financial Modernization Act

The Financial Modernization Act specifies several requirements insurers and other financial institutions must fulfill in order to protect customer information.

1. When a customer relationship is established, and at least annually thereafter, the insurer must provide a notice to the customer describing its policies and practices regarding: a) disclosing nonpublic information to affiliates and nonaffiliated parties, including the categories of information that may be disclosed, b) disclosing nonpublic personal information of persons who are no longer customers of the insurer, and c) protecting the nonpublic personal information of consumers.

2. The insurer may not disclose to any nonaffiliated party any nonpublic personal information unless the insurer: a) has provided the customer with the required notice, and the notice includes the fact that the insurer may disclose this information to a third party, b) has provided

the customer with the opportunity to inform the insurer that the information may not be disclosed (this is known as “opting-out), before the information is disclosed, and c) provided the customer with the information concerning how to opt-out, or how to inform the insurer if the customer does not want the information disclosed.

State Regulation and the Financial Modernization Act

Since insurance is regulated by the states, the Financial Modernization Act requires states to adopt laws to regulate insurers in accordance with the Act. The NAIC, or National Association of Insurance Commissioners, created model regulations based on the Act, entitled “Standards for Safeguarding Customer Information Model Regulations.” Almost all states have now implemented regulations based on the Financial Modernization Act, with several using the NAIC’s Model Regulation as the basis for the state’s regulations.

California Insurance Information and Privacy Protection Act

On March 27, 2003 the California Department of Insurance issued notice that all insurance institutions, agents, and insurance support organizations ("Licensees") subject to the provisions of the California Insurance Information and Privacy Protection Act (California Insurance Code Sections 791-791.27) and the privacy provisions of the Federal Gramm-Leach-Bliley Financial Services Modernization Act that California's regulations governing the Privacy of Nonpublic Personal Information took effect on March 24, 2003. Those regulations are set forth at Title 10, California Code of Regulations, Sections 2689.1 through 2689.24. A copy of the regulations is available on the Department of Insurance website. at http://www.insurance.ca.gov/LGL/privacy.htm.

The regulations provide:

- ***Licensees generally must provide*** consumers with a ***notice describing the licensee's privacy practices at the time of policy application*** and annually thereafter.
- All Notices must clearly and conspicuously describe the categories of personal information collected about individuals, the categories of personal information disclosed about individuals, and the categories of third parties who may receive that information.
- If a licensee wishes to disclose personal financial information to nonaffiliated third parties, the licensee must provide a clear and conspicuous Opt-Out Notice and a cost-free method for the consumer to reply.

“***Nonpublic personal financial information***” ***means personally identifiable financial information*** a consumer provides to a licensee to obtain an insurance product or service from the licensee, information about a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer, or information the licensee obtains about a consumer in connection with providing an insurance product or service to that consumer.

“Nonpublic personal financial information” includes any list, description or other grouping of consumers that is derived using any personally identifiable financial information that is not publicly available. “Nonpublic personal financial information” does not include medical record information.

(j) ***"Opt-In***" means that a licensee must ***obtain a consumer's permission before sharing certain nonpublic personal information*** with others.

(k) "Opt-Out" means that a licensee must allow a consumer the opportunity to prevent the sharing of certain nonpublic personal financial information with others. [Regulation 2689.4(h), (j), (k)]

The regulations clarify what constitutes a clear and conspicuous notice:
"Clear and conspicuous" means that a notice is "reasonably understandable" and "designed to call attention to the nature and significance of the information" in the notice. All notices must be clear and conspicuous and accurately reflect the licensee's privacy policies and practices. [Regulation 2689.4 (a)]

- Insurance producers are responsible for providing notices only if they collect or disclose information in ways other than as set forth in the insurer's notice.
- Nonpublic personal medical record information may not be disclosed without prior written consent.

"Nonpublic personal information" means "personal information" as defined in California Insurance Code Section 791.02(s). "Nonpublic personal information" includes "nonpublic personal financial information" and "medical record information" (as defined in California Insurance Code Section 791.02(q) .

"Nonpublic personal information" includes any list, description or other grouping of consumers that is derived using any personally identifiable information that is not publicly available. "Nonpublic personal information" also includes any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer; any information the licensee collects through an Internet cookie (an information-collecting device from a web survey); and information from a consumer report.

If information about individuals associated with a business entity is collected or accessed in connection with a consumer transaction, or is used for marketing products or services intended for personal, family, or household purposes, it is nonpublic personal information for purposes of these regulations. Insurance transactions relating to products obtained by a policyholder for business, commercial, or agricultural purposes, but which actually provide insurance primarily for personal, family, or household purposes, involve nonpublic personal information for purposes of these regulations
.
A dual purpose policy providing only incidental or supplemental commercial coverages is still a policy primarily for personal, family or household purposes for purposes of these regulations. [Regulation 2689.4(i)

Standards are required for the safeguarding of nonpublic personal information.

Licensees not in compliance with all applicable provisions may be subject to enforcement action in accordance with California Insurance Code Section 791.15 and any other enforcement provisions available to the Commissioner.

Any questions regarding the specific requirements of the regulations can be addressed to Mary Ann Shulman, Staff Counsel, California Department of Insurance, Legal Division, Rate Enforcement Bureau, 45 Fremont Street, 21st Floor, San Francisco, CA 94105 (415) 538-4133.

The Regulations provide that the notice must contain the following information:

Section 2689.7. Information to be Included in Privacy Notices

(a) The initial, annual and revised privacy notices that a licensee provides under Sections 2689.5, 2689.6, and 2689.9 shall, at a minimum, include each of the following that applies to the licensee and to the consumers to whom the licensee sends its privacy notice:

(1) The categories of nonpublic personal information that the licensee collects;

(2) The categories of nonpublic personal information that the licensee discloses;

(3) The categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information, and the general types of businesses in which the third parties engage if the information is disclosed pursuant to California Insurance Code Section 791.13(k);

(4) The categories of nonpublic personal information about the licensee's former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information about the licensee's former customers, if the information is disclosed pursuant to California Insurance Code Section 791.13(k);

(5) If a licensee wishes to disclose or reserve the right to disclose nonpublic personal financial information to an affiliate for marketing purposes without affirmative authorization or the right to opt out of that disclosure, a statement explaining that the licensee may disclose nonpublic personal financial information to affiliates for marketing purposes without obtaining prior authorization and the law does not allow customers to restrict that disclosure .

(6) An explanation of the consumer's right to opt out of the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time ;

(7) Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) regarding the ability to opt out of disclosures of information among affiliates ;

(8) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information, including a general description as to who is authorized to have access to the information ;

(9) If applicable, a statement that the consumer has the right to access and request correction of recorded nonpublic personal information and a brief description of the manner in which those rights may be exercised and ;

(10) The categories of disclosures that the licensee makes under California Insurance Code Section 791.13.

(11) If applicable, the statement required by California Insurance Code Section 791.04(b)(5).

(12) A licensee does not adequately categorize the information that it discloses if the licensee uses only general terms, such as transaction information about the consumer.
The New Regulations still allow disclosure of information in the event of fraud. It provides:

Section 2689.11. Disclosure of Medical Record Information

(a) A licensee shall not disclose nonpublic personal medical record information about a consumer to affiliated or nonaffiliated third parties without the consumer's prior written authorization.

(b) This section does not prohibit or restrict the disclosure of nonpublic personal medical record information as permitted by California Insurance Code Section 791.13 or require an authorization for disclosure of nonpublic personal medical record information other than as required by California Insurance Code Section 791.13.

California Insurance Code 791.13 provides, in relevant part, that information can be disclosed if: the disclosure is: (a) With the written authorization of the individual,... [or without authorization to allow] (B) Detecting or preventing criminal activity, fraud, material misrepresentation or material nondisclosure in connection with an insurance transaction.

The Regulations protect those insureds who refuse to allow disclosure. It says:

A licensee shall not unfairly discriminate against any consumer or customer because that consumer or customer has opted out from the disclosure of his or her nonpublic personal information pursuant to the provisions of these regulations.

A licensee ***shall not unfairly discriminate*** against a consumer or customer because that consumer or customer has not granted authorization for the disclosure of his or her nonpublic personal medical record information pursuant to the provisions of these regulations.

As used in this section, ***"unfairly discriminate" includes denying a consumer or customer a product or service*** because he or she has not provided the consent required to authorize the financial institution to disclose or share his or her nonpublic personal information as provided in California Insurance Code Section 791.13(k).

These Regulations impose a major paper-work requirement on every person involved in the business of insurance. The Regulations are long, detailed and difficult to read. The notices are required to be easy to read and the Regulations impose multiple detailed limits on how the notices are to be written. Every insurer, insurance producer and claims handler/adjuster that do business in the state of California must be very careful in complying with the Regulation.
:

Protecting Patient Health Information

Overview: Each time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential health information. In the past, family doctors and other health care providers protected the confidentiality of those records by sealing them away in file cabinets and refusing to reveal them to anyone else. Today, the use and disclosure of this information is protected by a patchwork of state laws, leaving gaps in the protection of patients' privacy and confidentiality.

Congress recognized the need for national patient record privacy standards in 1996 when they enacted the ***Health Insurance Portability and Accountability Act*** of 1996 (HIPAA). The law included provisions designed to save money for health care businesses by ***encouraging electronic transactions***, but it also required ***new safeguards to protect the security and confidentiality of that information.*** The law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. When Congress did not enact such legislation after

three years, the law required the Department of Health and Human Services (HHS) to craft such protections by regulation.

In November 1999, HHS published proposed regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records. During an extended comment period, HHS received more than 52,000 communications from the public. In December 2000, HHS issued a final rule that made significant changes in order to address issues raised by the comments. To ensure that the provisions of the final rule would protect patients' privacy without creating unanticipated consequences that might harm patients' access to care or quality of care, HHS Secretary Tommy G. Thompson opened the final rule for comment for 30 days. After that comment period, President Bush and Secretary Thompson decided to allow the rule to take effect on April 14, 2001, as scheduled, and make appropriate changes in the next year to clarify the requirements and correct potential problems that could threaten access to or quality of care. Secretary Thompson's statement on this issue is available at http://www.hhs.gov/news/press/2001pres/20010412.html.

Compliance Schedule

The final rule took effect on April 14, 2001. As required by the HIPAA law, most covered entities have two full years – until April 14, 2003 – to comply with the final rule's provisions. The law gives HHS the authority to make appropriate changes to the rule prior to the compliance date.

Covered Entities

As required by HIPAA, the final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., electronic billing and funds transfers) electronically.

Information Protected

All medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally, are covered by the final rule.

Consumer Control Over Health Information

Under the final rule, patients will have significant new rights to understand and control how their health information is used.

- **Patient education on privacy protections.** Providers and health plans will be required to give patients a clear written explanation of how the covered entity may use and disclose their health information.

- **Ensuring patient access to their medical records.** Patients will be able to see and get copies of their records, and request amendments. In addition, a history of non-routine disclosures must be made accessible to patients.

- **Receiving patient consent before information is released.** Health care providers who see patients will be required to obtain patient consent before sharing their information for treatment, payment, and health care operations. In addition, separate patient authorization must be obtained for non-routine disclosures and most non-health care purposes. Patients will have the right to request restrictions on the uses and disclosures of their information.

- **Providing recourse if privacy protections are violated.** People will have the right to file a formal complaint with a covered provider or health plan, or with HHS, about violations of the provisions of this rule or the policies and procedures of the covered entity.

Boundaries On Medical Record Use And Release

With few exceptions, such as appropriate law enforcement needs, an individual's health information may only be used for health purposes.

- **Ensuring that health information is not used for non-health purposes.** Health information covered by the rule generally may not be used for purposes not related to health care – such as disclosures to employers to make personnel decisions, or to financial institutions – without explicit authorization from the individual.

- **Providing the minimum amount of information necessary**. In general, disclosures of information will be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the disclosure of medical records for treatment purposes because physicians, specialists, and other providers need access to the full record to provide quality care.

Ensure Security of Personal Health Information

The final rule establishes the privacy safeguard standards that covered entities must meet, but it gives covered entities the flexibility to design their own policies and procedures to meet those standards. The requirements are flexible and scalable to account for the nature of each entity's business, and its size and resources. Covered entities generally will have to:

- **Adopt written privacy procedures.** These include who has access to protected information, how it will be used within the entity, and when the information may be disclosed. Covered entities will also need to take steps to ensure that their business associates protect the privacy of health information.

- **Train employees and designate a privacy officer.** Covered entities will need to train their employees in their privacy procedures, and must designate an individual to be responsible for ensuring the procedures are followed.

Establish Accountability For Medical Records

In HIPAA, Congress provided penalties for covered entities that misuse personal health information.

- **Civil penalties**. Health plans, providers and clearinghouses that violate these standards will be subject to civil liability. Civil money penalties are $100 per violation, up to $25,000 per person, per year for each requirement or prohibition violated.

- **Federal criminal penalties.** Under HIPAA, Congress also established criminal penalties for knowingly violating patient privacy. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to ***$250,000 and up to 10 years in prison*** for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

Balancing Public Responsibility With Privacy Protections

In limited circumstances, the final rule permits – but does not require – covered entities to continue certain existing disclosures of health information without individual authorization for specific public responsibilities.

These permitted disclosures include: emergency circumstances; identification of the body of a deceased person, or the cause of death; public health needs; research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board; oversight of the health care system; judicial and administrative proceedings; limited law enforcement activities; and activities related to national defense and security.

All of these disclosures could occur today under existing laws and regulations, although the privacy rule generally establishes new safeguards and limits. If there is no other law requiring that information be disclosed, covered entities will use their professional judgments to decide whether to disclose any information, reflecting their own policies and ethical principles.

Special Protection For Psychotherapy Notes

Psychotherapy notes (used only by a psychotherapist) are held to a higher standard of protection because they are not part of the medical record and are never intended to be shared with anyone else. All other personal health information is considered to be sensitive and protected consistently under this rule.

Government Entities

The provisions of the final rule generally apply equally to private sector and public sector entities. For example, both private hospitals and government medical units have to comply with the full range of requirements, such as providing notice, access rights and requiring consent for routine uses.

Cost of Implementation

The final rule projected the implementation costs at $17.6 billion over 10 years – a figure more than offset by the $29.9 billion in projected savings under the final electronic transactions regulation issued in August 2000.

State Confidentiality Laws

As required by the HIPAA law itself, stronger state laws (like those covering mental health, HIV infection, and AIDS information) continue to apply. These confidentiality protections are cumulative; the final rule will set a national "floor" of privacy standards that protect all Americans, but in some states individuals enjoy additional protection. In circumstances where states have decided through law to require certain disclosures of health information, the final rule does not preempt these mandates.

Compliance and Enforcement

The final rule will be enforced by the HHS Office for Civil Rights (OCR). Before covered entities must comply with the rule, OCR will provide assistance to providers, plans and health clearinghouses in meeting the requirements of the regulation. A Web site on the new regulation is available at http://www.hhs.gov/ocr/hipaa/.

Note: All HHS press releases, fact sheets and other press materials are available at www.hhs.gov/news.

NAIC Model Regulations

The NAIC created Model regulations for HIPAA, entitled the ”Privacy of Consumer Financial and Health Information Model Regulation.” Some states have adopted some or all of these regulations which you can view below.

R590-206-2. Purpose and Scope.
(1) Purpose. This rule governs the treatment of nonpublic personal health information and nonpublic personal financial information about individuals by all licensees of the Utah Insurance Department. This rule:
(a) Requires a licensee to provide notice to individuals about its privacy policies and practices;
(b) Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal financial information about individuals to affiliates and nonaffiliated third parties; and
(c) Provides methods for individuals to prevent a licensee from disclosing that information.

(2) Scope. This rule applies to:
(a) Nonpublic personal financial information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This rule does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and
(b) All nonpublic personal health information…

(3) This rule does not apply to a financial institution, securities broker or dealer, or a credit union that engages in activities or functions that do not require a license from the Utah insurance commissioner…

R590-206-4. Definitions.
As used in this rule, unless the context requires otherwise:

(1) "Affiliate" means any company that controls, is controlled by or is under common control with another company.

(2)(a) "Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice…

(3) "Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

(4) "Commissioner" means the Utah insurance commissioner.

(5) "Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

(6)(a) “Consumer” is defined as listed earlier in the discussion of Utah’s *Standards for Standards for Safeguarding Customer Information…*

(7) "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

(8) "Control" means:
(a) Ownership, control or power to vote 25% or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;
(b) Control in any manner over the election of a majority of the directors, trustees or general partners, or individuals exercising similar functions, of the company; or
(c) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.

(9) "Customer" is defined as listed earlier in the discussion of Utah's *Standards for Standards for Safeguarding Customer Information…*

(10)(a) "Customer relationship" is defined as listed earlier in the discussion of Utah's *Standards for Standards for Safeguarding Customer Information…*

(11) (a) "Financial institution" means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).
(b) Financial institution does not include:
(i) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 et seq.);
(ii) The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.); or
(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

(12) (a) "Financial product or service" means any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section (4)(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).
(b) Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

(13) "Health care" means:
(a) Preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, services, procedures, tests or counseling that:
(i) Relates to the physical, mental or behavioral condition of an individual; or
(ii) Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs or any other tissue; or
(b) Prescribing, dispensing or furnishing to an individual drugs or biologicals, or medical devices or health care equipment and supplies.

(14) "Health care provider" means a physician or other health care practitioner licensed, accredited or certified to perform specified health services consistent with state law, or a health care facility.

(15) "Health information" means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:
(a) The past, present or future physical, mental or behavioral health or condition of an individual;
(b) The provision of health care to an individual; or
(c) Payment for the provision of health care to an individual.
(16) (a) "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.
(b) Insurance service includes a licensee's evaluation, brokerage or distribution of information that the licensee collects in connection with a request or an application from a consumer for a insurance product or service.

(17) (a) "Licensee" is defined as listed earlier in the discussion of Utah's *Standards for Standards for Safeguarding Customer Information…*

(18) (a) "Nonaffiliated third party" means any person except:
(i) A licensee's affiliate; or
(ii) A person employed jointly by a licensee and any company that is not the licensee's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).
(b) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Subsection R590-206-4.(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

(19) "Nonpublic personal information" means nonpublic personal financial information and nonpublic personal health information.

(20) (a) "Nonpublic personal financial information" means:
(i) Personally identifiable financial information; and
(ii) Any list, description or other grouping of consumers, and publicly available information pertaining to them, that is derived using any personally identifiable financial information that is not publicly available.
(b) Nonpublic personal financial information does not include:
(i) Health information
(ii) Publicly available information, except as included on a list described in Subsection R590-206-4.(20)(a)(ii); or
(iii) Any list, description or other grouping of consumers, and publicly available information pertaining to them, that is derived without using any personally identifiable financial information that is not publicly available…

(21) "Nonpublic personal health information" means health information:
(a) That identifies an individual who is the subject of the information; or
(b) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.

(22) (a) "Personally identifiable financial information" means any information:
(i) A consumer provides to a licensee to obtain an insurance product or service from the licensee;
(ii) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(iii) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.
(b) Examples.
(i) Information included. Personally identifiable financial information includes:
(A) Information a consumer provides to a licensee on an application to obtain an insurance product or service;
(B) Account balance information and payment history;
(C) The fact that an individual is or has been one of the licensee's customers or has obtained an insurance product or service from the licensee;
(D) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;
(E) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;
(F) Any information the licensee collects through an Internet cookie, an information-collecting device from a web server; and
(G) Information from a consumer report.
(ii) Information not included. Personally identifiable financial information does not include:
(A) Health information;
(B) A list of names and addresses of customers of an entity that is not a financial institution; and
(C) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

(23) (a) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:
(i) Federal, state or local government records;
(ii) Widely distributed media; or
(iii) Disclosures to the general public that are required to be made by federal, state or local law.
(b) Reasonable basis. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:
(i) That the information is of the type that is available to the general public; and
(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee's consumer has not done so…

A notice that discloses the insurer's privacy policy must be provided to customers no later than when a customer relationship is established:

R590-206-5. Initial Privacy Notice to Consumers Required.

(1) Initial notice requirement. A licensee shall provide clear and conspicuous notice that accurately reflects its privacy policies and practices to:
(a) Customer. An individual who becomes the licensee's customer, not later than when the licensee establishes a customer relationship, except as provided in Subsection R590-206-5.(5) of this section; and

A notice that discloses the insurer's privacy policy must be provided to consumers before any nonpublic personal financial information is disclosed to any nonaffiliated third party, unless the disclosure fits under one of the exceptions listed under Sections 15 and 16:
(b) Consumer. A consumer, before the licensee discloses any nonpublic personal financial information about the consumer to any nonaffiliated third party, if the licensee makes a disclosure other than as authorized by Sections 15 and 16.

There are times when the disclosure is not required:

(2) When initial notice to a consumer is not required. A licensee is not required to provide an initial notice to a consumer under Subsection R590-206-5.(1)(b) of this section if:
(a) The licensee does not disclose any nonpublic personal financial information about the consumer to any nonaffiliated third party, other than as authorized by Sections 15 and 16, and the licensee does not have a customer relationship with the consumer; or
(b) A notice has been provided by an affiliated licensee, as long as the notice clearly identifies all licensees to whom the notice applies and is accurate with respect to the licensee and the other institutions.

The trigger event for the requirement of providing the privacy notice is when the licensee establishes a customer relationship. This is explained next:

(3) When the licensee establishes a customer relationship.
(a) General rule. A licensee establishes a customer relationship at the time the licensee and the consumer enter into a continuing relationship.
(b) Examples of establishing customer relationship. A licensee establishes a customer relationship when the consumer:
(i) Becomes a policyholder of a licensee that is an insurer when the insurer delivers an insurance policy or contract to the consumer, or in the case of a licensee that is an insurance producer or insurance broker, obtains insurance through that licensee; or
(ii) Agrees to obtain financial, economic or investment advisory services relating to insurance products or services for a fee from the licensee.

(4) Existing customers. When an existing customer obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection R590-206-5.(1) of this section as follows:
(a) The licensee may provide a revised policy notice, under Section 9, that covers the customer's new insurance product or service; or (b) If the initial, revised or annual notice that the licensee most recently provided to that customer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new privacy notice under Subsection R590-206-5.(1) of this section…

(5) Delivery. When a licensee is required to deliver an initial privacy notice by this section, the licensee shall deliver it according to Section 10. If the licensee uses a short-form initial notice for non-customers according to Subsection R590-206-7.(4) the licensee may deliver its privacy notice according to Subsection R590-206-7.(4)(c).

Notice is also required annually after the customer relationship has been established: *R590-206-6. Annual Privacy Notice to Customers Required.*

(1) (a) General rule. A licensee shall provide a clear and conspicuous notice to customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship. Annually means at least once in any period of 12 consecutive months during which that relationship exists. A licensee may define the 12 consecutive month period, but the licensee shall apply it to the customer on a consistent basis…
(2) (a) Termination of customer relationship. A licensee is not required to provide an annual notice to a former customer. A former customer is an individual with whom a licensee no longer has a continuing relationship…

(3) Delivery. When a licensee is required by this section to deliver an annual privacy notice, the licensee shall deliver it according to Section 10.

The information that must be included in the privacy notice is spelled out in the regulations:
R590-206-7. Information to be Included in Privacy Notices.

(1) General rule. The initial, annual and revised privacy notices that a licensee provides under Sections 5, 6 and 9 shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its privacy notice:
(a) The categories of nonpublic personal financial information that the licensee collects;
(b) The categories of nonpublic personal financial information that the licensee discloses;
(c) The categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information, other than those parties to whom the licensee discloses information under Sections 15 and 16;
(d) The categories of nonpublic personal financial information about the licensee's former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information about the licensee's former customers, other than those parties to whom the licensee discloses information under Sections 15 and 16;
(e) If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under Section 14, and no other exception in Sections 15 and 16 applies to that disclosure, a separate description of the categories of information the licensee discloses and the categories of third parties with whom the licensee has contracted;
(f) An explanation of the consumer's right under Subsection R590-206-11.(1) to opt out of the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;
(g) Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);
(h) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal financial information; and
(i) Any disclosure that the licensee makes under Subsection R590-206-7.(2).

(2) Description of parties subject to exceptions. If a licensee discloses nonpublic personal financial information as authorized under Sections 15 and 16, the licensee is not required to list those exceptions in the initial or annual privacy notices required by Sections 5 and 6. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law…

Consumers (not customers) may be provided a short-form of notice in certain circumstances:

(3) Short-form initial notice with opt out notice for non-customers.
(a) A licensee may satisfy the initial notice requirements in Subsections R590-206-5.(1)(b) and Subsection R590-206-8.(3) for a consumer who is not a customer by providing a short-form initial notice at the same time as the licensee delivers an opt out notice as required in Section 8.
(b) A short-form initial notice shall:
(i) Be clear and conspicuous;
(ii) State that the licensee's privacy notice is available upon request; and
(iii) Explain a reasonable means by which the consumer may obtain that notice.
(c) The licensee shall deliver its short-form initial notice according to Section 10. The licensee is not required to deliver its privacy notice with its short-form initial notice. The licensee instead may simply provide the consumer a reasonable means to obtain its privacy notice. If a

consumer who receives the licensee's short-form notice requests the licensee's privacy notice, the licensee shall deliver its privacy notice according to Section 10.

The regulations state that the short-form notice must include a reasonable method for the consumer to obtain the privacy notice:
(d) Examples of obtaining privacy notice. The licensee provides a reasonable means by which a consumer may obtain a copy of its privacy notice if the licensee:
(i) Provides a toll-free telephone number that the consumer may call to request the notice; or
(ii) For a consumer who conducts business in person at the licensee's office, maintains copies of the notice on hand that the licensee provides to the consumer immediately upon request.

Although the insurer may not be currently disclosing certain types of information, the insurer may reserve the right to disclose the information in the future:

(4) Future disclosures. The licensee's notice may include:
(a) Categories of nonpublic personal financial information that the licensee reserves the right to disclose in the future, but does not currently disclose; and
(b) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal financial information...

Under the regulations, opt-out notices must include specific information:
R590-206-8. Form of Opt Out Notice to Consumers and Opt Out Methods.

(1) (a) Form of opt out notice. If a licensee is required to provide an opt out notice under Subsection R590-206-11.(1), it shall provide a clear and conspicuous notice to each of its consumers that accurately explains the right to opt out under that section. The notice shall state:
(i) That the licensee discloses or reserves the right to disclose nonpublic personal financial information about its consumer to a nonaffiliated third party;
(ii) That the consumer has the right to opt out of that disclosure; and
(iii) A reasonable means by which the consumer may exercise the opt out right…

(2) Same form as initial notice permitted. A licensee may provide the opt out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 5.

(3) Initial notice required when opt out notice delivered subsequent to initial notice. If a licensee provides the opt out notice later than required for the initial notice in accordance with Section 5, the licensee shall also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

(4) Joint relationships.
(a) If two or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt out notice. The licensee's opt out notice shall explain how the licensee will treat an opt out direction by a joint consumer, as explained in Subsection R590-206-8.(4)(e).
(b) Any of the joint consumers may exercise the right to opt out. The licensee may either:
(i) Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or
(ii) Permit each joint consumer to opt out separately.
(c) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all of the joint consumers.

(d) A licensee may not require all joint consumers to opt out before it implements any opt out direction…

(5) Time to comply with opt out. A licensee shall comply with a consumer's opt out direction as soon as reasonably practicable after the licensee receives it.

(6) Continuing right to opt out. A consumer may exercise the right to opt out at any time.

(7) Duration of consumer's opt out direction.
(a) A consumer's direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.
(b) When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal financial information that the licensee collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with the licensee, the opt out direction that applied to the former relationship does not apply to the new relationship.

(8) Delivery. When a licensee is required to deliver an opt out notice by this section, the licensee shall deliver it according to Section 10.

If the insurer changes its privacy policies, it must inform the consumers before making the changes, giving consumers the opportunity to opt-out.

R590-206-9. Revised Privacy Notices.

(1) General rule. Except as otherwise authorized in this rule, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party other than as described in the initial notice that the licensee provided to that consumer under Section 5, unless:
(a) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;
(b) The licensee has provided to the consumer a new opt out notice;
(c) The licensee has given the consumer a reasonable opportunity,
before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and
(d) The consumer does not opt out…

(2) Delivery. When a licensee is required to deliver a revised privacy notice by this section, the licensee shall deliver it according to Section 10.

Section 10 provides the requirements of delivering the privacy notices. It includes the delivery circumstances that meet the “reasonable expectation” standard, meaning that it can be reasonably expected that the consumer has been delivered the notice.

R590-206-10. Delivery.

(1) How to provide notices. A licensee shall provide any notices that this rule requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically.

(2) (a) Examples of reasonable expectation of actual notice. A licensee may reasonably expect that a consumer will receive actual notice if the licensee:
(i) Hand-delivers a printed copy of the notice to the consumer;

(ii) Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;
(iii) For a consumer who conducts transactions electronically, posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;
(iv) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.

The regulations also include what circumstances do not meet the “reasonable expectation” standard:
(b) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:
(i) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or
(ii) Sends the notice via electronic mail to a consumer who does not obtain an insurance product or service from the licensee electronically.

(3) Annual notices only. A licensee may reasonably expect that a customer will receive actual notice of the licensee's annual privacy notice if:
(a) The customer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or
(b) The customer has requested that the licensee refrain from sending any information regarding the customer relationship, and the licensee's current privacy notice remains available to the customer upon request.

(4) Oral description of notice insufficient. A licensee may not provide any notice required by this rule solely by orally explaining the notice, either in person or over the telephone.

(5) Retention or accessibility of notices for customers.
(a) For customers only, a licensee shall provide the initial notice required by Subsection R590-206-5.(1)(a), the annual notice required by Subsection R590-206-6.(1), and the revised notice required by Section 9 so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.
(b) Examples of retention or accessibility. A licensee provides a privacy notice to the customer so that the customer can retain it or obtain it later if the licensee:
(i) Hand-delivers a printed copy of the notice to the customer;
(ii) Mails a printed copy of the notice to the last known address of the customer; or
(iii) Makes its current privacy notice available on a web site (or a link to another web site) for the customer who obtains an insurance product or service electronically and agrees to receive the notice at the web site.

(6) Joint notice with other financial institutions. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.

(7) Joint relationships. If two or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of

Subsections R590-206-5.(1), 6.(1) and 9.(1), respectively, by providing one notice to those consumers jointly.

One of the key features of these privacy regulations is that financial institutions must disclose, and allow the consumer to opt-out of, the information sharing between the financial institutions and nonaffiliated third parties.

R590-206-11. Limits on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties.

(1) (a) Conditions for disclosure. Except as otherwise authorized in this rule, a licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party unless:
(i) The licensee has provided to the consumer an initial notice as required under Section 5;
(ii) The licensee has provided to the consumer an opt out notice as required in Section 8;
(iii) The licensee has given the consumer a reasonable opportunity, before it discloses the information to the nonaffiliated third party, to opt out of the disclosure; and
(iv) The consumer does not opt out.

The regulations also provide examples of when a consumer is given a reasonable opportunity to opt out of the insurer's information sharing with a nonaffiliated third party:

(b) Opt out definition. Opt out means a direction by the consumer that the licensee not disclose nonpublic personal financial information about that consumer to a nonaffiliated third party, other than as permitted by Sections 14, 15 and 16.
(c) Examples of reasonable opportunity to opt out. A licensee provides a consumer with a reasonable opportunity to opt out if:
(i) By mail. The licensee mails the notices required in Subsection R590-206-11.(1)(a) to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within 30 days from the date the licensee mailed the notices.
(ii) By electronic means. A customer opens an on-line account with a licensee and agrees to receive the notices required in Subsection R590-206-11.(1)(a) electronically, and the licensee allows the customer to opt out by any reasonable means within 30 days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.
(iii) Isolated transaction with consumer. For an isolated transaction such as providing the consumer with an insurance quote, a licensee provides the consumer with a reasonable opportunity to opt out if the licensee provides the notices required in Subsection R590-206-11.

(1)(a) at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

(2) Application of opt out to all consumers and all nonpublic personal financial information.
(a) A licensee shall comply with this section, regardless of whether the licensee and the consumer have established a customer relationship.
(b) Unless a licensee complies with this section, the licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer that the licensee has collected, regardless of whether the licensee collected it before or after receiving the direction to opt out from the consumer.

(3) Partial opt out. A licensee may allow a consumer to select certain nonpublic personal financial information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out…

In order to protect the consumer's identity, the regulations also include limits on sharing account numbers. The purpose of these rules is to help make sure that no one gains unauthorized access to a consumer's accounts, such as for identity theft purposes:

R590-206-13. Limits on Sharing Account Number Information for Marketing Purposes.

(1) General prohibition on disclosure of account numbers. A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

(2) Exceptions. R590-206-13.(1) does not apply if a licensee discloses a policy number or similar form of access number or access code:
(a) To the licensee's service provider solely in order to perform marketing for the licensee's own products or services, as long as the service provider is not authorized to directly initiate charges to the account;
(b) To a licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or
(c) To a participant in an affinity or similar program where the participants in the program are identified to the customer when the customer enters into the program.

(3) Examples.
(a) Policy number. A policy number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as the licensee does not provide the recipient with a means to decode the number or code.
(b) Policy or transaction account. For the purposes of this section, a policy or transaction account is an account other than a deposit account or a credit card account. A policy or transaction account does not include an account to which third parties cannot initiate charges.

Sometimes an insurer may enter into an agreement with a third party to provide services to the insurer, or provide services on behalf of the insurer. The regulations also address the privacy requirements of these relationships:

R590-206-14. Exception to Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information for Service Providers and Joint Marketing.

(1) General rule.
(a) The opt out requirements in Sections 8 and 11 do not apply when a licensee provides nonpublic personal financial information to a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf, if the licensee:
(i) Provides the initial notice in accordance with Section 5; and
(ii) Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections 15 or 16 in the ordinary course of business to carry out those purposes.
(b) Example. If a licensee discloses nonpublic personal financial information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of Paragraph (1)(b) of this subsection if it prohibits the institution from disclosing or using the nonpublic personal financial

information except as necessary to carry out the joint marketing or under an exception in Sections 15 or 16 in the ordinary course of business to carry out that joint marketing.

(2) Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under Subsection R590-206-14.(1) of this section may include marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and one or more financial institutions.

(3) Definition of "joint agreement." For purposes of this section, "joint agreement" means a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Some information sharing is necessary, even when it includes nonpublic personal financial information. Following is “Section 15”, cited several times in these rules as containing exceptions to disclosure and opt out requirements:

R590-206-15. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information for Processing and Servicing Transactions.

(1) Exceptions for processing transactions at consumer's request.
The requirements for initial notice in Subsection R590-206-5.(1)(b), the opt out in Sections 8 and 11, and service providers and joint marketing provisions in Section 14 do not apply if the licensee discloses nonpublic personal financial information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or to enforce a contractual obligation or other legal claim against a customer, or in connection with:
(a) Servicing or processing an insurance product or service that a consumer requests or authorizes;
(b) Maintaining or servicing the consumer's account with a licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;
(c) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or
(d) Reinsurance or stop loss or excess loss insurance.

(2) "Necessary to effect, administer or enforce a transaction" means that the disclosure is:
(a) Required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or
(b) Required, or is a usual, appropriate or acceptable method:
(i) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the insurance product or service;
(ii) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;
(iii) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer's agent or broker;
(iv) To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;
(v) To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits, including utilization review activities,

participating in research projects or as otherwise required or specifically permitted by federal or state law; or
(vi) In connection with:
(A) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;
(B) The transfer of receivables, accounts or interests therein; or
(C) The audit of debit, credit or other payment information.

Section 16 is the other Section that includes exceptions to the notice and opt out rules:

R590-206-16. Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information.

(1) Exceptions to opt out requirements. The requirements for initial notice to consumers in Subsection R590-206-5.(1)(b), the opt out in Sections 8 and 11, and service providers and joint marketing in Section 14 do not apply when a licensee discloses nonpublic personal financial information:
(a) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;
(b)(i) To protect the confidentiality or security of a licensee's records pertaining to the consumer, service, product or transaction;
(ii) To protect against or prevent actual or potential fraud or unauthorized transactions;
(iii) For required institutional risk control or for resolving consumer disputes or inquiries;
(iv) To persons holding a legal or beneficial interest relating to the consumer; or
(v) To persons acting in a fiduciary or representative capacity on behalf of the consumer;
(c) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee's compliance with industry standards, and the licensee's attorneys, accountants and auditors;
(d) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21, Financial Record keeping, a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;
(e)(i) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or
(ii) From a consumer report reported by a consumer reporting agency;
(f) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal financial information concerns solely consumers of the business or unit;
(g)(i) To comply with federal, state or local laws, rules and other applicable legal requirements;
(ii) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities;
(iii) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or
(h) For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers' compensation policy.

(2) A licensed or admitted insurer that is the subject of a formal delinquency proceeding under Sections 31A-27-303, 31A-27-307 and 31A-27-310, are not subject to the requirements of R590-206-5.(1)(b), the opt out in Sections (8) and (11), and other notice requirements of R590-206.

(3) Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal financial information as permitted under Subsection R590-206-8.(6).

The agent must be careful not to disclose any personal health information about consumers or clients, unless the agent has received authorization:

R590-206-17. When Authorization Required for Disclosure of Nonpublic Personal Health Information.

(1) General Rule. A licensee shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed.

(2) Exceptions. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee or an affiliate of the licensee: claims administration; claims adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; underwriting; policy placement, issuance or renewal; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; actuarial, scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan or workers compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services; disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.

Authorizations to disclosure personal health information must meet the following requirements:
R590-206-18. Authorizations.

(1) A valid authorization to disclose nonpublic personal health information pursuant to Sections 17 though 21 shall be in written or electronic form and shall contain all of the following:
(a) The identity of the consumer or customer who is the subject of the nonpublic personal health information;
(b) A general description of the types of nonpublic personal health information to be disclosed;
(c) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(d) The signature of the consumer or customer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and
(e) Notice of the length of time for which the authorization is valid and that the consumer or customer may revoke the authorization at any time and the procedure for making a revocation.

(2) An authorization for the purposes of Sections 17 through 21 shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than 24 months.

(3) A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to Sections 17 through 21 at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

(4) A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

No discrimination is allowed against a customer or consumer who opts out of allowing the insurer to disclose personal information:

R590-206-23. Nondiscrimination.

(1) A licensee shall not unfairly discriminate against any consumer or customer because that consumer or customer has opted out from the disclosure of his or her nonpublic personal financial information pursuant to the provisions of this rule.

(2) A licensee shall not unfairly discriminate against a consumer or customer because that consumer or customer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this rule.

If any licensee violates these rules, the Insurance Department has the right to take action, including assessing penalties and revoking the license:

R590-206-24. Violation.

Pursuant to Section 31A-23-302, the commissioner finds that the failure to observe the requirements of this rule is misleading to the public and individuals transacting business with licensees of the department or any person or individual who should be licensed by the department. The failure to observe the requirements of this rule is also an unreasonable restraint on competition. Violation of any provisions of the rule will result in appropriate enforcement action by the department which may include forfeiture, penalties, and revocation of license.

Federal Legislation

The main pieces of federal legislation that affect identity theft are the Identity Theft and Assumption Deterrence Act of 1998, the Fair Credit Reporting Act, the Fair and Accurate Credit Transactions Act of 2003, the Fair Credit Billing Act, the Fair Debt Collection Practices Act, and the Electronic Fund Transfer Act.

Identity Theft and Assumption Deterrence Act

A landmark change in identity theft prosecution occurred when the Identity Theft and Assumption Deterrence Act became effective in October 1998.

The Act is important because it establishes that the person whose identity is stolen is truly a victim. This is because the Act defines identity theft as a crime. Previously, in many cases only the credit grantors were considered victims of the crimes. The Act includes provisions for the victim to seek restitution, if the defendant is found guilty.

Prior to the enactment of the law, police would often not investigate identity theft, because they required the creditors to press charges, not the victim. It was the creditor that "ate" the charges racked up by the thief. Creditors did not always prosecute, because of the difficulty of meeting the definition of "fraud" under many state statutes. In addition, fraud does not always fall under sentencing rules commensurate with the seriousness of the crime of identity theft. This legal situation allowed identity thieves to commit the crime without fear of severe punishment. Remember the testimony of Congressman LaTourette from Ohio that was quoted at the beginning of the course? The identity thief he quoted boasted, *"I did not use a gun. I did not use a knife. Call my lawyer and I will plead guilty and they will put me on probation."* The Identity Theft and Assumption Deterrence Act addresses this issue by criminalizing identity theft.

The act includes guidelines on punishment of criminals and helps to regulate sentencing. There is now a maximum fifteen-year sentence and a maximum fine of $250,000 for this crime.

What is Identity Theft Under the Act?

Identity theft is defined under the Identity Theft Act. Title 18, USC 1028, as follows:

Whoever, in a circumstance described in subsection of this section –

(1) knowingly and without lawful authority produces an identification document or a false identification document;
(2) knowingly transfers an identification document or a false identification document knowing that such document was stolen or produced without lawful authority;
(3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor) or false identification documents;
(4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor) or a false identification document, with the intent such document be used to defraud the United States;
(5) knowingly produces, transfers, or possesses a document-making implement with the intent such document-making implement will be used in the production of a false identification document or another document-making implement which will be so used;
(6) knowingly possess an identification document that is or appears to be an identification document of the United States which is stolen or produced without lawful authority knowing that such document was stolen or produced without such authority shall be punished as provided in subsection (b) of this section; or
(7) knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law or that constitutes a felony under any applicable State or local law;
shall be punished as provided in subsection (b) of this section.

This definition means that fraud does not have to be proved in order for identity thieves to be prosecuted. The definition includes a broad array of activities that qualify as identity theft.

What is Punishment Under the Act?

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

The punishment under this Act ranges from three to 25 years, depending on the how much wealth or property is involved in the theft over a one year period, and if the crime is committed in conjunction with drug trafficking, organized crime, a prior conviction, or even terrorism. Generally, if the value of the property aggregated is over $1000, the criminal may receive a fine or imprisonment of not more than three years. If the crime includes transferring a birth certificate, driver's license, or an identification document issued under the authority of the United States, or creating false ID, the criminal may be fined or receive up to fifteen years imprisonment. Criminals who commit identity theft to facilitate a drug trafficking crime, in connection with a crime of violence, or after a prior conviction, the punishment can be a fine or imprisonment of up to 20 years. If identity theft is committed to facilitate an act of international terrorism, the criminal could be imprisoned for up to 25 years.

Including these sentencing guidelines in the Act provides more consistency in the sentencing of these criminals than exists if individual state laws alone are applied.

Schemes to commit identity theft or fraud may also involve violations of other statutes, such as credit card fraud, computer fraud, mail fraud, wire fraud, financial institution fraud, or Social Security fraud. Each of these federal offenses is a felony and carries substantial penalties — in some cases, as high as 30 years in prison as well as fines and criminal forfeiture.

What Else Does the Act Do?

The Act also places the Federal Trade Commission in a position of providing support and services to identity theft victims. The FTC acts as a centralized complaint depository and consumer education service. This course has referred to some of the FTC's identity theft tools, such as the ID Theft Affidavit. The FTC also refers victims to other government agencies that are able to provide other services and support to the victim.

The Fair Credit Reporting Act

The Fair Credit Reporting Act was enacted to ensure that consumer reporting agencies, such as the three credit reporting agencies, adopt reasonable procedures to meet the needs of commerce for consumer credit, personnel, insurance, and other information to better serve the banks, credit agencies, and consumers.

Purpose of the Act

The Act includes the following purpose:

Reasonable procedures. It is the purpose of this title to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the

consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this title.

Purpose of Generating Consumer Reports

The Act includes the allowable purposes for generating a consumer report, which include generating a report in connection with a credit transaction:

§ 604. Permissible purposes of consumer reports [15 U.S.C. § 1681b]
(a) In general. Subject to subsection (c), any consumer reporting agency may furnish a consumer report under the following circumstances and no other:
(1) In response to the order of a court having jurisdiction to issue such an order, or a subpoena issued in connection with proceedings before a Federal grand jury.
(2) In accordance with the written instructions of the consumer to whom it relates.
(3) To a person which it has reason to believe
(A) intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or
(B) intends to use the information for employment purposes; or
(C) intends to use the information in connection with the underwriting of insurance involving the consumer; or
(D) intends to use the information in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status; or
(E) intends to use the information, as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation; or
(F) otherwise has a legitimate business need for the information
(i) in connection with a business transaction that is initiated by the consumer; or
(ii) to review an account to determine whether the consumer continues to meet the terms of the account…

Generating Reports Not Requested by the Consumer

The Act also addresses under what circumstances a report may be generated without the authorization of the consumer. These circumstances are very limited, as is the type of information that may be provided without the consumer's authorization:
(c) Furnishing reports in connection with credit or insurance transactions that are not initiated by the consumer.

(1) In general. A consumer reporting agency may furnish a consumer report relating to any consumer pursuant to subparagraph (A) or (C) of subsection (a)(3) in connection with any credit or insurance transaction that is not initiated by the consumer only if
(A) the consumer authorizes the agency to provide such report to such person; or
(B) (i) the transaction consists of a firm offer of credit or insurance;
(ii) the consumer reporting agency has complied with subsection (e); and
(iii) there is not in effect an election by the consumer, made in accordance with subsection (e), to have the consumer's name and address excluded from lists of names provided by the agency pursuant to this paragraph.

(2) Limits on information received under paragraph (1)(B). A person may receive pursuant to paragraph (1)(B) only
(A) the name and address of a consumer;

(B) an identifier that is not unique to the consumer and that is used by the person solely for the purpose of verifying the identity of the consumer; and

(C) other information pertaining to a consumer that does not identify the relationship or experience of the consumer with respect to a particular creditor or other entity.

(3) Information regarding inquiries. Except as provided in section 609(a)(5) [§ 1681g] (which deal with security and criminal investigations)*, a consumer reporting agency shall not furnish to any person a record of inquiries in connection with a credit or insurance transaction that is not initiated by a consumer.*

Opting Out of Unauthorized Reports

The Act provides a method for consumers to notify consumer reporting agencies that they do not want any unauthorized reports being generated:

(e) Election of consumer to be excluded from lists.

(1) In general. A consumer may elect to have the consumer's name and address excluded from any list provided by a consumer reporting agency under subsection (c)(1)(B) in connection with a credit or insurance transaction that is not initiated by the consumer, by notifying the agency in accordance with paragraph (2) that the consumer does not consent to any use of a consumer report relating to the consumer in connection with any credit or insurance transaction that is not initiated by the consumer.

(2) Manner of notification. A consumer shall notify a consumer reporting agency under paragraph (1)

(A) through the notification system maintained by the agency under paragraph (5); or

(B) by submitting to the agency a signed notice of election form issued by the agency for purposes of this subparagraph.

By taking one's name off these optional reporting lists, the consumer can help limit access to his or her personal information, and thereby reduce the risk of identity theft.

Information In Reports

Generally, unless a credit transaction or employment situation involves large sums of money, consumer reports must follow these rules:

- Bankruptcies over ten years old may not be reported
- Civil suits, civil judgments and arrests over seven years old may not be reported
- Paid tax liens over seven years old may not be reported
- Collection accounts or accounts written off by the creditor over seven years old may not be reported
- Any other adverse item, other than records of convictions of crimes, over seven years old may not be reported.
- If the consumer notifies the reporting agency that any item is disputed, the report must note that the item is disputed

Responsibility to Verify Identity of Report Users

The consumer reporting agency must maintain procedures to verify users of the report, and the purpose for which the report will be used.

§ 607. Compliance procedures [15 U.S.C. § 1681e]

(a) Identity and purposes of credit users. Every consumer reporting agency shall maintain reasonable procedures designed to avoid violations of section 605 [§ 1681c] and to limit the furnishing of consumer reports to the purposes listed under section 604 [§ 1681b] of this title. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. Every consumer reporting agency shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report. No consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a purpose listed in section 604 [§ 1681b] of this title.

Responsibility for Accuracy

The consumer reporting agency also has the responsibility to establish procedures to assure accuracy:

§ 607. (b) Accuracy of report. Whenever a consumer reporting agency prepares a consumer report it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.

Report May Be Disclosed to Consumer in the Case of an Adverse Action

If an adverse action, such as denying credit to the consumer, occurs, the user may disclose the contents of the credit report to the consumer:
§ 607. (c) Disclosure of consumer reports by users allowed. A consumer reporting agency may not prohibit a user of a consumer report furnished by the agency on a consumer from disclosing the contents of the report to the consumer, if adverse action against the consumer has been taken by the user based in whole or in part on the report.

Other Disclosure Rights

A critical part of the Fair Credit Reporting Act in the fight against identity theft is the disclosure rights it includes. Section 609 of the act describes the disclosure provisions:
§ 609. Disclosures to consumers [15 U.S.C. § 1681g
]

(a) Information on file; sources; report recipients. Every consumer reporting agency shall, upon request, and subject to 610(a)(1) [§ 1681h], clearly and accurately disclose to the consumer:

(1) All information in the consumer's file at the time of the request, except that nothing in this paragraph shall be construed to require a consumer reporting agency to disclose to a consumer any information concerning credit scores or any other risk scores or predictors relating to the consumer. *(This provision is amended by the FACT Act, discussed shortly)*

(2) The sources of the information; except that the sources of information acquired solely for use in preparing an investigative consumer report and actually used for no other purpose need not be disclosed: Provided, That in the event an action is brought under this title, such sources shall be available to the plaintiff under appropriate discovery procedures in the court in which the action is brought.

The Act also includes the requirement that “inquiries” be listed in the report. As mentioned earlier, inquiries by unauthorized creditors can be a sign to the consumer that unauthorized credit activity may be occurring:

(3)(A) Identification of each person (including each end-user identified under section 607(e)(1) [§ 1681e]) that procured a consumer report
(i) for employment purposes, during the 2-year period preceding the ate on which the request is made; or
(ii) for any other purpose, during the 1-year period preceding the date on which the request is made.
(B) An identification of a person under subparagraph (A) shall include (i) the name of the person or, if applicable, the trade name (written in full) under which such person conducts business; and
(ii) upon request of the consumer, the address and telephone number of the person.
(C) Subparagraph (A) does not apply if--
(i) the end user is an agency or department of the United States Government that procures the report from the person for purposes of determining the eligibility of the consumer to whom the report relates to receive access or continued access to classified information (as defined in section 604(b)(4)(E)(i)); and
(ii) the head of the agency or department makes a written finding as prescribed under section 604(b)(4)(A).

(4) The dates, original payees, and amounts of any checks upon which is based any adverse characterization of the consumer, included in the file at the time of the disclosure.

(5) A record of all inquiries received by the agency during the 1-year period preceding the request that identified the consumer in connection with a credit or insurance transaction that was not initiated by the consumer…

When the consumer receives his or her consumer report, the credit reporting agency must include a summary of the consumer’s rights as pertains to the information in the credit report.

These rights are expanded under the FACT Act:

(c) Summary of rights required to be included with disclosure.
(1) Summary of rights. A consumerreporting agency shall provide to a consumer, with each written disclosure by the agency to the consumer under this section
(A) a written summary of all of the rights that the consumer has under this title; and
(B) in the case of a consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, a toll-free telephone number established by the agency, at which personnel are accessible to consumers during normal business hours.
(2) Specific items required to be included. The summary of rights required under paragraph (1) shall include
(A) a brief description of this title and all rights of consumers under this title;
(B) an explanation of how the consumer may exercise the rights of the consumer under this title;
(C) a list of all Federal agencies responsible for enforcing any provision of this title and the address and any appropriate phone number of each such agency, in a form that will assist the consumer in selecting the appropriate agency;
(D) a statement that the consumer may have additional rights under State law and that the consumer may wish to contact a State or local consumer protection agency or a State attorney general to learn of those rights; and

(E) a statement that a consumer reporting agency is not required to remove accurate derogatory information from a consumer's file, unless the information is outdated under section 605 [§ 1681c] or cannot be verified.

Procedures for Disputing Information

If identity fraud has occurred, the victim must dispute the incorrect information in the credit report. Disputes also occur when there has simply been some kind of error in the consumer report. The Act provides the rules for disputing report information:

§ 611. Procedure in case of disputed accuracy [15 U.S.C. § 1681i]

(a) Reinvestigations of disputed information.

(1) Reinvestigation required.

(A) In general. If the completeness or accuracy of any item of information contained in a consumer's file at a consumer reporting agency is disputed by the consumer and the consumer notifies the agency directly of such dispute, the agency shall reinvestigate free of charge and record the current status of the disputed information, or delete the item from the file in accordance with paragraph (5), before the end of the 30-day period beginning on the date on which the agency receives the notice of the dispute from the consumer.

(B) Extension of period to reinvestigate. Except as provided in subparagraph (C), the 30-day period described in subparagraph (A) may be extended for not more than 15 additional days if the consumer reporting agency receives information from the consumer during that 30-day period that is relevant to the reinvestigation.

(C) Limitations on extension of period to reinvestigate. Subparagraph (B) shall not apply to any reinvestigation in which, during the 30-day period described in subparagraph (A), the information that is the subject of the reinvestigation is found to be inaccurate or incomplete or the consumer reporting agency determines that the information cannot be verified.

The consumer reporting agency must notify the creditor or other entity that furnished the disputed information that the consumer is disputing it within 5 business days from the date the consumer notifies the agency of the dispute:

(2) Prompt notice of dispute to furnisher of information.

(A) In general. Before the expiration of the 5-business-day period beginning on the date on which a consumer reporting agency receives notice of a dispute from any consumer in accordance with paragraph

(1), the agency shall provide notification of the dispute to any person who provided any item of information in dispute, at the address and in the manner established with the person. The notice shall include all relevant information regarding the dispute that the agency has received from the consumer.

(B) Provision of other information from consumer. The consumer reporting agency shall promptly provide to the person who provided the information in dispute all relevant information regarding the dispute that is received by the agency from the consumer after the period referred to in subparagraph (A) and before the end of the period referred to in paragraph (1)(A).

The consumer reporting agency must notify the consumer if the agency determines the dispute is frivolous or irrelevant within five business days of making this determination:

(3) Determination that dispute is frivolous or irrelevant.

(A) In general. Notwithstanding paragraph (1), a consumer reporting agency may terminate a reinvestigation of information disputed by a consumer under that paragraph if the agency reasonably determines that the dispute by the consumer is frivolous or irrelevant, including by reason of a failure by a consumer to provide sufficient information to investigate the disputed information.

(B) Notice of determination. Upon making any determination in accordance with subparagraph (A) that a dispute is frivolous or irrelevant, a consumer reporting agency shall

notify the consumer of such determination not later than 5 business days after making such determination, by mail or, if authorized by the consumer for that purpose, by any other means available to the agency.

(C) Contents of notice. A notice under subparagraph (B) shall include

(i) the reasons for the determination under subparagraph (A); and

(ii) identification of any information required to investigate the disputed information, which may consist of a standardized form describing the general nature of such information.

The consumer reporting agency is responsible to consider all relevant information when investigating a dispute:

(4) Consideration of consumer information. In conducting any reinvestigation under paragraph (1) with respect to disputed information in the file of any consumer, the consumer reporting agency shall review and consider all relevant information submitted by the consumer in the period described in paragraph (1)(A) with respect to such disputed information.

The consumer reporting agency must delete information that it finds is inaccurate or unverifiable:

(5) Treatment of inaccurate or unverifiable information.

(A) In general. If, after any reinvestigation under paragraph (1) of any information disputed by a consumer, an item of the information is found to be inaccurate or incomplete or cannot be verified, the consumer reporting agency shall promptly delete that item of information from the consumer's file or modify that item of information, as appropriate, based on the results of the reinvestigation.

Information that is deleted subsequent to dispute may only be reinserted in the consumer's file if certain steps are taken to ensure that the information is complete and accurate:

(B) Requirements relating to reinsertion of previously deleted material.

(i) Certification of accuracy of information. If any information is deleted from a consumer's file pursuant to subparagraph (A), the information may not be reinserted in the file by the consumer reporting agency unless the person who furnishes the information certifies that the information is complete and accurate.

(ii) Notice to consumer. If any information that has been deleted from a consumer's file pursuant to subparagraph (A) is reinserted in the file, the consumer reporting agency shall notify the consumer of the reinsertion in writing not later than 5 business days after the reinsertion or, if authorized by the consumer for that purpose, by any other means available to the agency.

(iii) Additional information. As part of, or in addition to, the notice under clause (ii), a consumer reporting agency shall provide to a consumer in writing not later than 5 business days after the date of the reinsertion

(I) a statement that the disputed information has been reinserted;

(II) the business name and address of any furnisher of information contacted and the telephone number of such furnisher, if reasonably available, or of any furnisher of information that contacted the consumer reporting agency, in connection with the reinsertion of such information; and

(III) a notice that the consumer has the right to add a statement to the consumer's file disputing the accuracy or completeness of the disputed information.

The consumer reporting agency is responsible for maintaining procedures to keep deleted information from reappearing in a consumer's file, unless it has been reinserted according to the procedures allowed under the Act:

C) Procedures to prevent reappearance. A consumer reporting agency shall maintain reasonable procedures designed to prevent the reappearance in a consumer's file, and in consumer reports on the consumer, of information that is deleted pursuant to this paragraph (other than information that is reinserted in accordance with subparagraph (B)(i)).

If a consumer reporting agency operates on a nationwide basis, as do the three credit reporting bureaus TransUnion, Experian and Equifax, the agency must have a system for reporting the results of a dispute investigation to the other agencies.

D) Automated reinvestigation system. Any consumer reporting agency that compiles and maintains files on consumers on a nationwide basis shall implement an automated system through which furnishers of information to that consumer reporting agency may report the results of a reinvestigation that finds incomplete or inaccurate information in a consumer's file to other such consumer reporting agencies.

The consumer reporting agency must also provide written notice of the results of a dispute investigation within 5 business days after the completion of the investigation:

(6) Notice of results of reinvestigation.

(A) In general. A consumer reporting agency shall provide written notice to a consumer of the results of a reinvestigation under this subsection not later than 5 business days after the completion of the reinvestigation, by mail or, if authorized by the consumer for that purpose, by other means available to the agency.

(B) Contents. As part of, or in addition to, the notice under subparagraph (A), a consumer reporting agency shall provide to a consumer in writing before the expiration of the 5-day period referred to in subparagraph (A)

(i) a statement that the reinvestigation is completed;

(ii) a consumer report that is based upon the consumer's file as that file is revised as a result of the reinvestigation;

(iii) a notice that, if requested by the consumer, a description of the procedure used to determine the accuracy and completeness of the information shall be provided to the consumer by the agency, including the business name and address of any furnisher of information contacted in connection with such information and the telephone number of such furnisher, if reasonably available;

(iv) a notice that the consumer has the right to add a statement to the consumer's file disputing the accuracy or completeness of the information; and

(v) a notice that the consumer has the right to request under subsection (d) that the consumer reporting agency furnish notifications under that subsection.

(7) Description of reinvestigation procedure. A consumer reporting agency shall provide to a consumer a description referred to in paragraph (6)(B)(iii) by not later than 15 days after receiving a request from the consumer for that description.

If the consumer reporting agency is able to resolve a dispute by deleting inaccurate or unverifiable information no later than 3 business days after being notified by the consumer, than the reporting agency may follow a more streamlined notification process:

(8) Expedited dispute resolution. If a dispute regarding an item of information in a consumer's file at a consumer reporting agency is resolved in accordance with paragraph (5)(A) by the deletion of the disputed information by not later than 3 business days after the date on which the agency receives notice of the dispute from the consumer in accordance with paragraph (1)(A), then the agency shall not be required to comply with paragraphs (2), (6), and (7) with respect to that dispute if the agency

(A) provides prompt notice of the deletion to the consumer by telephone;

(B) includes in that notice, or in a written notice that accompanies a confirmation and consumer report provided in accordance with subparagraph (C), a statement of the consumer's right to request under subsection (d) that the agency furnish notifications under that subsection; and

(C) provides written confirmation of the deletion and a copy of a consumer report on the consumer that is based on the consumer's file after the deletion, not later than 5 business days after making the deletion.

The consumer has the right to file a brief statement concerning the dispute if the reinvestigation does not resolve it:

(b) Statement of dispute. If the reinvestigation does not resolve the dispute, the consumer may file a brief statement setting forth the nature of the dispute. The consumer reporting agency may limit such statements to not more than one hundred words if it provides the consumer with assistance in writing a clear summary of the dispute.

The consumer report must include the consumer's statement about the dispute:

(c) Notification of consumer dispute in subsequent consumer reports. Whenever a statement of a dispute is filed, unless there is reasonable grounds to believe that it is frivolous or irrelevant, the consumer reporting agency shall, in any subsequent consumer report containing the information in question, clearly note that it is disputed by the consumer and provide either the consumer's statement or a clear and accurate codification or summary thereof.

The consumer agency must also furnish notification of deleted information to anyone the consumer would like such notice sent, as long as the person had received a consumer report within a specified period that contained the disputed information that has now been deleted:

(d) Notification of deletion of disputed information. Following any deletion of information which is found to be inaccurate or whose accuracy can no longer be verified or any notation as to disputed information, the consumer reporting agency shall, at the request of the consumer, furnish notification that the item has been deleted or the statement, codification or summary pursuant to subsection (b) or (c) of this section to any person specifically designated by the consumer who has within two years prior thereto received a consumer report for employment purposes, or within six months prior thereto received a consumer report for any other purpose, which contained the deleted or disputed information.

The FACT Act

On December 5, 2003, the Fair and Accurate Credit Transactions Act was signed into law by President Bush. This Act includes the following provisions that impact identity theft:

- Gives consumers the right to view their credit report for free once each year
- Requires merchants the leave all but the last five digits of a credit card number off store and restaurant receipts
- Creates a national system of fraud detection so that identity thieves can be caught more easily
- Establishes a nationwide system of fraud alerts for consumers to place on credit files

The Act amends and appends several sections of the Fair Credit Reporting Act. Changes were implemented in 2004.

Free Credit Reports

The FACT Act includes several provisions related to providing free credit reports annually. One provision allows a free credit report if a fraud alert is placed with the credit bureau:

''(2) ACCESS TO FREE REPORTS.—In any case in which a consumer reporting agency includes a fraud alert in the file of a consumer pursuant to this subsection, the consumer reporting agency shall—

''(A) disclose to the consumer that the consumer may request a free copy of the file of the consumer pursuant to section 612(d); and

‘‘(B) provide to the consumer all disclosures required to be made under section 609, without charge to the consumer, not later than 3 business days after any request described in subparagraph (A).

Another provision allows for one free consumer report annually, as long as the request is made through the new centralized, streamlined process that is to be developed under the provisions of the Act. It is expected that this process will be in place within one year after the effective date of the Act, or by the end of 2004 :

‘‘(a) FREE ANNUAL DISCLOSURE.—
‘‘(1) NATIONWIDE CONSUMER REPORTING AGENCIES.—
‘‘(A) IN GENERAL.—All consumer reporting agencies described in subsections (p) and (w) of section 603 shall make all disclosures pursuant to section 609 once during any 12-month period upon request of the consumer and without charge to the consumer.
‘‘(B) CENTRALIZED SOURCE.—Subparagraph (A) shall apply with respect to a consumer reporting agency described in section 603(p) only if the request from the consumer is made using the centralized source established for such purpose in accordance with section 211(c) of the Fair and Accurate Credit Transactions Act of 2003.
‘‘(C) NATIONWIDE SPECIALTY CONSUMER REPORTING AGENCY.—
‘‘(i) IN GENERAL.—The Commission shall prescribe regulations applicable to each consumer reporting agency described in section 603(w) to require the establishment of a streamlined process for consumers to request consumer reports under subparagraph (A), which shall include, at a minimum, the establishment by each such agency of a toll-free telephone number for such requests.
‘‘(ii) CONSIDERATIONS.—In prescribing regulations under clause (i), the Commission shall consider—
‘‘(I) the significant demands that may be placed on consumer reporting agencies in providing such consumer reports;
‘‘(II) appropriate means to ensure that consumer reporting agencies can satisfactorily meet those demands, including the efficacy of a system of staggering the availability to consumers of such consumer reports; and
‘‘(III) the ease by which consumers should be able to contact consumer reporting agencies with respect to access to such consumer reports.
‘‘(iii) DATE OF ISSUANCE.—The Commission shall issue the regulations required by this subparagraph in final form not later than 6 months after the date of enactment of the Fair and Accurate Credit Transactions Act of 2003.

‘‘(iv) CONSIDERATION OF ABILITY TO COMPLY.—The regulations of the Commission under this subparagraph shall establish an effective date by which each nationwide specialty consumer reporting agency (as defined in section 603(w)) shall be required to comply with subsection (a), which effective date—
‘‘(I) shall be established after consideration of the ability of each nationwide specialty consumer reporting agency to comply with subsection (a);
and
‘‘(II) shall be not later than 6 months after the date on which such regulations are issued in final form (or such additional period not to exceed 3 months, as the Commission determines appropriate).

When a consumer requests a report under the new annual report provisions, the consumer reporting agency must provide it no later than 15 days after it is requested:

‘‘(2) TIMING.—A consumer reporting agency shall provide a consumer report under paragraph (1) not later than 15 days after the date on which the request is received under paragraph (1).
‘‘(3) REINVESTIGATIONS.—Notwithstanding the time periods specified in section 611(a)(1), a reinvestigation under that section by a consumer reporting agency upon a request of a

consumer that is made after receiving a consumer report under this subsection shall be completed not later than 45 days after the date on which the request is received.
''(4) EXCEPTION FOR FIRST 12 MONTHS OF OPERATION.—This subsection shall not apply to a consumer reporting agency that has not been furnishing consumer reports to third parties on a continuing basis during the 12-month period preceding a request under paragraph (1), with respect to consumers residing nationwide.''

One Call Fraud Alert Provisions

Even though the Fair Credit Reporting Act requires the credit bureaus that operate nationally to pass on the results of dispute investigations to the other national bureaus, this does not always occur, and the FTC currently recommends that victims contact all three credit bureaus about disputed information. The FACT Act amends the Fair Credit Reporting Act to allow for victims to contact just one bureau to place a fraud alert, and requires the bureaus to pass the fraud alert on to the other bureaus:

605A. Identity theft prevention; fraud alerts and active duty alerts

''(a) ONE-CALL FRAUD ALERTS.—
''(1) INITIAL ALERTS.—Upon the direct request of a consumer, or an individual acting on behalf of or as a personal representative of a consumer, who asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft, a consumer reporting agency described in section 603(p) that maintains a file on the consumer and has received appropriate proof of the identity of the requester shall—
''(A) include a fraud alert in the file of that consumer, and also provide that alert along with any credit score generated in using that file, for a period of not less than 90 days, beginning on the date of such request, unless the consumer or such representative requests that such fraud alert be removed before the end of such period, and the agency has received appropriate proof of the identity of the requester for such purpose; and
''(B) refer the information regarding the fraud alert under this paragraph to each of the other consumer reporting agencies described in section 603(p), in accordance with procedures developed under section 621(f).

Many identity theft victims have resulting problems with their credit for years. Recognizing this, the FACT Act includes provisions for fraud alerts to be reported along with generated credit reports for up to seven years. It also provides for the consumer who has submitted an identity theft report to be omitted from any lists of consumers created as part of a "transaction not initiated by the consumer":

''(b) EXTENDED ALERTS.—

''(1) IN GENERAL.—Upon the direct request of a consumer, or an individual acting on behalf of or as a personal representative of a consumer, who submits an identity theft report to a consumer reporting agency described in section 603(p) that maintains a file on the consumer, if the agency has received appropriate proof of the identity of the requester, the agency shall—
''(A) include a fraud alert in the file of that consumer, and also provide that alert along with any credit score generated in using that file, during the 7-year period beginning on the date of such request, unless the consumer or such representative requests that such fraud alert be removed before the end of such period and the agency has received appropriate proof of the identity of the requester for such purpose;
''(B) during the 5-year period beginning on the date of such request, exclude the consumer from any list of consumers prepared by the consumer reporting agency and provided to any third party to offer credit or insurance to the consumer as part of a transaction that was not initiated

by the consumer, unless the consumer or such representative requests that such exclusion be rescinded before the end of such period; and
‘‘(C) refer the information regarding the extended fraud alert under this paragraph to each of the other consumer reporting agencies described in section 603(p), in accordance with procedures developed under section 621(f).

A reseller of credit bureau information must also include fraud alert or active duty alerts (which apply to active military personnel) in the file. (A reseller is often a business that combines the information from the larger credit bureaus into one report, to make it easier for the user to read and find information.)

‘‘(f) DUTY OF RESELLER TO RECONVEY ALERT.—A reseller shall include in its report any fraud alert or active duty alert placed in the file of a consumer pursuant to this section by another consumer reporting agency.

If a consumer does not contact one of the big three credit bureaus or other entity described in Section 603(p) of the Act, the agency that the consumer does contact must refer the consumer to the agencies included under Section 603(p) and to the FTC:

‘‘(g) DUTY OF OTHER CONSUMER REPORTING AGENCIES TO PROVIDE CONTACT INFORMATION.—If a consumer contacts any consumer reporting agency that is not described in section 603(p) to communicate a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft, the agency shall provide information to the consumer on how to contact the Commission and the consumer reporting agencies described in section 603(p) to obtain more detailed information and request alerts under this section.

Initial fraud alerts under this Act require that the consumer not open any new accounts or ask for new extensions of credit, and the alert states this:

1*) REQUIREMENTS FOR INITIAL AND ACTIVE DUTY ALERTS.—*
‘‘(A) NOTIFICATION.—Each initial fraud alert and active duty alert under this section shall include information that notifies all prospective users of a consumer report on the consumer to which the alert relates that the consumer does not authorize the establishment of any new creditplan or extension of credit, other than under an openend credit plan (as defined in section 103(i)), in the name of the consumer, or issuance of an additional card on an existing credit account requested by a consumer, or any increase in credit limit on an existing credit account requested by a consumer, except in accordance with subparagraph (B).

Users of consumer reports that include an initial fraud alert may not establish a new credit plan or extension of credit while the initial fraud alert is in place, unless there is a method of verifying the identity of the consumer making the request for the new credit:

‘‘(B) LIMITATION ON USERS.—
‘‘(i) IN GENERAL.—No prospective user of a consumer report that includes an initial fraud alert or an active duty alert in accordance with this section may establish a new credit plan or extension of credit, other than under an open-end credit plan (as defined in section 103(i)), in the name of the consumer, or issue an additional card on an existing credit account requested by a consumer, or grant any increase in credit limit on an existing credit account requested by a consumer, unless the user utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request.

‘‘(ii) VERIFICATION.—If a consumer requesting the alert has specified a telephone number to be used for identity verification purposes, before authorizing any new credit plan or extension described in clause (i) in the name of such consumer, a user of such consumer report shall contact the consumer using that telephone number or take reasonable steps to verify the consumer’s identity and confirm that the application for a new credit plan is not the result of identity theft.

New credit plans or extensions of credit also may not be made while extended alerts are in effect unless the creditor has a method for verifying the identity of the consumer:

‘‘(2) REQUIREMENTS FOR EXTENDED ALERTS.—
‘‘*(A) NOTIFICATION.—Each extended alert under this section shall include information that provides all prospective users of a consumer report relating to a consumer with—*
‘‘(i) notification that the consumer does not authorize the establishment of any new credit plan or extension of credit described in clause (i), other than under an open-end credit plan (as defined in section 103(i)), in the name of the consumer, or issuance of an additional card on an existing credit account requested by a consumer, or any increase in credit limit on an existing credit account requested by a consumer, except in accordance with subparagraph
(B); and
‘‘(ii) a telephone number or other reasonable contact method designated by the consumer.

‘‘(B) LIMITATION ON USERS.—No prospective user of a consumer report or of a credit score generated using the information in the file of a consumer that includes an extended fraud alert in accordance with this section may establish a new credit plan or extension of credit, other than under an open-end credit plan (as defined in section 103(i)), in the name of the consumer, or issue an additional card on an existing credit account requested by a consumer, or any increase in credit limit on an existing credit account requested by a consumer, unless the user contacts the consumer in person or using the contact method described in subparagraph (A)(ii) to confirm that the application for a new credit plan or increase in credit limit, or request for an additional card is not the result of identity theft.’’.

Truncating (Shortening) Credit Card Numbers

Account numbers may be stolen from merchant wastebaskets or dumpsters, or even by unscrupulous employees of the merchant. For this reason, the Act requires that only the last five digits of a credit card may appear on receipts:

SEC. 113. TRUNCATION OF CREDIT CARD AND DEBIT CARD ACCOUNT NUMBERS.
‘‘(g) TRUNCATION OF CREDIT CARD AND DEBIT CARD NUMBERS.—

‘‘(1) IN GENERAL.—Except as otherwise provided in this subsection, no person that accepts credit cards or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction.

‘‘(2) LIMITATION.—This subsection shall apply only to receipts that are electronically printed, and shall not apply to transactions in which the sole means of recording a credit card or debit card account number is by handwriting or by an imprint or copy of the card.

‘‘(3) EFFECTIVE DATE.—This subsection shall become effective—
‘‘(A) 3 years after the date of enactment of this subsection, with respect to any cash register or other machine or device that electronically prints receipts for credit card or debit card transactions that is in use before January 1, 2005; and

''(B) 1 year after the date of enactment of this subsection, with respect to any cash register or other machine or device that electronically prints receipts for credit card or debit card transactions that is first put into use on or after January 1, 2005.''

Address Changes

Section 114 of the Act includes methods of curtailing identity theft by acting upon "red flags" that could point to potential identity theft, such as an address change followed by the issuing of a new card:

SEC. 114. ESTABLISHMENT OF PROCEDURES FOR THE IDENTIFICATION OF POSSIBLE INSTANCES OF IDENTITY THEFT.

''(e) RED FLAG GUIDELINES AND REGULATIONS REQUIRED.—

''(1) GUIDELINES.—The Federal banking agencies, the National Credit Union Administration, and the Commission shall jointly, with respect to the entities that are subject to their respective enforcement authority under section 621—
''(A) establish and maintain guidelines for use by each financial institution and each creditor regarding identity theft with respect to account holders at, or customers of, such entities, and update such guidelines as often as necessary;
''(B) prescribe regulations requiring each financial institution and each creditor to establish reasonable policies and procedures for implementing the guidelines established pursuant to subparagraph (A), to identify possible risks to account holders or customers or to the safety and soundness of the institution or customers; and
''(C) prescribe regulations applicable to card issuers to ensure that, if a card issuer receives notification of a change of address for an existing account, and within a short period of time (during at least the first 30 days after such notification is received) receives a request for an additional or replacement card for the same account, the card issuer may not issue the additional or replacement card, unless the card issuer, in accordance with reasonable policies and procedures—
''(i) notifies the cardholder of the request at the former address of the cardholder and provides to the cardholder a means of promptly reporting incorrect address changes;
''(ii) notifies the cardholder of the request by such other means of communication as the cardholder and the card issuer previously agreed to; or
''(iii) uses other means of assessing the validity of the change of address, in accordance with reasonable policies and procedures established by the card issuer in accordance with the regulations prescribed under subparagraph (B).

''(2) CRITERIA.—

''(A) IN GENERAL.—In developing the guidelines required by paragraph (1)(A), the agencies described in paragraph (1) shall identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft.

''(B) INACTIVE ACCOUNTS.—In developing the guidelines required by paragraph (1)(A), the agencies described in paragraph (1) shall consider including reasonable guidelines providing that when a transaction occurs with respect to a credit or deposit account that has been inactive for more than 2 years, the creditor or financial institution shall follow reasonable policies and procedures that provide for notice to be given to a consumer in a manner reasonably designed to reduce the likelihood of identity theft with respect to such account.

''(3) CONSISTENCY WITH VERIFICATION REQUIREMENTS.—

Guidelines established pursuant to paragraph (1) shall not be inconsistent with the policies and procedures required under section 5318(l) of title 31, United States Code.''.

Consumers can also request that Social Security numbers be truncated in the consumer reports issued by the consumer reporting agencies:

SEC. 115. AUTHORITY TO TRUNCATE SOCIAL SECURITY NUMBERS.
Section 609(a)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681g(a)(1)) is amended by striking ''except that nothing'' and inserting the following: ''except that—
''(A) if the consumer to whom the file relates requests that the first 5 digits of the social security number (or similar identification number) of the consumer not be included in the disclosure and the consumer reporting agency has received appropriate proof of the identity of the requester, the consumer reporting agency shall so truncate such number in such disclosure; and
''(B) nothing''.

Summary of Identity Theft Victim's Rights

The Fair Credit Reporting Act includes the requirement that consumer reporting agencies provide a notice of consumer rights when reports are generated for consumers. The FACT Act expands these rights. These rights are to be developed by the FTC in conjunction with the Federal banking agencies and the National Credit Union Administration:
Subtitle B—Protection and Restoration of Identity Theft Victim Credit History

SEC. 151. SUMMARY OF RIGHTS OF IDENTITY THEFT VICTIMS.
''(d) SUMMARY OF RIGHTS OF IDENTITY THEFT VICTIMS.—

''(1) IN GENERAL.—The Commission, in consultation with the Federal banking agencies and the National Credit Union Administration, shall prepare a model summary of the rights of consumers under this title with respect to the procedures for remedying the effects of fraud or identity theft involving credit, an electronic fund transfer, or an account or transaction at or with a financial institution or other creditor.

The Act includes the rights that must be included in the summary:

''(c) SUMMARY OF RIGHTS TO OBTAIN AND DISPUTE INFORMATION

IN CONSUMER REPORTS AND TO OBTAIN CREDIT SCORES.—
''(1) COMMISSION SUMMARY OF RIGHTS REQUIRED.—
''(A) IN GENERAL.—The Commission shall prepare a model summary of the rights of consumers under this title.
''(B) CONTENT OF SUMMARY.—The summary of rights prepared under subparagraph (A) shall include a description of—
''(i) the right of a consumer to obtain a copy of a consumer report under subsection (a) from each consumer reporting agency;
''(ii) the frequency and circumstances under which a consumer is entitled to receive a consumer report without charge under section 612;
''(iii) the right of a consumer to dispute information in the file of the consumer under section 611;
''(iv) the right of a consumer to obtain a credit score from a consumer reporting agency, and a description of how to obtain a credit score;
''(v) the method by which a consumer can contact, and obtain a consumer report from, a consumer reporting agency without charge, as provided in the regulations of the Commission prescribed under section 211(c) of the Fair and Accurate Credit Transactions Act of 2003; and

‘‘(vi) the method by which a consumer can contact, and obtain a consumer report from, a consumer reporting agency described in section 603(w), as provided in the regulations of the Commission prescribed under section 612(a)(1)(C).

C) AVAILABILITY OF SUMMARY OF RIGHTS.—The Commission shall—
‘‘(i) actively publicize the availability of the summary of rights prepared under this paragraph;
‘‘(ii) conspicuously post on its Internet website the availability of such summary of rights; and
‘‘(iii) promptly make such summary of rights available to consumers, on request.

‘‘(2) SUMMARY OF RIGHTS REQUIRED TO BE INCLUDED WITH AGENCY DISCLOSURES.—A consumer reporting agency shall provide to a consumer, with each written disclosure by the agency to the consumer under this section—
‘‘(A) the summary of rights prepared by the Commission under paragraph (1);
‘‘(B) in the case of a consumer reporting agency described in section 603(p), a toll-free telephone number established by the agency, at which personnel are accessible to consumers during normal business hours;
‘‘(C) a list of all Federal agencies responsible for enforcing any provision of this title, and the address and Public information. any appropriate phone number of each such agency, in a form that will assist the consumer in selecting the appropriate agency;
‘‘(D) a statement that the consumer may have additional rights under State law, and that the consumer may wish to contact a State or local consumer protection agency or a State attorney general (or the equivalent thereof) to learn of those rights; and
‘‘(E) a statement that a consumer reporting agency is not required to remove accurate derogatory information from the file of a consumer, unless the information is outdated under section 605 or cannot be verified.’’.

The summary of rights will be provided to consumers who contact a consumer reporting agency and express a belief that they are a victim of fraud or identity theft:

‘‘(2) SUMMARY OF RIGHTS AND CONTACT INFORMATION.—
Beginning 60 days after the date on which the model summary of rights is prescribed in final form by the Commission pursuant to paragraph (1), if any consumer contacts a consumer reporting agency and expresses a belief that the consumer is a victim of fraud or identity theft involving credit, an electronic fund transfer, or an account or transaction at or with a financial institution or other creditor, the consumer reporting agency shall, in addition to any other action that the agency may take, provide the consumer with a summary of rights that contains all of the information required by the Commission under paragraph (1), and information on how to contact the Commission to obtain more detailed information.

Release of Information to Victims

In order to straighten out an identity theft victim’s finances, the victim often needs documentation of the crime. The FACT Act requires that creditors release credit applications and business transactions related to the identity theft to the victim and authorized law enforcement agencies upon proper submission of a request by the victim and verification of identity by the creditor:

‘‘(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—
''(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.

Before releasing the information to the victim, the creditor must be provided with appropriate identification so that the creditor can verify the victim's identity:

''(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.

The request for the release of information must follow a particular form:

''(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.

The creditor may not charge the victim for this information:

''(4) NO CHARGE TO VICTIM.—Information required to be provided under paragraph (1) shall be so provided without charge.

The creditor may decline the request for information in certain circumstances:

''(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.

The Act prohibits holding a business entity civilly liable for disclosing information in good faith according to the provisions of this Section:

''(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.

The creditor does not have to establish new recordkeeping procedures to fulfill this obligation, but must provide the documentation that the creditor would normally compiled:

''(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…

This Section defines "victim," for purposes of the release of the application and other documents the victim may need to straighten out the mess caused by identity theft. Note that the definition includes a consumer whose identification and financial information has been alleged to have been used or transferred. The veracity of the claim does not have to be proven prior to the information being released to the victim:

''(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.

''(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.''.

Blocking Information
The FACT Act requires the
consumer reporting agency to block the reporting of information that the consumer identifies as resulting from identity theft within four business days of receiving the required information from the consumer:

SEC. 152. BLOCKING OF INFORMATION RESULTING FROM IDENTITY THEFT.

‘‘§ 605B. Block of information resulting from identity theft ‘‘(a) BLOCK.—Except as otherwise provided in this section, a consumer reporting agency shall block the reporting of any information in the file of a consumer that the consumer identifies as information that resulted from an alleged identity theft, not later than 4 business days after the date of receipt by such agency of—
‘‘(1) appropriate proof of the identity of the consumer;
‘‘(2) a copy of an identity theft report;
‘‘(3) the identification of such information by the consumer;
and
‘‘(4) a statement by the consumer that the information is not information relating to any transaction by the consumer.

‘‘(b) NOTIFICATION.—A consumer reporting agency shall promptly notify the furnisher of information identified by the consumer under subsection (a)—
‘‘(1) that the information may be a result of identity theft;
‘‘(2) that an identity theft report has been filed;
‘‘(3) that a block has been requested under this section;
and
‘‘(4) of the effective dates of the block.

Under certain circumstances, the consumer reporting agency may decline to block the information the consumer contends if due to identity theft:

‘‘(c) AUTHORITY TO DECLINE OR RESCIND.—

‘‘(1) IN GENERAL.—A consumer reporting agency may decline to block, or may rescind any block, of information relating to a consumer under this section, if the consumer reporting agency reasonably determines that—
‘‘(A) the information was blocked in error or a block was requested by the consumer in error;
‘‘(B) the information was blocked, or a block was requested by the consumer, on the basis of a material misrepresentation of fact by the consumer relevant to the request to block; or
‘‘(C) the consumer obtained possession of goods, services, or money as a result of the blocked transaction or transactions.

‘‘(2) NOTIFICATION TO CONSUMER.—If a block of information is declined or rescinded under this subsection, the affected consumer shall be notified promptly, in the same manner as consumers are notified of the reinsertion of information under section 611(a)(5)(B).

‘‘(3) SIGNIFICANCE OF BLOCK.—For purposes of this subsection, if a consumer reporting agency rescinds a block, the presence of information in the file of a consumer prior to the blocking of such information is not evidence of whether the consumer knew or should have known that the consumer obtained possession of any goods, services, or money as a result of the block.

Resellers are subject to some exceptions to the blocking requirements:

‘‘(d) EXCEPTION FOR RESELLERS.—

‘‘(1) NO RESELLER FILE.—This section shall not apply to a consumer reporting agency, if the consumer reporting agency—
‘‘(A) is a reseller;
‘‘(B) is not, at the time of the request of the consumer under subsection (a), otherwise furnishing or reselling a consumer report concerning the information identified by the consumer; and

‘‘(C) informs the consumer, by any means, that the consumer may report the identity theft to the Commission to obtain consumer information regarding identity theft.

‘‘(2) RESELLER WITH FILE.—The sole obligation of the consumer reporting agency under this section, with regard to any request of a consumer under this section, shall be to block the consumer report maintained by the consumer reporting agency from any subsequent use, if—
‘‘(A) the consumer, in accordance with the provisions of subsection (a), identifies, to a consumer reporting agency, information in the file of the consumer that resulted from identity theft; and
‘‘(B) the consumer reporting agency is a reseller of the identified information.

‘‘(3) NOTICE.—In carrying out its obligation under paragraph (2), the reseller shall promptly provide a notice to the consumer of the decision to block the file. Such notice shall contain the name, address, and telephone number of each consumer reporting agency from which the consumer information was obtained for resale.

Law enforcement agencies may still have access to blocked information:

‘‘(f) ACCESS TO BLOCKED INFORMATION BY LAW ENFORCEMENT AGENCIES.—No provision of this section shall be construed as requiring a consumer reporting agency to prevent a Federal, State, or local law enforcement agency from accessing blocked information in a consumer file to which the agency could otherwise obtain access under this title.’’.

Centralized Identity Theft Investigations

To make identity theft investigations easier to investigate and resolve, the Act establishes centralized coordination of identity theft complaints:

SEC. 153. COORDINATION OF IDENTITY THEFT COMPLAINT INVESTIGATIONS.

‘‘(1) IN GENERAL.—Each consumer reporting agency described in section 603(p) shall develop and maintain procedures for the referral to each other such agency of any consumer complaint received by the agency alleging identity theft, or requesting a fraud alert under section 605A or a block under section 605B.

A model identity theft reporting form (the ID Theft Affidavit reproduced in the first chapter) is required under the Act to be developed by the FTC, in coordination with the Federal banking agencies and the National Credit Union Administration:

‘‘(2) MODEL FORM AND PROCEDURE FOR REPORTING IDENTITY THEFT.—The Commission, in consultation with the Federal banking agencies and the National Credit Union Administration, shall develop a model form and model procedures to be used by consumers who are victims of identity theft for contacting and informing creditors and consumer reporting agencies of the fraud.

Preventing Deleted Information From Reappearing in Reports

One of the problems with identity theft is that the erroneous information may reappear in consumer reports after the consumer has successfully disputed it. The FACT Act includes provisions to help eliminate this problem, by requiring reporters of information to consumer reporting agencies to have procedures in place to prevent re-reporting of blocked information.
:
SEC. 154. PREVENTION OF REPOLLUTION OF CONSUMER REPORTS.

‘‘(6) DUTIES OF FURNISHERS UPON NOTICE OF IDENTITY THEFT-RELATED INFORMATION.—

‘‘(A) REASONABLE PROCEDURES.—A person that furnishes information to any consumer reporting agency shall have in place reasonable procedures to respond to any notification that it receives from a consumer reporting agency under section 605B relating to information resulting from identity theft, to prevent that person from refurnishing such blocked information.

‘‘(B) INFORMATION ALLEGED TO RESULT FROM IDENTITY THEFT.—If a consumer submits an identity theft report to a person who furnishes information to a consumer reporting agency at the address specified by that person for receiving such reports stating that information maintained by such person that purports to relate to the consumer resulted from identity theft, the person may not furnish such information that purports to relate to the consumer to any consumer reporting agency, unless the person subsequently knows or is informed by the consumer that the information is correct.’’.

The FACT Act also requires debt collectors to notify the creditors they work for if the debt collector is notified that information related to a debt they are collecting may be fraudulent or the result of identity theft.

SEC. 155. NOTICE BY DEBT COLLECTORS WITH RESPECT TO FRAUDULENT INFORMATION.
Section 615 of the Fair Credit Reporting Act (15 U.S.C. 1681m), as amended by this Act, is amended by adding at the end the following:

‘‘(g) DEBT COLLECTOR COMMUNICATIONS CONCERNING IDENTITY THEFT.—If a person acting as a debt collector (as that term is defined in title VIII) on behalf of a third party that is a creditor or other user of a consumer report is notified that any information relating to a debt that the person is attempting to collect may be fraudulent or may be the result of identity theft, that person shall—
‘‘(1) notify the third party that the information may be fraudulent or may be the result of identity theft; and
‘‘(2) upon request of the consumer to whom the debt purportedly relates, provide to the consumer all information to which the consumer would otherwise be entitled if the consumer were not a victim of identity theft, but wished to dispute the debt under provisions of law applicable to that person.’’

The Fair Credit Billing Act

The Fair Credit Billing Act includes procedures for resolving billing errors on credit card accounts. These same procedures apply to errors that occur due to identity theft.

If an “obligor”, or the person who is the authorized user on a credit card account, notifies the creditor of a billing error, the creditor must either correct the error or explain to the obligor why the charges are not in error, no later than two billing cycles or 90 days from being notified, whichever is shorter:

ß 161. Correction of billing errors

(a) If a creditor, within sixty days after having transmitted to an obligor a statement of the obligor’s account in connection with an extension of consumer credit, receives … a written notice (other than notice on a payment stub or other payment medium supplied by the creditor if

the creditor so stipulates with the disclosure required under section 127(a) (8)) from the obligor in which the obligor—

(1) sets forth or otherwise enables the creditor to identify the name and account number (if any) of the obligor,

(2) indicates the obligor's belief that the statement contains a billing error and the amount of such billing error, and

(3) sets forth the reasons for the obligor's belief (to the extent applicable) that the statement contains a billing error, the creditor shall, unless the obligor has, after giving such written notice and before the expiration of the time limits herein specified, agreed that the statement was correct--

(A) not later than thirty days after the receipt of the notice, send a written acknowledgment thereof to the obligor, unless the action required in subparagraph (B) is taken within such thirty-day period, and

(B) not later than two complete billing cycles of the creditor (in no event later than ninety days) after the receipt of the notice and prior to taking any action to collect the amount, or any part thereof, indicated by the obligor under paragraph (2) either--
(i) make appropriate corrections in the account of the obligor, including the crediting of any finance charges on amounts erroneously billed, and transmit to the obligor a notification of such corrections and the creditor's explanation of any cage in the amount indicated by the obligor under paragraph (2) and, if any such change is made and the obligor so requests, copies of documentary evidence of the obligor's indebtedness; or
(ii) send a written explanation or clarification to the obligor, after having conducted an investigation, setting forth to the extent applicable the reasons why the creditor believes the account of the obligor was correctly shown in the statement and, upon request of the obligor, provide copies of documentary evidence of the obligor's indebtedness. In the case of a billing error where the obligor alleges that the creditor's billing statement reflects goods not delivered to the obligor or his designee in accordance with the agreement made at the time of the transaction, a creditor may not construe such amount to be correctly shown unless he determines that such goods were actually delivered, mailed, or otherwise sent to the obligor and provides the obligor with a statement of such determination.
After complying with the provisions of this subsection with respect to an alleged billing error, a creditor has no further responsibility under this section if the obligor continues to make substantially the same allegation with respect to such error.

Billing errors as defined under the Act include those that could occur due to identity theft:
(b) For the purpose of this section, a "billing error" consists of any of the following:

(1) A reflection on a statement of an extension of credit which was not made to the obligor or, if made, was not in the amount reflected on such statement.

(2) A reflection on a statement of an extension of credit for which the obligor requests additional clarification including documentary evidence thereof.

(3) A reflection on a statement of goods or services not accepted by the obligor or his designee or not delivered to the obligor or his designee in accordance with the agreement made at the time of a transaction.

(4) The creditor's failure to reflect properly on a statement a payment made by the obligor or a credit issued to the obligor.

(5) A computation error or similar error of an accounting nature of the creditor on a statement.

(6) Any other error described in regulations of the Board.
(c) For the purposes of this section, “action to collect the amount, or any part thereof, indicated by an obligor under paragraph (2)” does not include the sending of statements of account to the obligor following written notice from the obligor as specified under subsection (a) if--

(1) the obligor's account is not restricted or closed because of the failure of the obligor to pay the amount indicated under paragraph (2) of subsection (a) and

(2) the creditor indicates the payment of such amount is not required pending the creditor's compliance with this section.

Nothing in this section shall be construed to prohibit any action by a creditor to collect any amount which has not been indicated by the obligor to contain a billing error…

The creditor cannot file adverse information concerning the disputed amount until the creditor has investigated the matter and provided notice to the customer as required under the Act.

ß 162. Regulation of credit reports

(a) After receiving a notice from an obligor as provided in section 161(a), a creditor or his agent may not directly or indirectly threaten to report to any person adversely on the obligor's credit rating or credit standing because of the obligor's failure to pay the amount indicated by the obligor under section 161(a) (2) and such amount may not be reported as delinquent to any third party until the creditor has met the requirements of section 161 and has allowed the obligor the same number of days (not less than ten) thereafter to make payment as is provided under the credit agreement with the obligor for the payment of undisputed amounts.
(b) If a creditor receives a further written notice from an obligor that an amount is still in dispute within the time allowed for payment under subsection (a) of this section, a creditor may not report to any third party that the amount of the obligor is delinquent because the obligor has failed to pay an amount which he has indicated under section 161(a) (2), unless the creditor also reports that the amount is in dispute and, at the same time, notifies the obligor of the name and address of each party to whom the creditor is reporting information concerning the delinquency.

If the creditor has reported delinquencies based on the disputed amounts, and the delinquencies are resolved, the creditor must also report that the delinquencies are resolved:
(c) A creditor shall report any subsequent resolution of any delinquencies reported pursuant to subsection (b) to the parties to whom such delinquencies were initially reported.

The Fair Debt Collection Practices Act

The purpose of the Fair Debt Collection Practices Act is to prohibit debt collectors from using unfair or deceptive practices to collect overdue bills.

Recall that it is recommended that the victim of identity theft not pay any unauthorized amounts, but rather that the victim should tell the debt collector that the victim did not authorize the

charges. The Fair Debt Collection Practices Act prohibits the debt collector from harassing the victim, or taking other unfair or deceptive steps in order to try to collect the debt.

Section 805 of the Act sets forth the rules the debt collector must follow when communicating in connection with debt collection. These requirements include, generally:

- A debt collector may not communicate with a consumer before 8 AM or after 9 PM.
- A debt collector is to communicate with the consumer's attorney if the debt collector knows that the consumer is represented by an attorney
- A debt collector should not contact a consumer at work if the debt collector knows that the consumer's employer does not allow such communication
- A debt collector may not, without prior consent from the consumer given directly to the debt collector, communicate with anyone other than the consumer, the consumer's attorney, the creditor, the creditor's attorney, the attorney of the debt collector or a consumer reporting agency, concerning the collection of the debt
- If a consumer notifies the debt collector in writing that the consumer refuses to pay a debt or that the consumer wishes the debt collector to cease further communication with the consumer, the debt collector must not communicate with the consumer about the debt, other than to notify the consumer that the debt collector may take specified actions as a result of the consumer's notice

Section 806 of the Act prohibits the debt collector from harassing or abusing the consumer:
Harassment or abuse [15 USC 1692d]
A debt collector may not engage in any conduct the natural consequence of which is to harass, oppress, or abuse any person in connection with the collection of a debt. Without limiting the general application of the foregoing, the following conduct is a violation of this section:

(1) The use or threat of use of violence or other criminal means to harm the physical person, reputation, or property of any person.

(2) The use of obscene or profane language or language the natural consequence of which is to abuse the hearer or reader.

(3) The publication of a list of consumers who allegedly refuse to pay debts, except to a consumer reporting agency or to persons meeting [certain requirements]

(4) The advertisement for sale of any debt to coerce payment of the debt.

(5) Causing a telephone to ring or engaging any person in telephone conversation repeatedly or continuously with intent to annoy, abuse, or harass any person at the called number.

(6) Except as provided in section 804, the placement of telephone calls without meaningful disclosure of the caller's identity.

Under this Act, there are also provisions for the debt to be validated or disputed. Section 809 provides that the debt collector must provide a statement that discloses the consumer's right to notify the debt collector within thirty days of receiving written notice from the debt collector that all or part of the debt is disputed. The debt collector must suspend collection activities until the debt collector receives verification of the debt or copy of a judgment, and mails it to the consumer.

The Electronic Fund Transfer Act

The Electronic Fund Transfer Act regulates debit cards and other electronic means to debit or credit an account. Before the provisions of this Act were passed, the rights of the electronic fund transfer user were undefined. Under the act, specific regulations are set forth concerning the use of electronic transfers. Consumers now have stated rights and protections through the enactment of the Act.

The Act includes the amount of unauthorized transfers a consumer may be held liable for, depending on when the consumer notifies the financial institution. Liability is lower if the consumer is able to notify the financial institution soon after the unauthorized transactions. This is one important reason why bank statements should be checked as soon as received :

§ 205.6 Liability of consumer for unauthorized transfers.

(a) Conditions for liability. A consumer may be held liable, within the limitations described in paragraph (b) of this section, for an unauthorized electronic fund transfer {{4-30-01 p.7365}} involving the consumer's account only if the financial institution has provided the disclosures required by § 205.7(b)(1), (2), and (3). If the unauthorized transfer involved an access device, it must be an accepted access device and the financial institution must have provided a means to identify the consumer to whom it was issued.

(b) Limitations on amount of liability. A consumer's liability for an unauthorized electronic fund transfer or a series of related unauthorized transfers shall be determined as follows:

(1) Timely notice given. If the consumer notifies the financial institution within two business days after learning of the loss or theft of the access device, the consumer's liability shall not exceed the lesser of $50 or the amount of unauthorized transfers that occur before notice to the financial institution.

(2) Timely notice not given. If the consumer fails to notify the financial institution within two business days after learning of the loss or theft of the access device, the consumer's liability shall not exceed the lesser of $500 or the sum of:

(i) $50 or the amount of unauthorized transfers that occur within the two business days, whichever is less; and

(ii) The amount of unauthorized transfers that occur after the close of two business days and before notice to the institution, provided the institution establishes that these transfers would not have occurred had the consumer notified the institution within that two-day period.

(3) Periodic statement; timely notice not given. A consumer must report an unauthorized electronic fund transfer that appears on a periodic statement within 60 days of the financial institution's transmittal of the statement to avoid liability for subsequent transfers. If the consumer fails to do so, the consumer's liability shall not exceed the amount of the unauthorized transfers that occur after the close of the 60 days and before notice to the institution, and that the institution establishes would not have occurred had the consumer notified the institution within the 60-day period. When an access device is involved in the unauthorized transfer, the consumer may be liable for other amounts set forth in paragraphs (b)(1) or (b)(2) of this section, as applicable.

(4) Extension of time limits. If the consumer's delay in notifying the financial institution was due to extenuating circumstances, the institution shall extend the times specified above to a reasonable period.

The Act also includes what methods may be used by the consumer to notify the financial institution of unauthorized transactions:

(5) Notice to financial institution.

(i) Notice to a financial institution is given when a consumer takes steps reasonably necessary to provide the institution with the pertinent information, whether or not a particular employee or agent of the institution actually receives the information.

(ii) The consumer may notify the institution in person, by telephone, or in writing.

(iii) Written notice is considered given at the time the consumer mails the notice or delivers it for transmission to the institution by any other usual means. Notice may be considered constructively given when the institution becomes aware of circumstances leading to the reasonable belief that an unauthorized transfer to or from the consumer's account has been or may be made.

(6) Liability under state law or agreement. If state law or an agreement between the consumer and the financial institution imposes less liability than is provided by this section, the consumer's liability shall not exceed the amount imposed under the state law or agreement.

Other important provisions in the Act include the procedures for resolving errors.

§ 205.11 Procedures for resolving errors.

(a) Definition of error--(1) Types of transfers or inquiries covered. The term error means:

(i) An unauthorized electronic fund transfer;

(ii) An incorrect electronic fund transfer to or from the consumer's account;

(iii) The omission of an electronic fund transfer from a periodic statement;

(iv) A computational or bookkeeping error made by the financial institution relating to an electronic fund transfer;

(v) The consumer's receipt of an incorrect amount of money from an electronic terminal;

(vi) An electronic fund transfer not identified in accordance with §§ 205.9 or 205.10(a); or

(vii) The consumer's request for documentation required by §§ 205.9 or 205.10(a) or for additional information or clarification concerning an electronic fund transfer, {{10-30-98 p.7370}} including a request the consumer makes to determine whether an error exists under paragraphs (a)(1)(i) through (vi) of this section.

(2) Types of inquiries not covered. The term error does not include:

(i) A routine inquiry about the consumer's account balance;

(ii) A request for information for tax or other record keeping purposes; or

(iii) A request for duplicate copies of documentation.

The financial institution may accept oral notification of an unauthorized transaction, but may also require written documentation after oral notification is received

(b) Notice of error from consumer—

(1) Timing; contents. A financial institution shall comply with the requirements of this section with respect to any oral or written notice of error from the consumer that:

(i) Is received by the institution no later than 60 days after the institution sends the periodic statement or provides the passbook documentation, required by § 205.9, on which the alleged error is first reflected;

(ii) Enables the institution to identify the consumer's name and account number; and

(iii) Indicates why the consumer believes an error exists and includes to the extent possible the type, date, and amount of the error, except for requests described in paragraph (a)(1)(vii) of this section.

(2) Written confirmation. A financial institution may require the consumer to give written confirmation of an error within 10 business days of an oral notice. An institution that requires written confirmation shall inform the consumer of the requirement and provide the address where confirmation must be sent when the consumer gives the oral notification.

(3) Request for documentation or clarifications. When a notice of error is based on documentation or clarification that the consumer requested under paragraph (a)(1)(vii) of this section, the consumer's notice of error is timely if received by the financial institution no later than 60 days after the institution sends the information requested.

The financial institution is generally given ten business days to complete an investigation of a disputed amount. If the financial institution is not able to complete the investigation within that

time frame, it can take up to 45 days from the date it received the consumer's notice. Under certain circumstances, these time frames may be extended:

(c) Time limits and extent of investigation--(1) Ten-day period. A financial institution shall investigate promptly and, except as otherwise provided in this paragraph (c), shall determine whether an error occurred within 10 business days of receiving a notice of error. This institution shall report the results to the consumer within three business days after completing its investigation. The institution shall correct the error within one business day after determining that an error occurred.

(2) Forty-five day period. If the financial institution is unable to complete its investigation within 10 business days, the institution may take up to 45 days from receipt of a notice of error to investigate and determine whether an error occurred, provided the institution does the following:

(i) Provisionally credits the consumer's account in the amount of the alleged error (including interest where applicable) within 10 business days of receiving the error notice. If the financial institution has a reasonable basis for believing that an unauthorized electronic fund transfer has occurred and the institution has satisfied the requirements of § 205.6(a), the institution may withhold a maximum of $50 from the amount credited. An institution need not provisionally credit the consumer's account if:

(A) The institution requires but does not receive written confirmation within 10 business days of an oral notice of error; or

(B) The alleged error involves an account that is subject to Regulation T (Securities Credit by Brokers and Dealers, 12 CFR part 220);

(ii) Informs the consumer, within two business days after the provisional crediting, of the amount and date of the provisional crediting and gives the consumer full use of the funds during the investigation;

(iii) Corrects the error, if any, within one business day after determining that an error occurred; and

(iv) Reports the results to the consumer within three business days after completing its investigation (including, if applicable, notice that a provisional credit has been made final).

(3) Extension of time periods. The time periods in paragraphs (c)(1) and (c)(2) of this section are extended as follows:

(i) The applicable time is 20 business days in place of 10 business days under paragraphs (c)(1) and (c)(2) of this section if the notice of error involves an electronic fund {{10-30-98 p.7371}} transfer to or from the account within 30 days after the first deposit to the account was made.

(ii) The applicable time is 90 days in place of 45 days under paragraph (c)(2) of this section, for completing an investigation, if a notice of error involves an electronic fund transfer that:

(A) Was not initiated within a state;

(B) Resulted from a point-of-sale debit card transaction; or

(C) Occurred within 30 days after the first deposit to the account was made.

(4) Investigation. With the exception of transfers covered by §205.14, a financial institution's review of its own records regarding an alleged error satisfies the requirements of this section if:

(i) The alleged error concerns a transfer to or from a third party; and

(ii) There is no agreement between the institution and the third party for the type of electronic fund transfer involved.

If the financial institution determines that there was no error, or that a different error occurred from the error the consumer reported, the financial institution must provide a written explanation. If the account is given provisional credit, pending the completed investigation, the financial institution must notify the consumer of the amount and how it will honor transactions against the account with the provisional credit:

(d) Procedures if financial institution determines no error or different error occurred. In addition to following the procedures specified in paragraph (c) of this section, the financial institution shall follow the procedures set forth in this paragraph (d) if it determines that no error occurred or that an error occurred in a manner or amount different from that described by the consumer:

(1) Written explanation. The institution's report of the results of its investigation shall include a written explanation of the institution's findings and shall note the consumer's right to request the documents that the institution relied on in making its determination. Upon request, the institution shall promptly provide copies of the documents.

(2) Debiting provisional credit. Upon debiting a provisionally credited amount, the financial institution shall:

(i) Notify the consumer of the date and amount of the debiting;

(ii) Notify the consumer that the institution will honor checks, drafts, or similar instruments payable to third parties and preauthorized transfers from the consumer's account (without charge to the consumer as a result of an overdraft) for five business days after the notification. The institution shall honor items as specified in the notice, but need honor only items that it would have paid if the provisionally credited funds had not been debited.

The Credit Repair Organizations Act

The Credit Repair Organizations Act regulates organizations that provide credit repair services.

The Credit Repair Organizations Act addresses credit repair organizations and their requirements to their customers.

SEC. 402. FINDINGS AND PURPOSES

(a) *Findings.--The Congress makes the following findings:*

(1) Consumers have a vital interest in establishing and maintaining their credit worthiness and credit standing in order to obtain and use credit. As a result, consumers who have experienced credit problems may seek assistance from credit repair organizations which offer to improve the credit standing of such consumers.

(*2) Certain advertising and business practices of some companies engaged in the business of credit repair services have worked a financial hardship upon consumers, particularly those of limited economic means and who are inexperienced in credit matters.*

(b) Purposes--The purposes of this title are--

(1) to ensure that prospective buyers of the services of credit repair organizations are provided with the information necessary to make an informed decision regarding the purchase of such services; and

(2) to protect the public from unfair or deceptive advertising and business practices by credit repair organizations.

Index