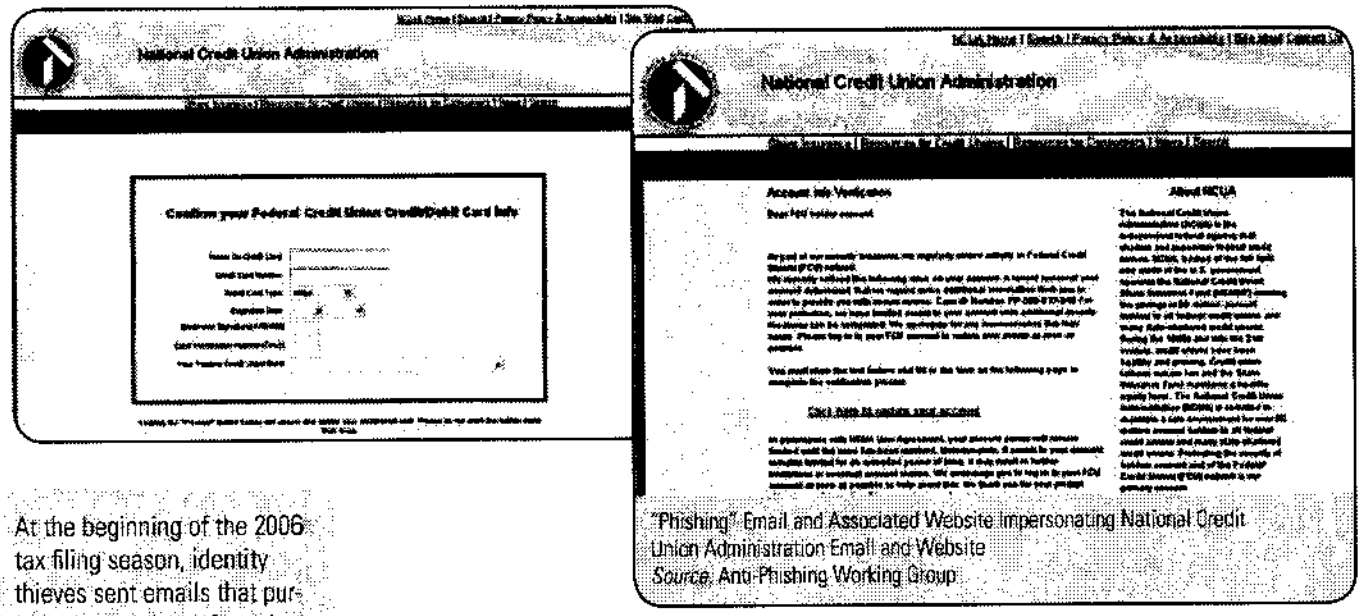


"Phishing" Email and Associated Website Impersonating National Credit Union Administration Email and Website
Source: Anti-Phishing Working Group

At the beginning of the 2006 tax filing season, identity thieves sent emails that purported to originate from the IRS's website to taxpayers, falsely informing them that there was a problem with their tax refunds. The emails requested that the taxpayers provide their SSNs so that the IRS could match their identities to the proper tax accounts. In fact, when the users entered their personal information – such as their SSNs, website usernames and passwords, bank or credit-card account numbers and expiration dates, among other things – the phishers simply harvested the data at another location on the Internet. Many of these schemes originated abroad, particularly in Eastern Europe. Since November 2005, the Treasury Inspector General for Tax Administration (TIGTA) and the IRS have received over 17,500 complaints about phishing scams, and TIGTA has identified and shut down over 230 phishing host sites targeting the IRS.

Phishing: "Phishing" is one of the most prevalent forms of social engineering. Phishers send emails that appear to be coming from legitimate, well-known sources—often, financial institutions or government agencies. In one example, these email messages tell the recipient that he must verify his personal information for an account or other service to remain active. The emails provide a link, which goes to a website that appears legitimate. After following the link, the web user is instructed to enter personal identifying information, such as his name, address, account number, PIN, and SSN. This information is then harvested by the phishers. In a variant of this practice, victims receive emails warning them that to avoid losing something of value (e.g., Internet service or access to a bank account) or to get something of value, they must click on a link in the body of the email to "reenter" or "validate" their personal data. Such phishing schemes often mimic financial institutions' websites and emails, and a number of them have even mimicked federal government agencies to add credibility to their demands for information. Additionally, phishing recently has taken on a new form, dubbed "vishing," in which the thieves use Voice Over Internet Protocol (VOIP) technology to spoof the telephone call systems of financial institutions and request callers provide their account information.[18]

Malware/Spyware/Keystroke Loggers: Criminals also can use spyware to illegally gain access to Internet users' computers and data without the users' permission. One email-based form of social engineering is the use of enticing emails offering free pornographic images to a group of victims; by opening the email, the victim launches the installation of malware, such as spyware or keystroke loggers, onto his computer. The keystroke loggers gather and send information on the user's Internet sessions back to the hacker, including user names and passwords for financial accounts and other personal information. These sophisticated methods of accessing personal information through

malware have supplemented other long-established methods by which criminals obtain victims' passwords and other useful data—such as "sniffing" Internet traffic, for example, by listening to network traffic on a shared physical network, or on unencrypted or weakly encrypted wireless networks.

Pretexting: Pretexting[19] is another form of social engineering used to obtain sensitive information. In many cases, pretexters contact a financial institution or telephone company, impersonating a legitimate customer, and request that customer's account information. In other cases, the pretext is accomplished by an insider at the financial institution, or by fraudulently opening an online account in the customer's name.[20]

Stolen Media

In addition to instances of deliberate theft of personal information, data also can be obtained by identity thieves in an "incidental" manner. Criminals frequently steal data storage devices, such as laptops or portable media, that contain personal information.[21] Although the criminal originally targeted the hardware, he may discover the stored personal information and realize its value and possibility for exploitation. Unless adequately safeguarded—such as through the use of technological tools for protecting data—this information can be accessed and used to steal the victim's identity. Identity thieves also may obtain consumer data when it is lost or misplaced.

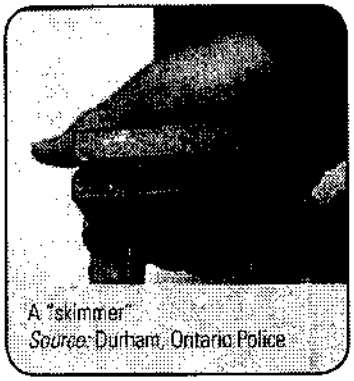
Failure to "Know Your Customer"

Data brokers compile consumer information from a variety of public and private sources and then offer it for sale to different entities for a range of purposes. For example, government agencies often purchase consumer information from data brokers to locate witnesses or beneficiaries, or for law enforcement purposes. Identity thieves, however, can steal personal information from data brokers who fail to ensure that their customers have a legitimate need for the data.

The Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLB Act) impose specific duties on certain types of data brokers that disseminate particular types of information.[22] For example, the FCRA requires data brokers that are consumer reporting agencies to make reasonable efforts to verify the identity of their customers and to ensure that those customers have a permissible purpose for obtaining the information. The GLB Act limits the ability of a financial institution to resell covered financial information.

Existing laws, however, do not reach every kind of personal information collected and sold by data brokers. In addition, when data brokers fail to comply with their statutory duties, they open the door to criminals who can access the personal information held by the data brokers by exploiting poor customer verification practices.

In January 2006, the FTC settled a lawsuit against data broker ChoicePoint, Inc., alleging that it violated the FCRA when it failed to perform due diligence in evaluating and approving new customers. The FTC alleged that ChoicePoint approved as customers for its consumer reports identity thieves who lied about their credentials and whose applications should have raised obvious red flags. Under the settlement, ChoicePoint paid $10 million in civil penalties and $5 million in consumer redress and agreed to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish a comprehensive information security program, and to obtain audits by an independent security professional every other year until 2026.



A "skimmer"
Source: Durham, Ontario Police

"Skimming"

Because it is possible to use someone's credit account without having physical access to the card, identity theft is easily accomplished when a criminal obtains a receipt with the credit account number, or uses other technology to collect that account information.[23] For example, over the past several years, law enforcement authorities have witnessed a substantial increase in the use of devices known as "skimmers." A skimmer is an inexpensive electronic device with a slot through which a person passes or "skims" a credit or debit card. Similar to the device legitimate businesses use in processing customer card payments, the skimmer reads and records the magnetically encoded data on the magnetic stripe on the back of the card. That data then can be downloaded either to make fraudulent copies of real cards, or to make purchases when the card is not required, such as online. A retail employee, such as a waiter, can easily conceal a skimmer until a customer hands him a credit card. Once he is out of the customer's sight, he can skim the card through the device, and then swipe it through the restaurant's own card reader to generate a receipt for the customer to sign. The waiter then can pass the recorded data to an accomplice, who can encode the data on blank cards with magnetic stripes. A variation of skimming involves an ATM-mounted device that is able to capture the magnetic information on the consumer's card, as well as the consumer's password.

In March 2006, a former candidate for the presidency of Peru pleaded guilty in a federal district court to charges relating to a large-scale credit card fraud and money laundering conspiracy. The defendant collected stolen credit card numbers from people in Florida who had used skimmers to obtain the information from customers of retail businesses where they worked, such as restaurants and rental car companies. He used some of the credit card fraud proceeds to finance various trips to Peru during his candidacy.

D. WHAT IDENTITY THIEVES DO WITH THE INFORMATION THEY STEAL: THE DIFFERENT FORMS OF IDENTITY THEFT

Once they obtain victims' personal information, criminals misuse it in endless ways, from opening new accounts in the victim's name, to accessing the victim's existing accounts, to using the victim's name when arrested. Recent survey data show that misuse of existing credit accounts, however, represents the single largest category of fraud.

Misuse of Existing Accounts

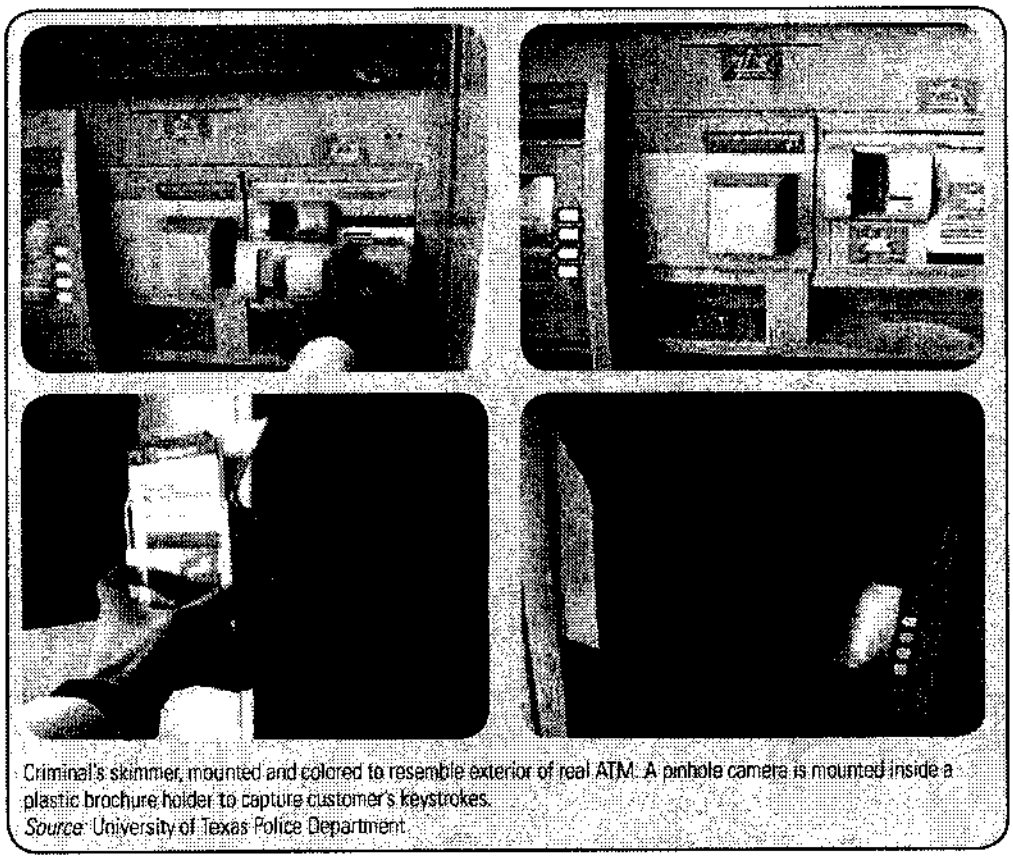
Misuse of existing accounts can involve credit, brokerage, banking, or utility accounts, among others. The most common form, however, involves credit accounts. This occurs when an identity thief obtains either the actual credit card, the numbers associated with the account, or the information derived from the magnetic strip on the back of the card. Because it is possible to make charges through remote purchases, such as online sales or by telephone, identity thieves are often able to commit fraud even as the card remains in the consumer's wallet.

Recent complaint data suggest an increasing number of incidents involving unauthorized access to funds in victims' bank accounts, including checking accounts—sometimes referred to as "account takeovers."[24] The Postal Inspection Service reports that it has seen an increase in account takeovers originating outside the United States. Criminals also have attempted to access funds in victims' online brokerage accounts.[25]

Federal law limits the liability consumers face from existing account misuse, generally shielding victims from direct losses due to fraudulent charges to their accounts. Nevertheless, consumers can spend many hours disputing the charges and making other corrections to their financial records.[26]

New Account Fraud

A more serious, if less prevalent, form of identity theft occurs when thieves are able to open new credit, utility, or other accounts in the victim's name, make charges indiscriminately, and then disappear. Victims often do not learn of the fraud until they are contacted by a debt collector or are turned down for a loan, a job, or other benefit because of a negative credit rating. While this is a less prevalent form of fraud, it causes more financial harm, is less likely to be discovered quickly by its victims, and requires the most time for recovery.



Criminal's skimmer, mounted and colored to resemble exterior of real ATM. A pinhole camera is mounted inside a plastic brochure holder to capture customer's keystrokes.
Source: University of Texas Police Department

In December 2005, a highly organized ring involved in identity theft, counterfeit credit and debit card fraud, and fencing of stolen products was shut down when Postal Inspectors and detectives from the Hudson County, New Jersey, Prosecutor's Office arrested 13 of its members. The investigation, which began in June 2005, uncovered more than 2,000 stolen identities and at least $1.3 million worth of fraudulent transactions. The investigation revealed an additional $1 million in fraudulent credit card purchases in more than 30 states and fraudulent ATM withdrawals. The account information came from computer hackers outside the United States who were able to penetrate corporate databases. Additionally, the ring used counterfeit bank debit cards encoded with legitimate account numbers belonging to unsuspecting victims to make fraudulent withdrawals of hundreds of thousands of dollars from ATMs in New Jersey, New York, and other states.

When criminals establish new credit card accounts in others' names, the sole purpose is to make the maximum use of the available credit from those accounts, whether in a short time or over a longer period. By contrast, when criminals establish new bank or loan accounts in others' names, the fraud often is designed to obtain a single disbursement of funds from a financial institution. In some cases, the criminal deposits a check drawn on an account with insufficient funds, or stolen or counterfeit checks, and then withdraws cash.

Federal identity theft charges were brought against 148 illegal aliens accused of stealing the identities of lawful U.S. citizens in order to gain employment. The aliens being criminally prosecuted were identified as a result of Operation Wagon Train, an investigation led by agents from U.S. Immigration and Customs Enforcement (ICE), working in conjunction with six U.S. Attorney's Offices. Agents executed civil search warrants at six meat processing plants. Numerous alien workers were arrested, and many were charged with aggravated identity theft, state identity theft, or forgery. Many of the names and Social Security numbers being used at the meat processing plants were reported stolen by identity theft victims to the FTC. In many cases, victims indicated that they received letters from the Internal Revenue Service demanding back taxes for income they had not reported because it was earned by someone working under their name. Other victims were denied driver's licenses, credit, or even medical services because someone had improperly used their personal information before.

"Brokering" of Stolen Data

Law enforcement has also witnessed an increase in the marketing of personal identification data from compromised accounts by criminal data brokers. For example, certain websites, known as "carding sites," traffic in large quantities of stolen credit-card data. Numerous individuals, often located in different countries, participate in these carding sites to acquire and review newly acquired card numbers and supervise the receipt and distribution of those numbers. The Secret Service calculated that the two largest current carding sites collectively have nearly 20,000 member accounts.

Immigration Fraud

In various parts of the country, illegal immigrants use fraudulently obtained SSNs or passports to obtain employment and assimilate into society. In extreme cases, an individual SSN may be passed on to and used by many illegal immigrants.[27] Although victims of this type of identity theft may not necessarily suffer financial harm, they still must spend hour upon hour attempting to correct their personal records to ensure that they are not mistaken for an illegal immigrant or cheated out of a government benefit.

Medical Identity Theft

Recent reports have brought attention to the problem of medical identity theft, a crime in which the victim's identifying information is used to obtain or make false claims for medical care.[28] In addition to the financial harm associated with other types of identity theft, victims of medical identity theft may have their health endangered by inaccurate entries in their medical records. This inaccurate information can potentially cause victims to receive improper medical care, have their insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs. Victims may not even be aware that a theft has occurred because medical identity theft can be difficult to discover, as few consumers regularly review their medical records, and victims may not realize that they have been victimized until they receive collection notices, or they attempt to seek medical care themselves, only to discover that they have reached their coverage limits.

Other Frauds

Identity theft is inherent in numerous other frauds perpetrated by criminals, including mortgage fraud and fraud schemes directed at obtaining government benefits, including disaster relief funds. The IRS's Criminal Investigation Division, for example, has seen an increase in the use of stolen SSNs to file tax returns. In some cases, the thief files a fraudulent return seeking a refund before the taxpayer files. When the real taxpayer files, the IRS may not accept his return because it is considered a duplicate return. Even if the taxpayer ultimately is made whole, the government suffers the loss from paying multiple refunds.

With the advent of the prescription drug benefit of Medicare Part D, the Department of Health and Human Services' Office of the Inspector General (HHS OIG) has noted a growing incidence of health care frauds involving identity theft. These frauds include telemarketers who fraudulently solicit potential Medicare Part D beneficiaries to disclose information such as their Health Insurance Claim Number (which includes the SSN) and bank account information, as well as marketers who obtain identities from nursing homes and other adult care facilities (including deceased beneficiaries and severely cognitively impaired persons) and use them fraudulently to enroll unwilling beneficiaries in alternate Part D plans in order to increase their sales commissions. The types of fraud that can be perpetrated by an identity thief are limited only by the ingenuity and resources of the criminal.

In July 2006, DOJ charged a defendant with 66 counts of false claims to the government, mail fraud, wire fraud, and aggravated identity theft, relating to the defendant's allegedly fraudulent applications for disaster assistance from the Federal Emergency Management Agency (FEMA) following Hurricane Katrina. Using fictitious SSNs and variations of her name, the defendant allegedly received $277,377 from FEMA.

Robert C. Ingardia, a registered representative who had been associated with several broker-dealers, assumed the identity of his customers. Without authorization, Mr. Ingardia changed the address information for their accounts, sold stock in the accounts worth more than $800,000, and, in an effort to manipulate the market for two thinly-traded penny stock companies, used the cash proceeds of the sales to buy more than $230,000 worth of stock in the companies. The SEC obtained a temporary restraining order against Mr. Ingardia in 2001, and a civil injunction against him in 2003 after the United States Attorney's Office for the Southern District of New York obtained a criminal conviction against him in 2002.

III. A Strategy to Combat Identity Theft

Identity theft is a multi-faceted problem for which there is no simple solution. Because identity theft has several stages in its "life cycle," it must be attacked at each of those stages, including:

- when the identity thief attempts to acquire a victim's personal information;
- when the thief attempts to misuse the information he has acquired; and
- after an identity thief has completed his crime and is enjoying the benefits, while the victim is realizing the harm.

The federal government's strategy to combat identity theft must address each of these stages by:

- keeping sensitive consumer data out of the hands of identity thieves in the first place through better data security and by educating consumers on how to protect it;
- making it more difficult for identity thieves, when they are able to obtain consumer data, to use the information to steal identities;
- assisting victims in recovering from the crime; and
- deterring identity theft by aggressively prosecuting and punishing those who commit the crime.

A great deal already is being done to combat identity theft, but there are several areas in which we can improve. The Task Force's recommendations, as described below, are focused on those areas.

A. PREVENTION: KEEPING CONSUMER DATA OUT OF THE HANDS OF CRIMINALS

Identity thieves can ply their trade only if they get access to consumer data. Reducing the opportunities for identity thieves to obtain the data in the first place is the first step to reducing identity theft. Government, the business community, and consumers all play a role in protecting data.

Data compromises can expose consumers to the threat of identity theft or related fraud, damage the reputation of the entity that experienced the breach, and impose the risk of substantial costs for all parties involved. Although there is no such thing as "perfect security," some entities fail to adopt even basic security measures, including many that are inexpensive and readily available.

The link between a data breach and identity theft often is unclear.

Depending on the nature of the breach, the kinds of information breached, and other factors, a particular breach may or may not pose a significant risk of identity theft. Little empirical evidence exists on the extent to which, and under what circumstances, data breaches lead to identity theft, and some studies indicate that data breaches and identity theft may not be strongly linked.[29] Nonetheless, because data thieves search for rich targets of consumer data, it is critical that organizations that collect and maintain sensitive consumer information take reasonable steps to protect it and explore new technologies to prevent data compromises.

1. DECREASING THE UNNECESSARY USE OF SOCIAL SECURITY NUMBERS

The SSN is especially valuable to identity thieves, because often it is the key piece of information used in authenticating the identities of consumers. An identity thief with a victim's SSN and certain other information generally can open accounts or obtain other benefits in the victim's name. As long as SSNs continue to be used for authentication purposes, it is important to prevent thieves from obtaining them.

SSNs are readily available to criminals because they are widely used as consumer identifiers throughout the private and public sectors. Although originally created in 1936 to track workers' earnings for social benefits purposes, use of SSNs has proliferated over ensuing decades. In 1961, the Federal Civil Service Commission established a numerical identification system for all federal employees using the SSN as the identification number. The next year, the IRS decided to begin using the SSN as its taxpayer identification number (TIN) for individuals. Indeed, the use by federal agencies of SSNs for the purposes of employment and taxation, employment verification, and sharing of data for law enforcement purposes, is expressly authorized by statute.

The simplicity and efficiency of using a seemingly unique number that most people already possessed encouraged widespread use of the SSN as an identifier by both government agencies and private enterprises, especially as they adapted their record-keeping and business systems to automated data processing. The use of SSNs is now common in our society.

Employers must collect SSNs for tax reporting purposes. Doctors or hospitals may need them to facilitate Medicare reimbursement. SSNs also are used in internal systems to sort and track information about individuals, and in some cases are displayed on identification cards. In 2004, an estimated 42 million Medicare cards displayed the entire SSN, as did approximately 8 million Department of Defense insurance cards. In addition, although the Veterans Health Administration (VHA) discontinued the issuance of Veterans Identification Cards that display SSNs in March 2004, and has issued new cards that do not display SSNs,

In June 2006, a federal judge in Massachusetts sentenced a defendant to five years in prison after a jury convicted him of passport fraud, SSN fraud, aggravated identity theft, identification document fraud, and furnishing false information to the SSA. The defendant had assumed the identity of a deceased individual and then used fraudulent documents to have the name of the deceased legally changed to a third name. He then used this new name and SSN to obtain a new SSN card, driver's licenses, and United States passport. The case was initiated based on information from the Joint Terrorism Task Force in Springfield, Massachusetts. The agencies involved in the investigation included SSA OIG, Department of State, Massachusetts State Police, and the Springfield and Boston police departments.

In September 2006, a defendant was sentenced by a federal judge in Pennsylvania to six months in prison after pleading guilty to Social Security card misuse and possession of a false immigration document. The defendant provided a fraudulent Permanent Resident Alien card and a fraudulent Social Security card to a state trooper as evidence of authorized stay and employment in the United States. The case was investigated by the SSA's Office of Inspector General (OIG), ICE, and the Pennsylvania State Police.

the VHA estimates that between 3 million and 4 million previously issued cards containing SSNs remain in circulation with veterans receiving VA health care services. Some universities still use the SSN as the students' identification number for a range of purposes, from administering loans to tracking grades, and may place it on students' identification cards, although usage for these purposes is declining.

SSNs also are widely available in public records held by federal agencies, states, local jurisdictions, and courts. As of 2004, 41 states and the District of Columbia, as well as 75 percent of U.S. counties, displayed SSNs in public records.[30] Although the number and type of records in which SSNs are displayed vary greatly across states and counties, SSNs are most often found in court and property records.

No single federal law regulates comprehensively the private sector or government use, display, or disclosure of SSNs; instead, there are a variety of laws governing SSN use in certain sectors or in specific situations. With respect to the private sector, for example, the GLB Act restricts the redisclosure to third parties of non-public personal information, such as SSNs, that was originally obtained from customers of a financial institution; the Health Insurance Portability and Accountability Act (HIPAA) limits covered health care organizations' disclosure of SSNs without patient authorization; and the Driver's Privacy Protection Act prohibits state motor vehicle departments from disclosing SSNs, subject to 14 "permissible uses."[31] In the public sector, the Privacy Act of 1974 requires federal agencies to provide notice to, and obtain consent from, individuals before disclosing their SSNs to third parties, except for an established routine use or pursuant to another Privacy Act exception.[32] A number of state statutes restrict the use and display of SSNs in certain contexts.[33] Even so, a report by the Government Accountability Office (GAO) concluded that, despite these laws, there were gaps in how the use and transfer of SSNs are regulated, and that these gaps create a risk that SSNs will be misused.[34]

There are many necessary or beneficial uses of the SSN. SSNs often are used to match consumers with their records and databases, including their credit files, to provide benefits and detect fraud. Federal, state, and local governments rely extensively on SSNs when administering programs that deliver services and benefits to the public.

Although SSNs sometimes are necessary for legal compliance or to enable disparate organizations to communicate about individuals, other uses are more a matter of convenience or habit. In many cases, for example, it may be unnecessary to use an SSN as an organization's internal identifier or to display it on an identification card. In these cases, a different unique identifier generated by the organization could be equally suitable, but without the risk inherent in the SSN's use as an authenticator.

Some private sector entities and federal agencies have taken steps to reduce unnecessary use of the SSN. For example, with guidance from the SSA OIG, the International Association of Chiefs of Police (IACP) adopted a resolution in September 2005 to end the practice of displaying SSNs in posters and other written materials relating to missing persons. Some health insurance providers also have stopped using SSNs as the subscriber's identification number.[35] Additionally, the Department of Treasury's Financial Management Service no longer includes personal identification numbers on the checks that it issues for benefit payments, federal income tax refund payments, and payments to businesses for goods and services provided to the federal government.

More must be done to eliminate unnecessary uses of SSNs. In particular, it would be optimal to have a unified and effective approach or standard for use or display of SSNs by federal agencies. The Office of Personnel Management (OPM), which issues and uses many of the federal forms and procedures using the SSN, and the Office of Management and Budget (OMB), which oversees the management and administrative practices of federal agencies, can play pivotal roles in restricting the unnecessary use of SSNs, offering guidance on better substitutes that are less valuable to identity thieves, and establishing greater consistency when the use of SSNs is necessary or unavoidable.

When purchasing advertising space in a trade magazine in 2002, a Colorado man wrote his birth date and Social Security number on the payment check. The salesman who received the check then used this information to obtain surgery in the victim's name. Two years later, the victim received a collection notice demanding payment of over $40,000 for the surgery performed on the identity thief. In addition to the damage this caused to his credit rating, the thief's medical information was added to the victim's medical records.

RECOMMENDATION: DECREASE THE UNNECESSARY USE OF SOCIAL SECURITY NUMBERS IN THE PUBLIC SECTOR

To limit the unnecessary use of SSNs in the public sector—and to begin to develop alternative strategies for identity management—the Task Force recommends the following:

- **Complete Review of Use of SSNs.** As recommended in the Task Force's interim recommendations, OPM undertook a review of the use of SSNs in its collection of human resource data from agencies and on OPM-based papers and electronic forms. Based on that review, which OPM completed in 2006, OPM should take steps to eliminate, restrict, or conceal the use of SSNs (including assigning employee identification numbers where practicable), in calendar year 2007. If necessary to implement this recommendation, Executive Order 9397, effective November 23, 1943, which requires federal agencies to use SSNs in "any system of permanent account numbers pertaining to individuals," should be partially rescinded. The use by federal agencies of SSNs for the purposes of employment and taxation, employment verification, and sharing of data for law enforcement purposes, however, is expressly authorized by statute and should continue to be permitted.

- **Issue Guidance on Appropriate Use of SSNs.** Based on its inventory, OPM should issue policy guidance to the federal human capital management community on the appropriate and inappropriate use of SSNs in employee records, including the appropriate way to restrict, conceal, or mask SSNs in employee records and human resource management information systems. OPM should issue this policy in calendar year 2007.

- **Require Agencies to Review Use of SSNs.** OMB has surveyed all federal agencies regarding their use of SSNs to determine the circumstances under which such use can be eliminated, restricted, or concealed in agency business processes, systems, and paper and electronic forms, other than those authorized or approved by OPM. OMB should complete the analysis of these surveys in the second quarter of 2007.[36]

- **Establish a Clearinghouse for Agency Practices that Minimize Use of SSNs.** Based on results from OMB's review of agency practices on the use of SSNs, the SSA should develop a clearinghouse for agency practices and initiatives that minimize use and display of SSNs to facilitate sharing of best practices—including the development of any alternative strategies for identity management—to avoid duplication of effort, and to promote interagency collaboration in the development of more effective measures. This should be accomplished by the fourth quarter of 2007.

- **Work with State and Local Governments to Review Use of SSNs.** In the second quarter of 2007, the Task Force should begin to work with state and local governments—through organizations such as the National Governor's Association, the National Association of Attorneys General, the National League of Cities, the National Association of Counties, the U.S. Conference of Mayors, the National District Attorneys Association, and the National Association for Public Health Statistics and Information Systems—to highlight and discuss the vulnerabilities created by the use of SSNs and to explore ways to eliminate unnecessary use and display of SSNs.

RECOMMENDATION: DEVELOP COMPREHENSIVE RECORD ON PRIVATE SECTOR USE OF SSNs

SSNs are an integral part of our financial system. They are essential in matching consumers to their credit file, and thus essential in granting credit and detecting fraud, but their availability to identity thieves creates a possibility of harm

to consumers. Beginning in 2007, the Task Force should develop a comprehensive record on the uses of the SSN in the private sector and evaluate their necessity. Specifically, the Task Force member agencies that have direct experience with the private sector use of SSNs, such as DOJ, FTC, SSA, and the financial regulatory agencies, should gather information from stakeholders—including the financial services industry, law enforcement agencies, the consumer reporting agencies, academics, and consumer advocates. The Task Force should then make recommendations to the President as to whether additional specific steps should be taken with respect to the use of SSNs. Any such recommendations should be made to the President by the first quarter of 2008.

2. *DATA SECURITY IN THE PUBLIC SECTOR*

While private organizations maintain consumer information for commercial purposes, public entities, including federal agencies, collect personal information about individuals for a variety of purposes, such as determining program eligibility and delivering efficient and effective services. Because this information often can be used to commit identity theft, agencies must guard against unauthorized disclosure or misuse of personal information.

a. Safeguarding of Information in the Public Sector

Two sets of laws and associated policies frame the federal government's responsibilities in the area of data security. The first specifically governs the federal government's information privacy program, and includes such laws as the Privacy Act, the Computer Matching and Privacy Protection Act, and provisions of the E-Government Act.[37] The other concerns the information and information technology security program. The Federal Information Security Management Act (FISMA), the primary governing statute for this program, establishes a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, and provides for development and maintenance of minimum controls required to protect federal information and information systems. FISMA assigns specific policy and oversight responsibilities to OMB, technical guidance responsibilities to the National Institute of Standards and Technology (NIST), implementation responsibilities to all agencies, and an operational assistance role to the Department of Homeland Security (DHS). FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. It further requires agency operational program officials, Chief Information Officers (CIOs), and Inspectors General (IGs) to conduct annual

reviews of the agency information security program and report the results to OMB. Additionally, as part of its oversight role, OMB issued several guidance memoranda last year on how agencies should safeguard sensitive information, including a memorandum addressing FISMA oversight and reporting, and which provided a checklist developed by NIST concerning protection of remotely accessed information, and that recommended that agencies, among other things, encrypt all data on mobile devices and use a "time-out" function for remote access and mobile devices.[38] The United States Computer Emergency Readiness Team (US-CERT) has also played an important role in public sector data security.[39]

Federal law also requires that agencies prepare extensive data collection analyses and report periodically to OMB and Congress. The President's Management Agenda (PMA) requires agencies to report quarterly to OMB on selected performance criteria for both privacy and security. Agency performance levels for both status and progress are graded on a PMA Scorecard.[40]

Federal agency performance on information security has been uneven. As a result, OMB and the agencies have undertaken a number of initiatives to improve the government security programs. OMB and DHS are leading an interagency Information Systems Security Line of Business (ISS LOB) working group, exploring ways to improve government data security practices. This effort already has identified a number of key areas for improving government-wide security programs and making them more cost-effective.

Employee training is essential to the effectiveness of agency security programs. Existing training programs must be reviewed continuously and updated to reflect the most recent changes, issues, and trends. This effort includes the development of annual general security awareness training for all government employees using a common curriculum; recommended security training curricula for all employees with significant security responsibilities; an information-sharing repository/portal of training programs; and opportunities for knowledge-sharing (e.g., conferences and seminars). Each of these components builds elements of agency security awareness and practices, leading to enhanced protection of sensitive data.

b. Responding to Data Breaches in the Public Sector

Several federal government agencies suffered high-profile security breaches involving sensitive personal information in 2006. As is true with private sector breaches, the loss or compromise of sensitive personal information by the government has made affected individuals feel exposed and vulnerable and may increase the risk of identity theft. Until this Task Force issued guidance on this topic in September 2006, government agencies had no comprehensive formal guidance on how to respond to

data breaches, and in particular, had no guidance on what factors to consider in deciding (1) whether a particular breach warrants notice to consumers, (2) the content of the notice, (3) which third parties, if any, should be notified, and (4) whether to offer affected individuals credit monitoring or other services.

The experience of the last year also has made one thing apparent: an agency that suffers a breach sometimes faces impediments in its ability to effectively respond to the breach by notifying persons and entities in a position to cooperate (either by assisting in informing affected individuals or by actively preventing or minimizing harms from the breach). For example, an agency that has lost data such as bank account numbers might want to share that information with the appropriate financial institutions, which could assist in monitoring for bank fraud and in identifying the account holders for possible notification. The very information that may be most necessary to disclose to such persons and entities, however, often will be information maintained by federal agencies that is subject to the Privacy Act. Critically, the Privacy Act prohibits the disclosure of any record in a system of records unless the subject individual has given written consent or unless the disclosure falls within one of 12 statutory exceptions.

RECOMMENDATION: EDUCATE FEDERAL AGENCIES ON HOW TO PROTECT THEIR DATA AND MONITOR COMPLIANCE WITH EXISTING GUIDANCE

To ensure that government agencies receive specific guidance on concrete steps that they can take to improve their data security measures, the Task Force recommends the following:

- **Develop Concrete Guidance and Best Practices.** OMB and DHS, through the current interagency Information Systems Security Line of Business (ISS LOB) task force, should (a) outline best practices in the area of automated tools, training, processes, and standards that would enable agencies to improve their security and privacy programs, and (b) develop a list of the most common 10 or 20 "mistakes" to avoid in protecting information held by the government. The Task Force made this recommendation as part of its interim recommendations to the President, and it should be implemented and completed in the second quarter of 2007.
- **Comply With Data Security Guidance.** OMB already has issued an array of data security regulations and standards aimed at urging agencies to better protect their data. Given that data breaches continue to occur, however, it is imperative that agencies continue to report compliance with its data security guidelines and

directives to OMB. If any agency does not comply fully, OMB should note that fact in the agency's quarterly PMA Scorecard.

- **Protect Portable Storage and Communications Devices.** Many of the most publicized data breaches in recent months involved losses of laptop computers. Because government employees increasingly rely on laptops and other portable communications devices to conduct government business, no later than the second quarter of 2007, all Chief Information Officers of federal agencies should remind the agencies of their responsibilities to protect laptops and other portable data storage and communication devices. If any agency does not fully comply, that failure should be reflected on the agency's PMA scorecard.

RECOMMENDATION: ENSURE EFFECTIVE, RISK-BASED RESPONSES TO DATA BREACHES SUFFERED BY FEDERAL AGENCIES

To assist agencies in responding to the difficult questions that arise following a data breach, the Task Force recommends the following:

- **Issue Data Breach Guidance to Agencies.** The Task Force developed and formally approved a set of guidelines, reproduced in Appendix A, that sets forth the factors that should be considered in deciding whether, how, and when to inform affected individuals of the loss of personal data that can contribute to identity theft, and whether to offer services such as free credit monitoring to the persons affected. In the interim recommendations, the Task Force recommended that OMB issue that guidance to all agencies and departments. OMB issued the guidance on September 20, 2006.

- **Publish a "Routine Use" Allowing Disclosure of Information Following a Breach.** To allow agencies to respond quickly to data breaches, including by sharing information about potentially affected individuals with other agencies and entities that can assist in the response, federal agencies should, in accordance with the Privacy Act exceptions, publish a routine use that specifically permits the disclosure of information in connection with response and remediation efforts in the event of a data breach. Such a routine use would serve to protect the interests of the people whose information is at risk by allowing agencies to take appropriate steps to facilitate a timely and effective response, thereby improving their ability to prevent, minimize, or remedy any harms that may result from a compromise of data maintained in their systems of records. This routine use should

not affect the existing ability of agencies to properly disclose and share information for law enforcement purposes. The Task Force offers the routine use that is reproduced in Appendix B as a model for other federal agencies to use in developing and publishing their own routine uses.[41] DOJ has now published such a routine use, which became effective as of January 24, 2007. The proposed routine use language reproduced in Appendix B should be reviewed and adapted by agencies to fit their individual systems of records.

3. DATA SECURITY IN THE PRIVATE SECTOR

Data protection in the private sector is the subject of numerous legal requirements, industry standards and guidelines, private contractual arrangements, and consumer and business education initiatives. But no system is perfect, and data breaches can occur even when entities have implemented appropriate data safeguards.

a. The Current Legal Landscape

Although there is no generally applicable federal law or regulation that protects all consumer information or requires that such information be secured, a variety of specific statutes and regulations impose data security requirements for particular entities in certain contexts. These include Title V of the GLB Act, and its implementing rules and guidance, which require financial institutions to maintain reasonable protections for the personal information they collect from customers [42]; Section 5 of the FTC Act, which prohibits unfair or deceptive practices [43]; the FCRA,[44] which restricts access to consumer reports and imposes safe disposal requirements, among other things [45]; HIPAA, which protects health information [46]; Section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act,[47] which requires verification of the identity of persons opening accounts with financial institutions; and the Drivers Privacy Protection Act of 1994 (DPPA), which prohibits most disclosures of drivers' personal information.[48] See Volume II, Part A, for a description of federal laws and regulations related to data security.

The federal bank regulatory agencies—the Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board (FRB), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS)—and the FTC and SEC, among others, have pursued active regulatory and enforcement programs to address the data security practices of those entities within their respective jurisdictions. Depending on the severity of a violation, the financial regulatory agencies have cited institutions for violations, without taking formal action when management quickly remedied the situation.

BJ's Wholesale Club, Inc. suffered a data breach that led to the loss of thousands of credit card numbers and millions of dollars in unauthorized charges. Following the breach, the FTC charged the company with engaging in an unfair practice by failing to provide reasonable security for credit card information. The FTC charged that BJ's stored the information in unencrypted clear text without a business need to do so, failed to defend its wireless systems against unauthorized access, failed to use strong credentials to limit access to the information, and failed to use adequate procedures for detecting and investigating intrusions. The FTC also charged that these failures were easy to exploit by hackers, and led to millions of dollars in fraudulent charges.

In April 2004, the New York Attorney General settled a case with Barnes&Noble.com, fining the company $60,000 and requiring it to implement a data security program after an investigation revealed that an alleged design vulnerability in the company's website permitted unauthorized access to consumers' personal information and enabled thieves to make fraudulent purchases. In addition, California, Vermont, and New York settled a joint action with Ziff Davis Media, Inc. involving security shortcomings that exposed the credit card numbers and other personal information of about 12,000 consumers.

In circumstances where the situation was not quickly remedied, the financial regulatory agencies have taken formal, public actions and sought civil penalties, restitution, and cease and desist orders. The FDIC has taken 17 formal enforcement actions between the beginning of 2002 and the end of 2006; the FRB has taken 14 formal enforcement actions since 2001; the OCC has taken 18 formal actions since 2002; and the OTS has taken eight formal enforcement actions in the past five years. Remedies in these cases have included substantial penalties and restitution, consumer notification, and restrictions on the use of customer information. Additionally, the FTC has obtained orders against 14 companies that allegedly failed to implement reasonable procedures to safeguard the sensitive consumer information they maintained. Most of these cases have been brought in the last two years. The SEC also has brought data security cases. See Volume II, Part B, for a description of enforcement actions relating to data security.

In addition to federal law, every state and the District of Columbia has its own laws to protect consumers from unfair or deceptive practices. Moreover, 37 states have data breach notice laws,[49] and some states have laws relevant to data security, including safeguards and disposal requirements.

Trade associations, industry collaborations, independent organizations with expertise in data security, and nonprofits have developed guidance and standards for businesses. Topics include: incorporating basic security and privacy practices into everyday business operations; developing privacy and security plans; employee screening, training, and management; implementing electronic and physical safeguards; employing threat recognition techniques; safeguarding international transactions; and credit and debit card security.[50]

Some entities that use service providers also have begun using contractual provisions that require third-party service vendors with access to the institution's sensitive data to safeguard that data.[51] Generally, these provisions also address specific practices for contracting organizations, including conducting initial and follow-up security audits of a vendor's data center, and requiring vendors to provide certification that they are in compliance with the contracting organization's privacy and data protection obligations.[52]

In 2006, the Federal Reserve Board issued a Cease and Desist Order against an Alabama-based financial institution for, among other things, failing to comply with an existing Board regulation that required implementation of an information security program.

b. Implementation of Data Security Guidelines and Rules

Many private sector organizations understand their vulnerabilities and have made significant strides in incorporating data security into their operations or improving existing security programs. See Volume II, Part C, for a description of education efforts for businesses on safeguarding data. For example, many companies and financial institutions now regularly require two-factor authentication for business conducted via

computer or telephone; send dual confirmations when customers submit a change of address; limit access to non-public personal information to necessary personnel; regularly monitor websites for phishing and firewalls for hacking; perform assessments of network security to determine the adequacy of protection from intrusion, viruses, and other data security breaches; and post identity theft education materials on company websites. Additionally, many firms within the consumer data industry offer services that provide companies with comprehensive background checks on prospective employees and tenants as permitted by law under the FCRA, and help companies verify the identity of customers.

Yet, as the reports of data breach incidents continue to show, further improvements are necessary. In a survey of financial institutions, 95 percent of respondents reported growth in their information security budget in 2005, with 71 percent reporting that they have a defined information security governance framework.[53] But many organizations also report that they are in the early stages of implementing comprehensive security procedures. For instance, in a survey of technology decision makers released in 2006, 85 percent of respondents indicated that their stored data was either somewhat or extremely vulnerable, while only 22 percent had implemented a storage security solution to prevent unauthorized access.[54] The same survey revealed that 58 percent of data managers responding believed their networks were not as secure as they could be.[55]

Small businesses face particular challenges in implementing effective data security policies for reasons of cost and lack of expertise. A 2005 survey found that while many small businesses are accelerating their adoption and use of information technology and the Internet, many do not have basic security measures in place.[56] For example, of the small businesses surveyed,

- nearly 20 percent did not use virus scans for email, a basic information security safeguard;
- over 60 percent did not protect their wireless networks with even the simplest of encryption solutions;
- over 70 percent reported expectations of a more challenging environment for detecting security threats, but only 30 percent reported increasing information security spending in 2005; and
- 74 percent reported having no information security plan in place.

Further complicating matters is the fact that some federal agencies are unable to receive data from private sector entities in an encrypted form. Therefore, some private sector entities that have to transmit sensitive data to federal agencies—sometimes pursuant to law or regulations issued by agencies—are unable to fully safeguard the transmitted data because they must decrypt the data before they can send it to the agencies. The

In 2005, the FTC settled a law enforcement action with Superior Mortgage, a mortgage company, alleging that the company failed to comply with the GLB Safeguards Rule. The FTC alleged that the company's security procedures were deficient in the areas of risk assessment, access controls, document protection, and oversight of service providers. The FTC also charged Superior with misrepresenting how it applied encryption to sensitive consumer information. Superior agreed to undertake a comprehensive data security program and retain an independent auditor to assess and certify its security procedures every two years for the next 10 years.

In 2004, an FDIC examination of a state-chartered bank disclosed significant computer system deficiencies and inadequate controls to prevent unauthorized access to customer information. The FDIC issued an order directing the bank to develop and implement an information security program, and specifically ordered the bank, among other things, to perform a formal risk assessment of internal and external threats that could result in unauthorized access to customer information. The bank also was ordered to review computer user access levels to ensure that access was restricted to only those individuals with a legitimate business need to access the information.

E-Authentication Presidential Initiative is currently addressing how agencies can more uniformly adopt appropriate technical solutions to this problem based on the level of risk involved, including, but not limited to, encryption.

c. Responding to Data Breaches in the Private Sector

Although the link between data breaches and identity theft is unclear, reports of private sector data security breaches add to consumers' fear of identity thieves gaining access to sensitive consumer information and undermine consumer confidence. Pursuant to the GLB Act, the financial regulatory agencies require financial institutions under their jurisdiction to implement programs designed to safeguard customer information. In addition, the federal bank regulatory agencies (FDIC, FRB, NCUA, OCC, and OTS) have issued guidance with respect to breach notification. In addition, 37 states have laws requiring that consumers be notified when their information has been subject to a breach.[57] Some of the laws also require that the entity that experienced the breach notify law enforcement, consumer reporting agencies, and other potentially affected parties.[58] Notice to consumers may help them avoid or mitigate injury by allowing them to take appropriate protective actions, such as placing a fraud alert on their credit file or monitoring their accounts. In some cases, the organization experiencing the breach has offered additional assistance, including free credit monitoring services. Moreover, prompt notification to law enforcement allows for the investigation and deterrence of identity theft and related unlawful conduct.

The states have taken a variety of approaches regarding when notice to consumers is required. Some states require notice to consumers whenever there is unauthorized access to sensitive data. Other states require notification only when the breach of information poses a risk to consumers. Notice is not required, for example, when the data cannot be used to commit identity theft, or when technological protections prevent fraudsters from accessing data. This approach recognizes that excessive breach notification can overwhelm consumers, causing them to ignore more significant incidents, and can impose unnecessary costs on consumers, the organization that suffered the breach, and others. Under this approach, however, organizations struggle to assess whether the risks are sufficient to warrant consumer notification. Factors relevant to that assessment often include the sensitivity of the breached information, the extent to which it is protected from access (e.g., by using technological tools for protecting data), how the breach occurred (e.g., whether the information was deliberately stolen as opposed to accidentally misplaced), and any evidence that the data actually have been misused.

A number of bills establishing a federal notice requirement have been introduced in Congress. Many of the state laws and the bills in Congress

address who should be notified, when notice should be given, what information should be provided in the notice, how notice should be effected, and the circumstances under which consumer notice should be delayed for law enforcement purposes.

Despite the substantial effort undertaken by the public and private sectors to educate businesses on how to respond to data breaches (see Volume II, Part D, for a description of education for businesses on responding to data breaches), there is room for improvement by businesses in planning for and responding to data breaches. Surveys of large corporations and retailers indicate that fewer than half of them have formal breach response plans. For example, an April 2006 cross-industry survey revealed that only 45 percent of large multinational corporations headquartered in the U.S. had a formal process for handling security violations and data breaches.[59] Fourteen percent of the companies surveyed had experienced a significant privacy breach in the past three years.[60] A July 2005 survey of large North American corporations found that although 80 percent of responding companies reported having privacy or data-protection strategies, only 31 percent had a formal notification procedure in the event of a data breach.[61] Moreover, one survey found that only 43 percent of retailers had formal incident response plans, and even fewer had tested their plans.[62]

When an online retailer became the target of an elaborate fraud ring, the company looked to one of the major credit reporting agencies for assistance. By using shared data maintained by that agency, the retailer was able to identify applications with common data elements and flag them for further scrutiny. By using the shared application data in connection with the activities of this fraud ring, the company avoided $26,000 in fraud losses.

RECOMMENDATION: ESTABLISH NATIONAL STANDARDS EXTENDING DATA PROTECTION SAFEGUARDS REQUIREMENTS AND BREACH NOTIFICATION REQUIREMENTS

Several existing laws mandate protection for sensitive consumer information, but a number of private entities are not subject to those laws. The GLB Act, for example, applies to "financial institutions," but generally not to other entities that collect and maintain sensitive information. Similarly, existing federal breach notification standards do not extend to all entities that hold sensitive consumer information, and the various state laws that contain breach notification requirements differ in various respects, complicating compliance. Accordingly, the Task Force recommends the development of (1) a national standard imposing safeguards requirements on all private entities that maintain sensitive consumer information; and (2) a national standard requiring entities that maintain sensitive consumer information to provide notice to consumers and law enforcement in the event of a breach. Such national standards should provide clarity and predictability for businesses and consumers, and should incorporate the following important principles.

Covered data. The national standards for data security and for breach notification should cover data that can be used to

perpetrate identity theft—in particular, any data or combination of consumer data that would allow someone to use, log into, or access an individual's account, or to establish a new account using the individual's identifying information. This identifying information includes a name, address, or telephone number paired with a unique identifier such as a Social Security number, a driver's license number, a biometric record, or a financial account number (together with a PIN or security code, if such PIN or code is required to access an account) (hereinafter "covered data"). The standards should not cover data, such as a name and address alone, that by itself typically would not cause harm. The definitions of covered data for data security and data breach notification requirements should be consistent.

Covered entities. The national standards for data security and breach notification should cover any private entity that collects, maintains, sells, transfers, disposes of, or otherwise handles covered data in any medium, including electronic and paper formats.

Unusable data. National standards should recognize that rendering data unusable to outside parties likely would prevent "acquisition" of the data, and thus ordinarily would satisfy an entity's legal obligations to protect the data and would not trigger notification of a breach. The standards should not endorse a specific technology because unusability is not a static concept and the effectiveness of particular technologies may change over time.

Risk-based standard for breach notification. The national breach notification standard should require that covered entities provide notice to consumers in the event of a data breach, but only when the risks to consumers are real—that is, when there is a significant risk of identity theft due to the breach. This "significant risk of identity theft" trigger for notification recognizes that excessive breach notification can overwhelm consumers, causing them to take costly actions when there is little risk, or conversely, to ignore the notices when the risks are real.

Notification to law enforcement. The national breach notification standard should provide for timely notification to law enforcement and expressly allow law enforcement to authorize a delay in required consumer notice, either for law enforcement or national security reasons (and either on its own behalf or on behalf of state or local law enforcement).

Relationship to current federal standards. The national standards for data security and breach notification should be drafted to be consistent with and so as not to displace any rules, regulations,

guidelines, standards, or guidance issued under the GLB Act by the FTC, the federal bank regulatory agencies, the SEC, or the Commodity Futures Trading Commission (CFTC), unless those agencies so determine.

Preemption of state laws. To ensure comprehensive national requirements that provide clarity and predictability, while maintaining an effective enforcement role for the states, the national data security and breach notification standards should preempt state data security and breach notification laws, but authorize enforcement by the state Attorneys General for entities not subject to the jurisdiction of the federal bank regulatory agencies, the SEC, or the CFTC.

Rulemaking and enforcement authority. Coordinated rulemaking authority under the Administrative Procedure Act should be given to the FTC, the federal bank regulatory agencies, the SEC, and the CFTC to implement the national standards. Those agencies should be authorized to enforce the standards against entities under their respective jurisdictions, and should specifically be authorized to seek civil penalties in federal district court.

Private right of action. The national standards should not provide for or create a private right of action.

Standards incorporating such principles will prompt covered entities to establish and implement administrative, technical, and physical safeguards to ensure the security and confidentiality of sensitive consumer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer. Because the costs associated with implementing safeguards or providing breach notice may be different for small businesses and larger businesses, or may differ based on the type of information held by a business, the national standard should expressly call for actions that are *reasonable* for the particular covered entity and should not adopt a one-size-fits-all approach to the implementation of safeguards.

When a major consumer lending institution encountered a problem when the loss ratio on many of its loans —including mortgages and consumer loans—became excessively high due to fraud, the bank hired a leading provider of fraud prevention products to authenticate potential customers during the application process prior to extending credit. The result was immediate: two million dollars of confirmed fraud losses were averted within the first six months of implementation.

RECOMMENDATION: BETTER EDUCATE THE PRIVATE SECTOR ON SAFEGUARDING DATA

Although much has been done to educate the private sector on how to safeguard data, the continued proliferation of data breaches suggests that more needs to be done. While there is no perfect data security system, a company that is sensitized to the

A leading payment processing and bill payment company recently deployed an automated fraud detection and case management system to more than 40 financial institutions. The system helps ensure that receiving and paying bills online remains a safe practice for consumers. To mitigate risk and reduce fraud for banks and consumers before it happens, the system combines the company's cumulative knowledge of payment patterns and a sophisticated analytics engine to help financial services organizations detect and stop unauthorized payments.

importance of data security, understands its legal obligations, and has the information it needs to secure its data adequately, is less likely to suffer a data compromise. The Task Force therefore makes the following recommendations concerning how to better educate the private sector:

- **Hold Regional Seminars for Businesses on Safeguarding Information.** By the fourth quarter of 2007, the federal financial regulatory agencies and the FTC, with support from other Task Force member agencies, should hold regional seminars and develop self-guided and online tutorials for businesses and financial institutions, about safeguarding information, preventing and reporting breaches, and assisting identity theft victims. The seminar's leaders should make efforts to include small businesses in these sessions and address their particular needs. These seminars could be co-sponsored by local bar associations, the Better Business Bureaus (BBBs), and other similar organizations. Self-guided tutorials should be made available through the Task Force's online clearinghouse at *www.idtheft.gov*.

- **Distribute Improved Guidance for Private Industry.** In the second quarter of 2007, the FTC should expand written guidance to private sector entities that are not regulated by the federal bank regulatory agencies or the SEC on steps they should take to safeguard information. The guidance should be designed to give a more detailed explanation of the broad principles encompassed in existing laws. Like the Information Technology Examination Handbook's Information Security Booklet issued under the auspices of the Federal Financial Institutions Examination Council,[63] the guidance should be risk-based and flexible, in recognition of the fact that different private sector entities will warrant different solutions.

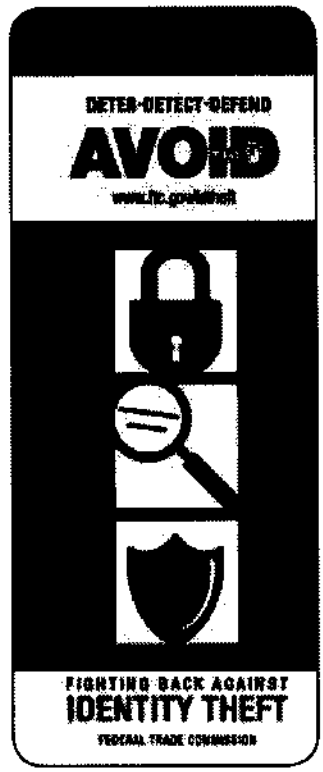
RECOMMENDATION: INITIATE INVESTIGATIONS OF DATA SECURITY VIOLATIONS

Beginning immediately, appropriate government agencies should initiate investigations of and, if appropriate, take enforcement actions against entities that violate the laws governing data security. The FTC, SEC, and federal bank regulatory agencies have used regulatory and enforcement efforts to require companies to maintain appropriate information safeguards under the law. Federal agencies should continue and expand these efforts to ensure that such entities use reasonable data security measures. Where appropriate, the agencies should share information about those enforcement actions on *www.idtheft.gov*.

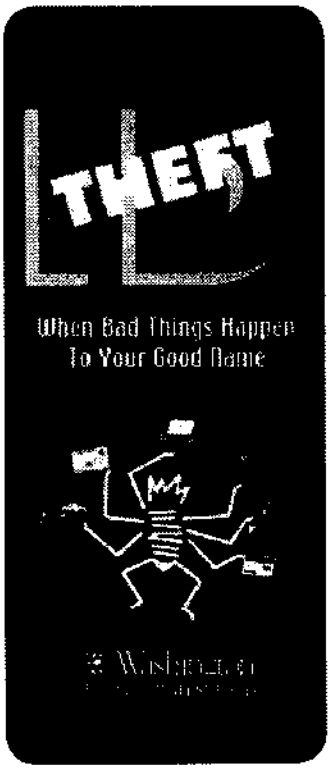
4. EDUCATING CONSUMERS ON PROTECTING THEIR PERSONAL INFORMATION

The first line of defense against identity theft often is an aware and motivated consumer who takes reasonable precautions to protect his information. Every day, unwitting consumers create risks to the security of their personal information. From failing to install firewall protection on a computer hard drive to leaving paid bills in a mail slot, consumers leave the door open to identity thieves. Consumer education is a critical component of any plan to reduce the incidence of identity theft.

The federal government has been a leading provider of consumer information about identity theft. Numerous departments and agencies target identity theft-related messages to relevant populations. *See* Volume II, Part E, for a description of federal consumer education efforts. The FTC, through its Identity Theft Clearinghouse and ongoing outreach, plays a primary role in consumer awareness and education, developing information that has been co-branded by a variety of groups and agencies. Its website, *www.ftc.gov/idtheft* serves as a comprehensive one-stop resource in both English and Spanish for consumers. The FTC also recently implemented a national public awareness campaign centered around the themes of "Deter, Detect, and Defend," which seeks to drive behavioral changes in consumers that will reduce their risk of identity theft (Deter); encourage them to monitor their credit reports and accounts to alert them of identity theft as soon as possible after it occurs (Detect); and mitigate the damage caused by identity theft should it occur (Defend). This campaign, mandated in the FACT Act, consists of direct messaging to consumers as well as material written for organizations, community leaders, and local law enforcement. The Deter, Detect, and Defend materials have been adopted and distributed by hundreds of entities, both public and private.



The SSA and the federal regulatory agencies are among the many other government bodies that also play a significant role in educating consumers on how to protect themselves. For example, the SSA added a message to its SSN verification printout warning the public not to share their SSNs with others. This warning was especially timely in the aftermath of Hurricane Katrina, which necessitated the issuance of a large number of those printouts. Similarly, the Senior Medicare Patrol (SMP) program, funded by U.S. Administration on Aging in the Department of Health and Human Services, uses senior volunteers to educate their peers about protecting their personal information and preventing and identifying consumer and health care fraud. The SMP program also has worked closely with the Centers for Medicare and Medicaid Services to protect seniors from new scams aimed at defrauding them of their Medicare numbers and other personal information. And the U.S. Postal Inspection Service has produced a number of consumer education materials, including several videos, alerting the public to the problems associated with identity theft.



Significant consumer education efforts also are taking place at the state level. Nearly all of the state Attorneys General offer information on the prevention and remediation of identity theft on their websites, and several states have conducted conferences and workshops focused on education and training in privacy protection and identity theft prevention. Over the past year, the Attorney General of Illinois and the Governors of New Mexico and California have hosted summit meetings, bringing together law enforcement, educators, victims' coordinators, consumer advocates, and the business community to develop better strategies for educating the public and fighting identity theft. The National Governors Association convened the National Strategic Policy Council on Cyber and Electronic Crime in September 2006 to trigger a coordinated education and prevention effort by federal, state, and local policymakers. The New York State Consumer Protection Board has conducted "Consumer Action Days," with free seminars about identity theft and other consumer protection issues.

Police departments also provide consumer education to their communities. Many departments have developed materials and make them available in police stations, in city government buildings, and on websites.[64] As of this writing, more than 500 local police departments are using the FTC's "Deter, Detect, Defend" campaign materials to teach their communities about identity theft. Other groups, including the National Apartment Association and the National Association of Realtors, also have promoted this campaign by distributing the materials to their membership.

Although most educational material is directed at consumers in general, some is aimed at and tailored to specific target groups. One such group is college students. For several reasons—including the vast amounts of personal data that colleges maintain about them and their tendency to keep personal data unguarded in shared dormitory rooms—students are frequent targets of identity thieves. According to one report, one-third to one-half of all reported personal information breaches in 2006 have occurred at colleges and universities.[65] In recognition of the increased vulnerability of this population, many universities are providing information to their students about the risks of identity theft through web sites, orientation campaigns, and seminars.[66]

Federal, state, and local government agencies provide a great deal of identity theft-related information to the public through the Internet, printed materials, DVDs, and in-person presentations. The messages the agencies provide—how to protect personal information, how to recognize a potential problem, where to report a theft, and how to deal with the aftermath—are echoed by industry, law enforcement, advocates, and the media. See Volume II, Part F, for a description of private sector consumer education efforts. But there is little coordination among the agencies on current education programs. Dissemination in some cases is random, information is