The President's Identity Theft Task Force

Combating Identity Theft
A Strategic Plan

April 2007

Table of Contents

APPENDICES

ENDNOTES

Glossary of Acronyms

AAMVA–American Association of Motor Vehicle Administrators

AARP–American Association of Retired Persons

ABA–American Bar Association

APWG–Anti-Phishing Working Group

BBB–Better Business Bureau

BIN–Bank Identification Number

BJA–Bureau of Justice Assistance

BJS–Bureau of Justice Statistics

CCIPS–Computer Crime and Intellectual Property Section (DOJ)

CCMSI–Credit Card Mail Security Initiative

CFAA–Computer Fraud and Abuse Act

CFTC–Commodity Futures Trading Commission

CIO–Chief Information Officer

CIP–Customer Identification Program

CIRFU–Cyber Initiative and Resource Fusion Center

CMRA–Commercial Mail Receiving Agency

CMS–Centers for Medicare and Medicaid Services (HHS)

CRA–Consumer reporting agency

CVV2–Card Verification Value 2

DBFTF–Document and Benefit Fraud Task Force

DHS–Department of Homeland Security

DOJ–Department of Justice

DPPA–Drivers Privacy Protection Act of 1994

FACT Act–Fair and Accurate Credit Transactions Act of 2003

FBI–Federal Bureau of Investigation

FCD–Financial Crimes Database

FCRA–Fair Credit Reporting Act

FCU Act–Federal Credit Union Act

FDI Act–Federal Deposit Insurance Act

FDIC–Federal Deposit Insurance Corporation

FEMA–Federal Emergency Management Agency

FERPA–Family and Educational Rights and Privacy Act of 1974

FFIEC–Federal Financial Institutions Examination Council

FIMSI–Financial Industry Mail Security Initiative

FinCEN–Financial Crimes Enforcement Network (Department of Treasury)

FISMA–Federal Information Security Management Act of 2002

FRB–Federal Reserve Board of Governors

FSI–Financial Services, Inc.

FTC–Federal Trade Commission

FTC Act–Federal Trade Commission Act

GAO–Government Accountability Office

GLB Act–Gramm-Leach-Bliley Act

HHS–Department of Health and Human Services

HIPAA–Health Insurance Portability and Accountability Act of 1996

IACP–International Association of Chiefs of Police

IAFCI–International Association of Financial Crimes Investigators

IC3–Internet Crime Complaint Center

ICE–U.S. Immigration and Customs Enforcement

IRS–Internal Revenue Service

IRS CI–IRS Criminal Investigation Division

IRTPA–Intelligence Reform and Terrorism Prevention Act of 2004

ISI–Intelligence Sharing Initiative (U.S. Postal Inspection Service)

ISP–Internet service provider

ISS LOB–Information Systems Security Line of Business

ITAC–Identity Theft Assistance Center

ITCI–Information Technology Compliance Institute

ITRC–Identity Theft Resource Center

MCC–Major Cities Chiefs

NAC–National Advocacy Center

NASD–National Association of Securities Dealers, Inc.

NCFTA–National Cyber Forensic Training Alliance

NCHELP–National Council of Higher Education Loan Programs

NCUA–National Credit Union Administration

NCVS–National Crime Victimization Survey

NDAA–National District Attorneys Association

NIH–National Institutes of Health

NIST–National Institute of Standards and Technology

NYSE–New York Stock Exchange

OCC–Office of the Comptroller of the Currency

OIG–Office of the Inspector General

OJP–Office of Justice Programs (DOJ)

OMB–Office of Management and Budget

OPM–Office of Personnel Management

OTS–Office of Thrift Supervision

OVC–Office for Victims of Crime (DOJ)

PCI–Payment Card Industry

PIN–Personal Identification Number

PMA–President's Management Agenda

PRC–Privacy Rights Clearinghouse

QRP–Questionable Refund Program (IRS CI)

RELEAF–Operation Retailers & Law Enforcement Against Fraud

RISS–Regional Information Sharing Systems

RITNET–Regional Identity Theft Network

RPP–Return Preparer Program (IRS CI)

SAR–Suspicious Activity Report

SBA–Small Business Administration

SEC–Securities and Exchange Commission

SMP–Senior Medicare Patrol

SSA–Social Security Administration

SSL–Security Socket Layer

SSN–Social Security number

TIGTA–Treasury Inspector General for Tax Administration

UNCC–United Nations Crime Commission

USA PATRIOT Act–Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Pub. L. No. 107-56)

USB–Universal Serial Bus

US-CERT–United States Computer Emergency Readiness Team

USPIS–United States Postal Inspection Service

USSS–United States Secret Service

VHA–Veterans Health Administration

VOIP–Voice Over Internet Protocol

VPN–Virtual private network

WEDI–Workgroup for Electronic Data Interchange

Identity Theft Task Force Members

Alberto R. Gonzales, Chairman
Attorney General

Deborah Platt Majoras, Co-Chairman
Chairman, Federal Trade Commission

Henry M. Paulson
Department of Treasury

Carlos M. Gutierrez
Department of Commerce

Michael O. Leavitt
Department of Health and Human Services

R. James Nicholson
Department of Veterans Affairs

Michael Chertoff
Department of Homeland Security

Rob Portman
Office of Management and Budget

John E. Potter
United States Postal Service

Ben S. Bernanke
Federal Reserve System

Linda M. Springer
Office of Personnel Management

Sheila C. Bair
Federal Deposit Insurance Corporation

Christopher Cox
Securities and Exchange Commission

JoAnn Johnson
National Credit Union Administration

Michael J. Astrue
Social Security Administration

John C. Dugan
Office of the Comptroller of the Currency

John M. Reich
Office of Thrift Supervision

Alberto R. Gonzales, Chairman
Attorney General

Deborah Platt Majoras, Co-Chairman
Chairman, Federal Trade Commission

Letter to the President

APRIL 11, 2007

The Honorable George W. Bush
President of the United States
The White House
Washington, D.C.

Dear Mr. President:

By establishing the President's Task Force on Identity Theft by Executive Order 13402 on May 10, 2006, you launched a new era in the fight against identity theft. As you recognized, identity theft exacts a heavy financial and emotional toll from its victims, and it severely burdens our economy. You called for a coordinated approach among government agencies to vigorously combat this crime. Your charge to us was to craft a strategic plan aiming to make the federal government's efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution. To meet that charge, we examined the tools law enforcement can use to prevent, investigate, and prosecute identity theft crimes; to recover the proceeds of these crimes; and to ensure just and effective punishment of identity thieves. We also surveyed current education efforts by government agencies and the private sector on how individuals and corporate citizens can protect personal data. And because government must help reduce, rather than exacerbate, incidents of identity theft, we worked with many federal agencies to determine how the government can increase safeguards to better secure the personal data that it and private businesses hold. Like you, we spoke to many citizens whose lives have been uprooted by identity theft, and heard their suggestions on ways to help consumers guard against this crime and lessen the burdens of their recovery. We conducted meetings, spoke with stakeholders, and invited public comment on key issues.

The views you expressed in the Executive Order are widely shared. There is a consensus that identity theft's damage is widespread, that it targets all demographic groups, that it harms both consumers and businesses, and that its effects can range far beyond financial harm. We were pleased to learn that many federal departments and agencies, private businesses, and universities are trying to create a culture of security, although some have been faster than others to construct systems to protect personal information.

There is no quick solution to this problem. But, we believe that a coordinated strategic plan can go a long way toward stemming the injuries caused by identity theft and, we hope, putting identity thieves out of business. Taken as a whole, the recommendations that comprise this strategic plan are designed to strengthen the efforts of federal, state, and local law enforcement officers; to educate consumers and businesses on deterring, detecting, and defending against identity theft; to assist law enforcement officers in apprehending and prosecuting identity thieves; and to increase the safeguards employed by federal agencies and the private sector with respect to the personal data with which they are entrusted.

Thank you for the privilege of serving on this Task Force. Our work is ongoing, but we now have the honor, under the provisions of your Executive Order, of transmitting the report and recommendations of the President's Task Force on Identity Theft.

Very truly yours,

Alberto R. Gonzales, Chairman
Attorney General

Deborah Platt Majoras, Co-Chairman
Chairman, Federal Trade Commission

I. Executive Summary

From Main Street to Wall Street, from the back porch to the front office, from the kitchen table to the conference room, Americans are talking about identity theft. The reason: millions of Americans each year suffer the financial and emotional trauma it causes. This crime takes many forms, but it invariably leaves victims with the task of repairing the damage to their lives. It is a problem with no single cause and no single solution.

A. INTRODUCTION

Eight years ago, Congress enacted the Identity Theft and Assumption Deterrence Act,[1] which created the federal crime of identity theft and charged the Federal Trade Commission (FTC) with taking complaints from identity theft victims, sharing these complaints with federal, state, and local law enforcement, and providing the victims with information to help them restore their good name. Since then, federal, state, and local agencies have taken strong action to combat identity theft. The FTC has developed the Identity Theft Data Clearinghouse into a vital resource for consumers and law enforcement agencies; the Department of Justice (DOJ) has prosecuted vigorously a wide range of identity theft schemes under the identity theft statutes and other laws; the federal financial regulatory agencies[2] have adopted and enforced robust data security standards for entities under their jurisdiction; Congress passed, and the Department of Homeland Security issued draft regulations on, the REAL ID Act of 2005; and numerous other federal agencies, such as the Social Security Administration (SSA), have educated consumers on avoiding and recovering from identity theft. Many private sector entities, too, have taken proactive and significant steps to protect data from identity thieves, educate consumers about how to prevent identity theft, assist law enforcement in apprehending identity thieves, and assist identity theft victims who suffer losses.

Over those same eight years, however, the problem of identity theft has become more complex and challenging for the general public, the government, and the private sector. Consumers, overwhelmed with weekly media reports of data breaches, feel vulnerable and uncertain of how to protect their identities. At the same time, both the private and public sectors have had to grapple with difficult, and costly, decisions about investments in safeguards and what more to do to protect the public. And, at every level of government—from the largest cities with major police departments to the smallest towns with one fraud detective—identity theft has placed increasingly pressing demands on law enforcement.

Public comments helped the Task Force define the issues and challenges posed by identity theft and develop its strategic responses. To ensure that the Task Force heard from all stakeholders, it solicited comments from the public.

In addition to consumer advocacy groups, law enforcement, business, and industry, the Task Force also received comments from identity theft victims themselves.[3] The victims wrote of the burdens and frustrations associated with their recovery from this crime. Their stories reaffirmed the need for the government to act quickly to address this problem.

The overwhelming majority of the comments received by the Task Force strongly affirmed the need for a fully coordinated approach to fighting the problem through prevention, awareness, enforcement, training, and victim assistance. Consumers wrote to the Task Force exhorting the public and private sectors to do a better job of protecting their Social Security numbers (SSNs), and many of those who submitted comments discussed the challenges raised by the overuse of Social Security numbers as identifiers. Others, representing certain business sectors, pointed to the beneficial uses of SSNs in fraud detection. The Task Force was mindful of both considerations, and its recommendations seek to strike the appropriate balance in addressing SSN use. Local law enforcement officers, regardless of where they work, wrote of the challenges of multi-jurisdictional investigations, and called for greater coordination and resources to support the investigation and prosecution of identity thieves. Various business groups described the steps they have taken to minimize the occurrence and impact of the crime, and many expressed support for risk-based, national data security and breach notification requirements.

These communications from the public went a long way toward informing the Task Force's recommendation for a fully coordinated strategy. Only an approach that encompasses effective prevention, public awareness and education, victim assistance, and law enforcement measures, and fully engages federal, state, and local authorities will be successful in protecting citizens and private entities from the crime.

B. THE STRATEGY

Although identity theft is defined in many different ways, it is, fundamentally, the misuse of another individual's personal information to commit fraud. Identity theft has at least three stages in its "life cycle," and it must be attacked at each of those stages:

First, the identity thief attempts to acquire a victim's personal information.

Criminals must first gather personal information, either through low-tech methods—such as stealing mail or workplace records, or "dumpster diving"—or through complex and high-tech frauds, such as hacking and the use of malicious computer codes. The loss or theft of personal information by itself, however, does not immediately lead to identity theft. In some cases, thieves who steal personal items inadvertently steal personal information

that is stored in or with the stolen personal items, yet never make use of the personal information. It has recently been reported that, during the past year, the personal records of nearly 73 million people have been lost or stolen, but that there is no evidence of a surge in identity theft or financial fraud as a result. Still, because any loss or theft of personal information is troubling and potentially devastating for the persons involved, a strategy to keep consumer data out of the hands of criminals is essential.

Second, the thief attempts to misuse the information he has acquired.

In this stage, criminals have acquired the victim's personal information and now attempt to sell the information or use it themselves. The misuse of stolen personal information can be classified in the following broad categories:

- **Existing account fraud:** This occurs when thieves obtain account information involving credit, brokerage, banking, or utility accounts that are already open. Existing account fraud is typically a less costly, but more prevalent, form of identity theft. For example, a stolen credit card may lead to thousands of dollars in fraudulent charges, but the card generally would not provide the thief with enough information to establish a false identity. Moreover, most credit card companies, as a matter of policy, do not hold consumers liable for fraudulent charges, and federal law caps liability of victims of credit card theft at $50.
- **New account fraud:** Thieves use personal information, such as Social Security numbers, birth dates, and home addresses, to open new accounts in the victim's name, make charges indiscriminately, and then disappear. While this type of identity theft is less likely to occur, it imposes much greater costs and hardships on victims.

In addition, identity thieves sometimes use stolen personal information to obtain government, medical, or other benefits to which the criminal is not entitled.

Third, an identity thief has completed his crime and is enjoying the benefits, while the victim is realizing the harm.

At this point in the life cycle of the theft, victims are first learning of the crime, often after being denied credit or employment, or being contacted by a debt collector seeking payment for a debt the victim did not incur.

In light of the complexity of the problem at each of the stages of this life cycle, the Identity Theft Task Force is recommending a plan that marshals government resources to crack down on the criminals who traffic in stolen identities, strengthens efforts to protect the personal information of our nation's citizens, helps law enforcement officials investigate and prosecute identity thieves, helps educate consumers and businesses about protecting themselves, and increases the safeguards on personal data entrusted to federal agencies and private entities.

The Plan focuses on improvements in four key areas:

- keeping sensitive consumer data out of the hands of identity thieves through better data security and more accessible education;
- making it more difficult for identity thieves who obtain consumer data to use it to steal identities;
- assisting the victims of identity theft in recovering from the crime; and
- deterring identity theft by more aggressive prosecution and punishment of those who commit the crime.

In these four areas, the Task Force makes a number of recommendations summarized in greater detail below. Among those recommendations are the following broad policy changes:

- that federal agencies should reduce the unnecessary use of Social Security numbers (SSNs), the most valuable commodity for an identity thief;
- that national standards should be established to require private sector entities to safeguard the personal data they compile and maintain and to provide notice to consumers when a breach occurs that poses a significant risk of identity theft;
- that federal agencies should implement a broad, sustained awareness campaign to educate consumers, the private sector, and the public sector on deterring, detecting, and defending against identity theft; and
- that a National Identity Theft Law Enforcement Center should be created to allow law enforcement agencies to coordinate their efforts and information more efficiently, and investigate and prosecute identity thieves more effectively.

The Task Force believes that all of the recommendations in this strategic plan—from these broad policy changes to the small steps—are necessary to wage a more effective fight against identity theft and reduce its incidence and damage. Some recommendations can be implemented relatively quickly; others will take time and the sustained cooperation of government entities and the private sector. Following are the recommendations of the President's Task Force on Identity Theft:

PREVENTION: KEEPING CONSUMER DATA OUT OF THE HANDS OF CRIMINALS

Identity theft depends on access to consumer data. Reducing the opportunities for thieves to get the data is critical to fighting the crime. Government, the business community, and consumers have roles to play 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 carry financial costs for everyone involved. While "perfect security" does not exist, all entities that collect and maintain sensitive consumer information must take reasonable and appropriate steps to protect it.

Data Security in Public Sector

- **Decrease the Unnecessary Use of Social Security Numbers in the Public Sector by Developing Alternative Strategies for Identity Management**
  - Survey current use of SSNs by federal government
  - Issue guidance on appropriate use of SSNs
  - Establish clearinghouse for "best" agency practices that minimize use of SSNs
  - Work with state and local governments to review use of SSNs
- **Educate Federal Agencies on How to Protect Data; Monitor Their Compliance with Existing Guidance**
  - Develop concrete guidance and best practices
  - Monitor agency compliance with data security guidance
  - Protect portable storage and communications devices
- **Ensure Effective, Risk-Based Responses to Data Breaches Suffered by Federal Agencies**
  - Issue data breach guidance to agencies
  - Publish a "routine use" allowing disclosure of information after a breach to those entities that can assist in responding to the breach

Data Security in Private Sector

- **Establish National Standards for Private Sector Data Protection Requirements and Breach Notice Requirements**
- **Develop Comprehensive Record on Private Sector Use of Social Security Numbers**
- **Better Educate the Private Sector on Safeguarding Data**
  - Hold regional seminars for businesses on safeguarding information
  - Distribute improved guidance for private industry
- **Initiate Investigations of Data Security Violations**

- **Initiate a Multi-Year Public Awareness Campaign**
  - Develop national awareness campaign
  - Enlist outreach partners
  - Increase outreach to traditionally underserved communities
  - Establish "Protect Your Identity" Days
- **Develop Online Clearinghouse for Current Educational Resources**

PREVENTION: MAKING IT HARDER TO MISUSE CONSUMER DATA

Because security systems are imperfect and thieves are resourceful, it is essential to reduce the opportunities for criminals to misuse the data they steal. An identity thief who wants to open new accounts in a victim's name must be able to (1) provide identifying information to allow the creditor or other grantor of benefits to access information on which to base a decision about eligibility; and (2) convince the creditor that he is the person he purports to be.

Authentication includes determining a person's identity at the beginning of a relationship (sometimes called verification), and later ensuring that he is the same person who was originally authenticated. But the process can fail: Identity documents can be falsified; the accuracy of the initial information and the accuracy or quality of the verifying sources can be questionable; employee training can be insufficient; and people can fail to follow procedures.

Efforts to facilitate the development of better ways to authenticate consumers without burdening consumers or businesses—for example, multi-factor authentication or layered security—would go a long way toward preventing criminals from profiting from identity theft.

- **Hold Workshops on Authentication**
  - Engage academics, industry, entrepreneurs, and government experts on developing and promoting better ways to authenticate identity
  - Issue report on workshop findings
- **Develop a Comprehensive Record on Private Sector Use of SSNs**

VICTIM RECOVERY: HELPING CONSUMERS REPAIR THEIR LIVES

Identity theft can be committed despite a consumer's best efforts at securing information. Consumers have a number of rights and resources available, but some surveys indicate that they are not as well-informed as they could be. Government agencies must work together to ensure that victims have the knowledge, tools, and assistance necessary to minimize the damage and begin the recovery process.

- **Provide Specialized Training About Victim Recovery to First Responders and Others Offering Direct Assistance to Identity Theft Victims**
  - Train law enforcement officers
  - Provide educational materials for first responders that can be used as a reference guide for identity theft victims
  - Create and distribute an ID Theft Victim Statement of Rights
  - Design nationwide training for victim assistance counselors
- **Develop Avenues for Individualized Assistance to Identity Theft Victims**
- **Amend Criminal Restitution Statutes to Ensure That Victims Recover the Value of Time Spent in Trying to Remediate the Harms Suffered**
- **Assess Whether to Implement a National System That Allows Victims to Obtain an Identification Document for Authentication Purposes**
- **Assess Efficacy of Tools Available to Victims**
  - Conduct assessment of FACT Act remedies under FCRA
  - Conduct assessment of state credit freeze laws

LAW ENFORCEMENT: PROSECUTING AND PUNISHING IDENTITY THIEVES

Strong criminal law enforcement is necessary to punish and deter identity thieves. The increasing sophistication of identity thieves in recent years has meant that law enforcement agencies at all levels of government have had to increase the resources they devote to investigating related crimes. The investigations are labor-intensive and generally require a staff of detectives, agents, and analysts with multiple skill sets. When a suspected theft involves a large number of potential victims, investigative agencies often need additional personnel to handle victim-witness coordination.

Coordination and Information/Intelligence Sharing

- **Establish a National Identity Theft Law Enforcement Center**
- **Develop and Promote the Use of a Universal Identity Theft Report Form**
- **Enhance Information Sharing Between Law Enforcement and the Private Sector**
  - Enhance ability of law enforcement to receive information from financial institutions
  - Initiate discussions with financial services industry on countermeasures to identity theft
  - Initiate discussions with credit reporting agencies on preventing identity theft

Coordination with Foreign Law Enforcement

- **Encourage Other Countries to Enact Suitable Domestic Legislation Criminalizing Identity Theft**
- **Facilitate Investigation and Prosecution of International Identity Theft by Encouraging Other Nations to Accede to the Convention on Cybercrime**
- **Identify the Nations that Provide Safe Havens for Identity Thieves and Use All Measures Available to Encourage Those Countries to Change Their Policies**
- **Enhance the United States Government's Ability to Respond to Appropriate Foreign Requests for Evidence in Criminal Cases Involving Identity Theft**
- **Assist, Train, and Support Foreign Law Enforcement**

Prosecution Approaches and Initiatives

- **Increase Prosecutions of Identity Theft**
  - Designate an identity theft coordinator for each United States Attorney's Office to design a specific identity theft program for each district
  - Evaluate monetary thresholds for prosecution
  - Encourage state prosecution of identity theft
  - Create working groups and task forces
- **Conduct Targeted Enforcement Initiatives**
  - Conduct enforcement initiatives focused on using unfair or deceptive means to make SSNs available for sale
  - Conduct enforcement initiatives focused on identity theft related to the health care system
  - Conduct enforcement initiatives focused on identity theft by illegal aliens
- **Review Civil Monetary Penalty Programs**

Gaps in Statutes Criminalizing Identity Theft

▶ Close the Gaps in Federal Criminal Statutes Used to Prosecute Identity Theft-Related Offenses to Ensure Increased Federal Prosecution of These Crimes

- Amend the identity theft and aggravated identity theft statutes to ensure that identity thieves who misappropriate information belonging to corporations and organizations can be prosecuted
- Add new crimes to the list of predicate offenses for aggravated identity theft offenses
- Amend the statute that criminalizes the theft of electronic data by eliminating the current requirement that the information must have been stolen through interstate communications
- Penalize creators and distributors of malicious spyware and keyloggers
- Amend the cyber-extortion statute to cover additional, alternate types of cyber-extortion

▶ Ensure That an Identity Thief's Sentence Can Be Enhanced When the Criminal Conduct Affects More Than One Victim

Law Enforcement Training

▶ Enhance Training for Law Enforcement Officers and Prosecutors

- Develop course at National Advocacy Center focused on investigation and prosecution of identity theft
- Increase number of regional identity theft seminars
- Increase resources for law enforcement on the Internet
- Review curricula to enhance basic and advanced training on identity theft

Measuring the Success of Law Enforcement

▶ Enhance the Gathering of Statistical Data Impacting the Criminal Justice System's Response to Identity Theft

- Gather and analyze statistically reliable data from identity theft victims
- Expand scope of national crime victimization survey
- Review U.S. Sentencing Commission data
- Track prosecutions of identity theft and resources spent
- Conduct targeted surveys

II. The Contours of the Identity Theft Problem

Every day, too many Americans learn that their identities have been compromised, often in ways and to an extent they could not have imagined. Identity theft victims experience a sense of hopelessness when someone steals their good name and good credit to commit fraud. These victims also speak of their frustration in fighting against an unknown opponent.

"I was absolutely heartsick to realize our bank accounts were frozen, our names were on a bad check list, and my driver's license was suspended. I hold three licenses in the State of Ohio—my driver's license, my real estate license, and my R.N. license. After learning my driver's license was suspended, I was extremely fearful that my professional licenses might also be suspended as a result of the actions of my imposter."

Maureen Mitchell
Testimony Before
House Committee on
Financial Services,
Subcommittee on
Financial Institutions and
Consumer Credit
June 24, 2003

Identity theft—the misuse of another individual's personal information to commit fraud—can happen in a variety of ways, but the basic elements are the same. Criminals first gather personal information, either through low-tech methods such as stealing mail or workplace records, or "dumpster diving," or through complex and high-tech frauds such as hacking and the use of malicious computer code. These data thieves then sell the information or use it themselves to open new credit accounts, take over existing accounts, obtain government benefits and services, or even evade law enforcement by using a new identity. Often, individuals learn that they have become victims of identity theft only after being denied credit or employment, or when a debt collector seeks payment for a debt the victim did not incur.

Individual victim experiences best portray the havoc that identity thieves can wreak. For example, in July 2001, an identity thief gained control of a retired Army Captain's identity when Army officials at Fort Bragg, North Carolina, issued the thief an active duty military identification card in the retired captain's name and with his Social Security number. The military identification, combined with the victim's then-excellent credit history, allowed the identity thief to go on an unhindered spending spree lasting several months. From July to December 2001, the identity thief acquired goods, services, and cash in the victim's name valued at over $260,000. The victim identified more than 60 fraudulent accounts of all types that were opened in his name: credit accounts, personal and auto loans, checking and savings accounts, and utility accounts. The identity thief purchased two trucks valued at over $85,000 and a Harley-Davidson motorcycle for $25,000. The thief also rented a house and purchased a time-share in Hilton Head, South Carolina, in the victim's name.[4]

In another instance, an elderly woman suffering from dementia was victimized by her caregivers, who admitted to stealing as much as $200,000 from her before her death. The thieves not only used the victim's existing credit card accounts, but also opened new credit accounts in her name, obtained financing in her name to purchase new vehicles for themselves, and, using a fraudulent power of attorney, removed $176,000 in U.S. Savings Bonds from the victim's safe-deposit boxes.[5]

In these ways and others, consumers' lives are disrupted and displaced by identity theft. While federal agencies, the private sector, and consumers themselves already have accomplished a great deal to address the causes

and impact of identity theft, much work remains to be done. The following strategic plan focuses on a coordinated government response to: strengthen efforts to prevent identity theft; investigate and prosecute identity theft; raise awareness; and ensure that victims receive meaningful assistance.

A. PREVALENCE AND COSTS OF IDENTITY THEFT

There is considerable debate about the prevalence and cost of identity theft in the United States. Numerous studies have attempted to measure the extent of this crime. DOJ, FTC, the Gartner Group, and Javelin Research are just some of the organizations that have published reports of their identity theft surveys.[6] While some of the data from these surveys differ, there is agreement that identity theft exacts a serious toll on the American public.

Although greater empirical research is needed, the data show that annual monetary losses are in the billions of dollars. This includes losses associated with new account fraud, a more costly, but less prevalent form of identity theft, and misuse of existing accounts, a more prevalent but less costly form of identity theft. Businesses suffer most of the direct losses from both forms of identity theft because individual victims generally are not held responsible for fraudulent charges. Individual victims, however, also collectively spend billions of dollars recovering from the effects of the crime.

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, monetary costs of identity theft include indirect costs to businesses for fraud prevention and mitigation of the harm once it has occurred (e.g., for mailing notices to consumers and upgrading systems). Similarly, individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

Consumers' fears of becoming identity theft victims also may harm our digital economy. In a 2006 online survey conducted by the Business Software Alliance and Harris Interactive, nearly one in three adults (30 percent) said that security fears compelled them to shop online less or not at all during the 2005/2006 holiday season.[7] Similarly, a Cyber Security Industry Alliance

In an article entitled "Waitress Gets Own ID When Carding Patron," the Associated Press reported that a bar waitress checking to see whether a patron was old enough to legally drink alcohol was handed her own stolen driver's license, which she reported missing weeks earlier in Lakewood, Ohio. The patron was later charged with identity theft and receiving stolen property.

survey in June 2005 found that 48 percent of consumers avoided making purchases on the Internet because they feared that their financial information might be stolen.[8] Although no studies have correlated these attitudes with actual online buying habits, these surveys indicate that security concerns likely inhibit some commercial use of the Internet.

B. IDENTITY THIEVES: WHO THEY ARE

Unlike some groups of criminals, identity thieves cannot be readily classified. No surveys provide comprehensive data on their primary personal or demographic characteristics. For the most part, victims are not in a good position to know who stole their information or who misused it. According to the FTC's 2003 survey of identity theft, about 14 percent of victims claim to know the perpetrator, who may be a family member, friend, or in-home employee.

Identity thieves can act alone or as part of a criminal enterprise. Each poses unique threats to the public.

Individuals

In September 2005, a defendant was sentenced by a federal judge in Colorado to a year and one day in prison, and ordered to pay $181,517.05 in restitution, after pleading guilty to the misuse of a Social Security number. The defendant had obtained the identifying information of two individuals, including their SSNs, and used one such identity to obtain a false Missouri driver's license, to cash counterfeit checks, and to open fraudulent credit accounts. The defendant used the second identity to open a fraudulent credit account and to cash fraudulent checks. The case was investigated by the SSA OIG, FBI, U.S. Postal Inspection Service, and the St. Charles, Missouri, Police Department.

According to law enforcement agencies, identity thieves often have no prior criminal background and sometimes have pre-existing relationships with the victims. Indeed, identity thieves have been known to prey on people they know, including coworkers, senior citizens for whom they are serving as caretakers, and even family members. Some identity thieves rely on techniques of minimal sophistication, such as stealing mail from homeowners' mailboxes or trash containing financial documents. In some jurisdictions, identity theft by illegal immigrants has resulted in passport, employment, and Social Security fraud. Occasionally, small clusters of individuals with no significant criminal records work together in a loosely knit fashion to obtain personal information and even to create false or fraudulent documents.[9]

A number of recent reports have focused on the connection between individual methamphetamine ("meth") users and identity theft.[10] Law enforcement agencies in Albuquerque, Honolulu, Phoenix, Sacramento, Seattle, and other cities have reported that meth addicts are engaging in identity and data theft through burglaries, mail theft, and theft of wallets and purses. In Salt Lake City, meth users reportedly are organized by white-supremacist gangs to commit identity theft.[11] Tellingly, as meth use has risen sharply in recent years, especially in the western United States, some of the same jurisdictions reporting the highest levels of meth use also suffer from the highest incidence of identity theft. Some state law enforcement officials believe that the two increases might be related, and that identity theft may serve as a major funding mechanism for meth labs and purchases.

Significant Criminal Groups and Organizations

Law enforcement agencies around the country have observed a steady increase in the involvement of groups and organizations of repeat offenders or career criminals in identity theft. Some of these groups—including national gangs such as Hell's Angels and MS-13—are formally organized, have a hierarchical structure, and are well-known to law enforcement because of their longstanding involvement in other major crimes such as drug trafficking. Other groups are more loosely-organized and, in some cases, have taken advantage of the Internet to organize, contact each other, and coordinate their identity theft activities more efficiently. Members of these groups often are located in different countries and communicate primarily via the Internet. Other groups have a real-world connection with one another and share a nationality or ethnic group.

Law enforcement agencies also have seen increased involvement of foreign organized criminal groups in computer- or Internet-related identity theft schemes. In Asia and Eastern Europe, for example, organized groups are increasingly sophisticated both in the techniques they use to deceive Internet users into disclosing personal data, and in the complexity of tools they use, such as keyloggers (programs that record every keystroke as an Internet user logs onto his computer or a banking website), spyware (software that covertly gathers user information through the user's Internet connection, without the user's knowledge), and botnets (networks of computers that criminals have compromised and taken control of for some other purpose, ranging from distribution of spam and malicious computer code to attacks on other computers). According to law enforcement agencies, such groups also are demonstrating increasing levels of sophistication and specialization in their online crime, even selling goods and services—such as software templates for making counterfeit identification cards and payment card magnetic strip encoders—that make the stolen data even more valuable to those who have it.

C. HOW IDENTITY THEFT HAPPENS: THE TOOLS OF THE TRADE

Consumer information is the currency of identity theft, and perhaps the most valuable piece of information for the thief is the SSN. The SSN and a name can be used in many cases to open an account and obtain credit or other benefits in the victim's name. Other data, such as personal identification numbers (PINs), account numbers, and passwords, also are valuable because they enable thieves to access existing consumer accounts.

Identity theft is prevalent in part because criminals are able to obtain personal consumer information everywhere such data are located or stored. Homes and businesses, cars and health-club lockers, electronic networks, and even trash baskets and dumpsters have been targets for identity thieves. Some

In July 2003, a Russian computer hacker was sentenced in federal court to a prison term of four years for supervising a criminal enterprise in Russia dedicated to computer hacking, fraud, and extortion. The defendant hacked into the computer system of Financial Services, Inc. (FSI), an internet web hosting and electronic banking processing company located in Glen Rock, New Jersey, and stole 11 passwords used by FSI employees to access the FSI computer network as well as a text file containing approximately 3,500 credit card numbers and associated card holder information for FSI customers. One of the defendant's accomplices then threatened FSI that the hacker group would publicly release this stolen credit card information and hack into and further damage the FSI computer system unless FSI paid $6,000. After a period of negotiation, FSI eventually agreed to pay $5,000. In sentencing the defendant, the federal judge described the scheme as an "unprecedented, wide-ranging, organized criminal enterprise" that "engaged in numerous acts of fraud, extortion, and intentional damage to the property of others, involving the sophisticated manipulation of computer data, financial information, and credit card numbers." The court found that the defendant was responsible for an aggregate loss to his victims of approximately $25 million.

A ramp agent for a major airline participated in a scheme to steal financial documents, including checks and credit cards, from the U.S. mail at Thurgood Marshall Baltimore-Washington International Airport and transfer those financial documents to his co-conspirators for processing. The conspirators used the documents to obtain cash advances and withdrawals from lines of credit. In September 2005, a federal judge sentenced the ramp agent to 14 years in prison and ordered him to pay $7 million in restitution.

thieves use more technologically-advanced means to extract information from computers, including malicious-code programs that secretly log information or give criminals access to it.

The following are among the techniques most frequently used by identity thieves to steal the personal information of their victims.

Common Theft and Dumpster Diving

While often considered a "high tech" crime, data theft often is no more sophisticated than stealing paper documents. Some criminals steal documents containing personal information from mail boxes; indeed, mail theft appears to be a common way that meth users and producers obtain consumer data.[12] Other identity thieves simply take documents thrown into unprotected trash receptacles, a practice known as "dumpster diving."[13] Still others steal information using techniques no more sophisticated than purse snatching.

Progress is being made in reducing the opportunities that identity thieves have to obtain personal information in these ways. The Fair and Accurate Credit Transactions Act of 2003 (FACT Act)[14] requires merchants that accept

Partial display of credit cards, checks, and identifying documents seized in federal investigation of identity theft ring in Maryland, 2005.
Source: U.S. Department of Justice

credit or debit cards to truncate the numbers on receipts that are electronically printed—a measure that is intended, among other things, to reduce the ability of a "dumpster diver" to obtain a victim's credit card number simply by looking through that victim's discarded trash. Merchants had a period of time to comply with that requirement, which now is in full effect.[15]

Employee/Insider Theft

Dishonest insiders can steal sensitive consumer data by removing paper documents from a work site or accessing electronic records. Criminals also may bribe insiders, or become employees themselves to access sensitive data at companies. The failure to disable a terminated employee's access to a computer system or confidential databases contained within the system also could lead to the compromise of sensitive consumer data. Many federal agencies have taken enforcement actions to punish and deter such insider compromise.

In December 2003, the Office of the Comptroller of the Currency (OCC) directed a large financial institution to improve its employee screening policies, procedures, systems, and controls after finding that the institution had inadvertently hired a convicted felon who used his new post to engage in identity theft-related crimes. Deficiencies in the institution's screening practices came to light through the OCC's review of the former employee's activities.

Electronic Intrusions or Hacking

Hackers steal information from public and private institutions, including large corporate databases and residential wireless networks. First, they can intercept data during transmission, such as when a retailer sends payment card information to a card processor. Hackers have developed tools to penetrate firewalls, use automated processes to search for account data or other personal information, export the data, and hide their tracks.[16] Several recent government enforcement actions have targeted this type of data theft.

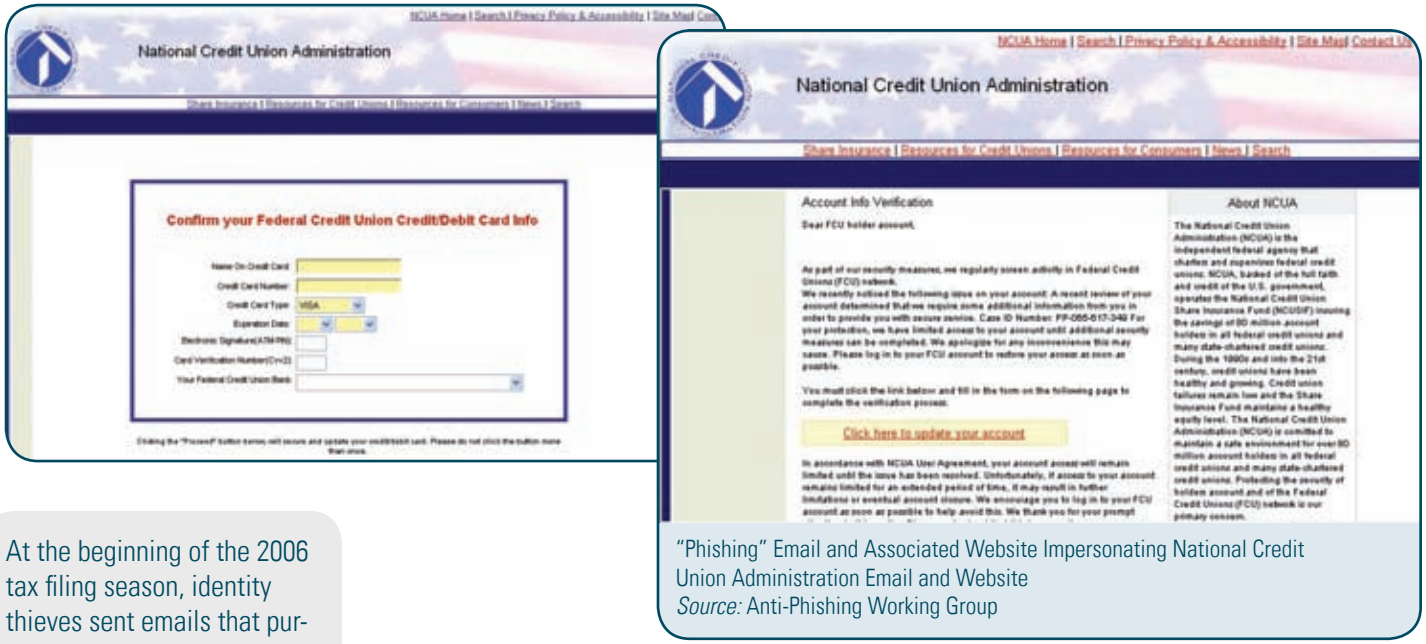
Second, hackers also can gain access to underlying applications—programs used to "communicate" between Internet users and a company's internal databases, such as programs to retrieve product information. One research firm estimates that nearly 75 percent of hacker attacks are targeted at the application, rather than the network.[17] It is often difficult to detect the hacker's application-level activities, because the hacker connects to the website through the same legitimate route any customer would use, and the communication is thus seen as permissible activity.

According to the Secret Service, many major breaches in the credit card system in 2006 originated in the Russian Federation and the Ukraine, and criminals operating in those two countries have been directly involved in some of the largest breaches of U.S. financial systems for the past five years.

In December 2004, a federal district judge in North Carolina sentenced a defendant to 108 months in prison after he pleaded guilty to crimes stemming from his unauthorized access to the nationwide computer system used by the Lowe's Corporation to process credit card transactions. To carry out this scheme, the defendant and at least one other person secretly compromised the wireless network at a Lowe's retail store in Michigan and gained access to Lowe's central computer system. The defendant then installed a computer program designed to capture customer credit card information on the computer system of several Lowe's retail stores. After an FBI investigation of the intrusion, the defendant and a confederate were charged.

Social Engineering: Phishing, Malware/Spyware, and Pretexting

Identity thieves also use trickery to obtain personal information from unwitting sources, including from the victim himself. This type of deception, known as "social engineering," can take a variety of forms.



"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***.

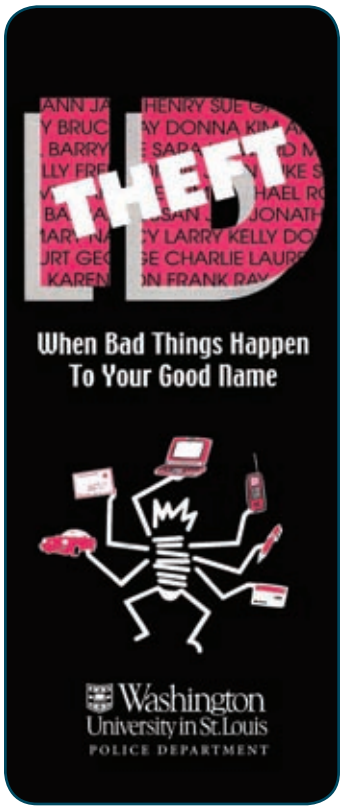
4. EDUCATING CONSUMERS ON PROTECTING THEIR PERSONAL INFORMATION

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

limited, and evaluation of effectiveness is almost nonexistent. Although a great deal of useful information is being disseminated, the extent to which the messages are reaching, engaging, or motivating consumers is unclear.

RECOMMENDATION: INITIATE A MULTI-YEAR PUBLIC AWARENESS CAMPAIGN

Because consumer education is a critical component of any plan to reduce the incidence of identity theft, the Task Force recommends that member agencies, in the third quarter of 2007, initiate a multi-year national public awareness campaign that builds on the FTC's current "AvoID Theft: Deter, Detect, Defend" campaign, developed pursuant to direction in the FACT Act. This campaign should include the following elements:

- **Develop a Broad Awareness Campaign.** By broadening the current FTC campaign into a multi-year awareness campaign, and by engaging the Ad Council or similar entities as partners, important and empowering messages should be disseminated more widely and by more partners. The campaign should include public service announcements on the Internet, radio, and television, and in newspapers and magazines, and should address the issue from a variety of perspectives, from prevention through mitigation and remediation, and reach a variety of audiences.
- **Enlist Outreach Partners.** The agencies conducting the campaign should enlist as outreach partners national organizations either that have been active in helping consumers protect themselves against identity theft, such as the AARP, the Identity Theft Resource Center (ITRC), and the Privacy Rights Clearinghouse (PRC), or that may be well-situated to help in this area, such as the White House Office of Faith-Based and Community Initiatives.
- **Increase Outreach to Traditionally Underserved Communities.** Outreach to underserved communities should include encouraging language translations of existing materials and involving community-based organizations as partners.
- **Establish "Protect Your Identity Days."** The campaign should establish "Protect Your Identity Days" to promote better data security by businesses and individual commitment to security by consumers. These "Protect Your Identity Days" should also build on the popularity of community "shred-ins" by encouraging community and business organizations to shred documents containing personal information.

RECOMMENDATION: DEVELOP AN ONLINE CLEARINGHOUSE" FOR CURRENT EDUCATIONAL RESOURCES

The Task Force recommends that in the third quarter of 2007, the Task Force member agencies develop an online "clearinghouse" for current identity theft educational resources for consumers, businesses, and law enforcement from a variety of sources at ***www.idtheft.gov***. This would make the materials immediately available in one place to any public or private entity willing to launch an education program, and to any citizen interested in accessing the information. Rather than recreate content, entities could link directly to the clearinghouse for timely and accurate information. Educational materials should be added to the website on an ongoing basis.

B. PREVENTION: MAKING IT HARDER TO MISUSE CONSUMER DATA

Keeping valuable consumer data out of the hands of criminals is the first step in reducing the incidence of identity theft. But, because no security is perfect and thieves are resourceful, it is essential to reduce the opportunities for criminals to misuse the data they do manage to steal.

An identity thief who wants to open new accounts in a victim's name must be able to (1) provide identifying information to enable the creditor or other grantor of benefits to access information on which to base an eligibility decision, and (2) convince the creditor or other grantor of benefits that he is, in fact, the person he purports to be. For example, a credit card grantor processing an application for a credit card will use the SSN to access the consumer's credit report to check his creditworthiness, and may rely on photo documents, the SSN, and/or other proof to access other sources of information intended to "verify" the applicant's identity. Thus, the SSN is a critical piece of information for the thief, and its wide availability increases the risk of identity theft.

Identity systems follow a two-fold process: first, determining ("identification") and setting ("enrollment") the identity of an individual at the onset of the relationship; and second, later ensuring that the individual is the same person who was initially enrolled ("authentication"). With the exception of banks, savings associations, credit unions, some broker-dealers, mutual funds, futures commission merchants, and introducing brokers (collectively, "financial institutions"), there is no generally-applicable legal obligation on private sector entities to use any particular means of identification. Financial institutions are required to follow certain verification procedures pursuant to regulations promulgated by the federal bank regulatory agencies, the Department of

Treasury, the SEC, and the CFTC under the USA PATRIOT Act.[67] The regulations require these financial institutions to establish a Customer Identification Program (CIP) specifying identifying information that will be obtained from each customer when accounts are opened (which must include, at a minimum, name, date of birth, address, and an identification number such as an SSN). The CIP requirement is intended to ensure that financial institutions form a reasonable belief that they know the true identity of each customer who opens an account. The government, too, is making efforts to implement new identification mechanisms. For example, REAL ID is a nationwide effort intended to prevent terrorism, reduce fraud, and improve the reliability and accuracy of identification documents that state governments issue.[68] See Volume II, Part G, for a description of recent laws relating to identification documents.

The verification process can fail, however, in a number of ways. First, identity documents may be falsified. Second, checking the identifying information against other verifying sources of information can produce varying results, depending on the accuracy of the initial information presented and the accuracy or quality of the verifying sources. The process also can fail because employees are trained improperly or fail to follow proper procedures. Identity thieves exploit each of these opportunities to circumvent the verification process.[69]

Once an individual's identity has been verified, it must be authenticated each time he wants the access for which he was initially verified, such as access to a bank account. Generally, businesses authenticate an individual by requiring him to present some sort of credential to prove that he is the same individual whose identity was originally verified. A credential is generally one or more of the following:

- Something a person knows—most commonly a password, but also may be a query that requires specific knowledge only the customer is likely to have, such as the exact amount of the customer's monthly mortgage payment.
- Something a person has—most commonly a physical device, such as a Universal Serial Bus (USB) token, a smart card, or a password-generating device.[70]
- Something a person is—most commonly a physical characteristic, such as a fingerprint, iris, face, and hand geometry. This type of authentication is referred to as biometrics.[71]

Some entities use a single form of authentication—most commonly a password—but if it is compromised, there are no other fail-safes in the system. To address this problem, the federal bank regulatory agencies issued guidance promoting stronger customer authentication methods for certain high-risk transactions. Such methods are to include the use of multi-factor authentication, layered security, or other similar controls

reasonably calculated to mitigate the exposure from any transactions that are identified as high-risk. The guidance more broadly provides that banks, savings associations, and credit unions conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing Internet-based financial services.[72] Financial institutions covered by the guidance were advised that the agencies expected them to have completed the risk assessment and implemented risk mitigation activities by year-end 2006.[73] Along with the financial services industry, other industries have begun to implement new authentication procedures using different types of credentials.

SSNs have many advantages and are widely used in our current marketplace to match consumers with their records (including their credit files) and as part of the authentication process. Keeping the authentication process convenient for consumers and credit grantors without making it too easy for criminals to impersonate consumers requires a fine balance. Notwithstanding improvements in certain industries and companies, efforts to facilitate the development of better ways to authenticate consumers without undue burden would help prevent criminals from profiting from their crime.

RECOMMENDATION: HOLD WORKSHOPS ON AUTHENTICATION

Because developing more reliable methods of authenticating the identities of individuals would make it harder for identity thieves to open new accounts or access existing accounts using other individuals' information, the Task Force will hold a workshop or series of workshops, involving academics, industry, and entrepreneurs, focused on developing and promoting improved means of authenticating the identities of individuals. These experts will discuss the existing problem and examine the limitations of current processes of authentication. With that information, the Task Force will probe viable technological and other solutions that will reduce identity fraud, and identify needs for future research. Such workshops have been successful in developing creative and timely responses to consumer protection issues, and the workshops are expected to be useful for both the private and public sectors. For example, the federal government has an interest as a facilitator of the development of new technologies and in implementing technologies that better protect the data it handles in providing benefits and services, and as an employer.

As noted in the Task Force's interim recommendations to the President, the FTC and other Task Force member agencies will host the first such workshop in the second quarter of 2007. The Task Force also recommends that a report be issued or subsequent workshops be held to report on any proposals or best practices identified during the workshop series.

RECOMMENDATION: DEVELOP COMPREHENSIVE RECORD ON PRIVATE SECTOR USE OF SSNs

As noted in Section III A 1, above, the Task Force recommends developing a comprehensive record on the uses of the SSN in the private sector and evaluating their necessity.

C. VICTIM RECOVERY: HELPING CONSUMERS REPAIR THEIR LIVES

Because identity theft can be committed despite the best of precautions, an essential step in the fight against this crime is ensuring that victims have the knowledge, tools, and assistance necessary to minimize the damage and begin the recovery process. Currently, consumers have a number of rights and available resources, but they may not be aware of them.

1. VICTIM ASSISTANCE: OUTREACH AND EDUCATION

Federal and state laws offer victims of identity theft an array of tools to avoid or mitigate the harms they suffer. For example, under the FACT Act, victims can: (1) place alerts on their credit files; (2) request copies of applications and other documents used by the thief; (3) request that the credit reporting agencies block fraudulent trade lines on credit reports; and (4) obtain information on the fraudulent accounts from debt collectors.

In some cases, the recovery process is relatively straightforward. Consumers whose credit card numbers have been used to make unauthorized purchases, for example, typically can get the charges removed without undue burden. In other cases, however, such as those involving new-account fraud, recovery can be an ordeal.

Widely-available guidance advises consumers of steps to take if they have become victims of identity theft, or if their personal information has been breached. For example, the FTC's website, ***www.ftc.gov/idtheft***, contains step-by-step recovery information for victims, as well as for those who may be at risk following a compromise of their data. Many other agencies and organizations link directly to the FTC site and themselves provide education and assistance to victims.

Fair and Accurate Credit Transaction Act (FACT Act) Rights

The Fair and Accurate Credit Transactions Act of 2003 added new sections to the Fair Credit Reporting Act that provide a number of new tools for victims to recover from identity theft. These include the right to place a fraud alert with the credit reporting agencies and receive a free copy of the credit report. An initial alert lasts for 90 days. A victim with an identity theft report documenting actual misuse of the consumer information is entitled to place a 7-year alert on his file. In addition, under the FACT Act, victims can request copies of documents relating to fraudulent transactions, and can obtain information from a debt collector regarding a debt fraudulently incurred in the victim's name. Victims who have a police report also can ask that fraudulent accounts be blocked from their credit report, and can prevent businesses from reporting information that resulted from identity theft to the credit reporting agencies.

Identity theft victims, and consumers who suspect that they may become victims because of lost data, are advised to act quickly to prevent or minimize harm. The steps are straightforward:

- *Contact one of the three major credit reporting agencies to place a fraud alert on their credit file. The agencies are required to transmit this information to the other two companies. Consumers who place this 90-day alert are entitled to a free copy of their credit report. Fraud alerts are most useful when a consumer's SSN is compromised, creating the risk of new account fraud.*
- *Contact any creditors where fraudulent accounts were opened or charges were made to dispute these transactions, and follow up in writing.*
- *Report actual incidents of identity theft to the local police department and obtain a copy of the police report. This document will be essential to exercising other remedies.*
- *Report the identity theft incident to the ID Theft Data Clearinghouse by filing a complaint online at ftc.gov/idtheft, or calling toll free 877 ID THEFT. The complaint will be entered into the Clearinghouse and shared with the law enforcement agencies who use the database to investigate and prosecute identity crimes.*
- *Some states provide additional protections to identity theft victims by allowing them to request a "credit freeze," which prevents consumers' credit reports from being released without their express consent. Because most companies obtain a credit report from a consumer before extending credit, a credit freeze will likely prevent the extension of credit in a consumer's name without the consumer's express permission.*

State governments also provide assistance to victims. State consumer protection agencies, privacy agencies, and state Attorneys General provide victim information and guidance on their websites, and some provide personal assistance as well. A number of states have established hotlines, counseling, and other assistance for victims of identity theft. For example, the Illinois Attorney General's office has implemented an Identity Theft Hotline; each caller is assigned a consumer advocate to assist with the recovery process and to help prevent further victimization.

A number of private sector organizations also provide critical victim assistance. Not-for-profit groups such as the Privacy Rights Clearinghouse (PRC) and the Identity Theft Resource Center (ITRC) offer counseling and assistance for identity theft victims who need help in going through the recovery process. The Identity Theft Assistance Center (ITAC), a victim assistance program established by the financial services industry, has helped approximately 13,000 victims resolve problems with disputed accounts and other fraud related to identity theft since its founding in 2004. Finally, many individual companies have established hotlines, distributed materials, and provided special services for customers whose information has been misused. Indeed, some companies rely on their identity theft services as marketing tools.

Despite this substantial effort by the public and private sectors to educate and assist victims, there is room for improvement. Many victims are not aware, or do not take advantage, of the resources available to them. For example, while the FTC receives roughly 250,000 contacts from victims every year, that number is only a small percentage of all identity theft victims. Moreover, although first responders could be a key resource for identity theft victims, the first responders often are overworked and may not have the information that they need about the steps for victim recovery. It is essential, therefore, that public and private outreach efforts be expanded, better coordinated, and better funded.

RECOMMENDATION: PROVIDE SPECIALIZED TRAINING ABOUT VICTIM RECOVERY TO FIRST RESPONDERS AND OTHERS PROVIDING DIRECT ASSISTANCE TO IDENTITY THEFT VICTIMS

First responders and others who provide direct assistance and support to identity theft victims must be adequately trained. Accordingly, the Task Force recommends the following:

- **Train Local Law Enforcement Officers.** By the third quarter of 2007, federal law enforcement agencies, which could include the U.S. Postal Inspection Service, the FBI, the Secret Service, and the FTC, should conduct training seminars—delivered in person, online, or via video—for local law enforcement officers on available resources and providing assistance for victims.

- **Provide Educational Materials for First Responders That Can Be Readily Used as a Reference Guide for Identity Theft Victims.** During the third quarter of 2007, the FTC and DOJ should develop a reference guide, which should include contact information for resources and information on first steps to recovery, and should make that guide available to law enforcement officers through the online clearinghouse at

www.idtheft.gov. Such guidance would assist first responders in directing victims on their way to recovery.

- **Distribute an Identity Theft Victim Statement of Rights.** Federal law provides substantial assistance to victims of identity theft. From obtaining a police report to blocking fraudulent accounts in a credit report, consumers—as well as law enforcement, private businesses, and other parties involved in the recovery process—need to know what remedies are available. Accordingly, the Task Force recommends that, during the third quarter of 2007, the FTC draft an ID Theft Victim Statement of Rights, a short and simple statement of the basic rights victims possess under current law. This document should then be disseminated to victims through law enforcement, the financial sector, and advocacy groups, and posted at ***www.idtheft.gov***.

- **Develop Nationwide Training for Victim Assistance Counselors.** Crime victims receive assistance through a wide array of federal and state-sponsored programs, as well as nonprofit organizations. Additionally, every United States Attorney's Office in the country has a victim-witness coordinator who is responsible for referring crime victims to the appropriate resources to resolve harms that resulted from the misuse of their information. All of these counselors should be trained to respond to the specific needs of identity theft victims, including assisting them in coping with the financial and emotional impact of identity crime. Therefore, the Task Force recommends that a standardized training curriculum for victim assistance be developed and promoted through a nationwide training campaign, including through DOJ's Office for Victims of Crime (OVC). Already, OVC has begun organizing training workshops, the first of which was held in December 2006. These workshops are intended to train not only victim-witness coordinators from U.S. Attorney's Offices, but also state, tribal, and local victim service providers. The program will help advocates learn how to assist victims in self-advocacy and how and when to intervene in a victim's recovery process. Training topics will include helping victims deal with the economic and emotional ramifications of identity theft, assisting victims with understanding how an identity theft case proceeds through the criminal justice system, and identity theft laws. Additional workshops should be held in 2007.

RECOMMENDATION: DEVELOP AVENUES FOR INDIVIDUALIZED ASSISTANCE TO IDENTITY THEFT VICTIMS

Although many victims are able to resolve their identity theft-related issues without assistance, some individuals would

benefit from individualized counseling. The availability of personalized assistance should be increased through national service organizations, such as those using retired seniors or similar groups, and pro bono activities by lawyers, such as those organized by the American Bar Association (ABA). In offering individualized assistance to identity theft victims, these organizations and programs should use the victim resource guides that are already available through the FTC and DOJ's Office for Victims of Crime. Specifically, the Task Force also recommends the following:

- **Engage the American Bar Association to Develop a Program Focusing on Assisting Identity Theft Victims with Recovery.** The ABA has expertise in coordinating legal representation in specific areas of practice through law firm volunteers. Moreover, law firms have the resources and expertise to staff an effort to assist victims of identity theft. Accordingly, the Task Force recommends that, beginning in 2007, the ABA, with assistance from the Department of Justice, develop a pro bono referral program focusing on assisting identity theft victims with recovery.

2. MAKING IDENTITY THEFT VICTIMS WHOLE

Identity theft inflicts many kinds of harm upon its victims, making it difficult for them to feel that they ever will recover fully. Beyond tangible forms of harm, statistics cannot adequately convey the emotional toll that identity theft often exacts on its victims, who frequently report feelings of violation, anger, anxiety, betrayal of trust, and even self-blame or hopelessness. These feelings may continue, or even increase, as victims work through the credit recovery and criminal justice processes. Embarrassment, cultural factors, or personal or family circumstances (e.g., if the victim has a relationship to the identity thief) may keep the victims from reporting the problem to law enforcement, in turn making them ineligible to take advantage of certain remedies. Often, these reactions are intensified by the ongoing, long-term nature of the crime. Criminals may not stop committing identity theft after having been caught; they simply use information against the same individual in a new way, or they sell the information so that multiple identity thieves can use it. Even when the fraudulent activity ceases, the effects of negative information on the victim's credit report can continue for years.

The many hours victims spend in attempting to recover from the harms they suffer often takes a toll on victims that is not reflected in their monetary losses. One reason that identity theft can be so destructive to its victims is the sheer amount of time and energy often required to recover from the offense, including having to correct credit reports, dispute charges with individual creditors, close and reopen bank accounts, and monitor credit reports for future problems arising from the theft.

"I received delinquent bills for purchases she [the suspect] made. I spent countless hours on calls with creditors in Texas who were reluctant to believe that the accounts that had been opened were fraudulent. I spent days talking to police in Texas in an effort to convince them that I was allowed by Texas law to file a report and have her [the suspect] charged with the theft of my identity.... I had to send more than 50 letters to the creditors to have them remove the more than 60 inquiries that were made by this woman...."

Nicole Robinson
Testimony before House Ways and Means Committee, Subcommittee on Social Security
May 22, 2001

In addition to losing time and money, some identity theft victims suffer the indignity of being mistaken for the criminal who stole their identities, and have been wrongfully arrested.[74] In one case, a victim's driver's license was stolen, and the information from the license was used to open a fraudulent bank account and to write more than $10,000 in bad checks. The victim herself was arrested when local authorities thought she was the criminal. In addition to the resulting feelings of trauma, this type of harm is a particularly difficult one for an identity theft victim to resolve.

RECOMMENDATION: AMEND CRIMINAL RESTITUTION STATUTES TO ENSURE THAT VICTIMS RECOVER FOR THE VALUE OF TIME SPENT IN ATTEMPTING TO REMEDIATE THE HARMS THEY SUFFERED

Restitution to victims from convicted thieves is available for the direct financial costs of identity theft offenses. However, there is no specific provision in the federal restitution statutes for compensation for the time spent by victims recovering from the crime, and court decisions interpreting the statutes suggest that such recovery would be precluded.

As stated in the Task Force's interim recommendations to the President, the Task Force recommends that Congress amend the federal criminal restitution statutes to allow for restitution from a criminal defendant to an identity theft victim, in an amount equal to the value of the victim's time reasonably spent attempting to remediate the intended or actual harm incurred from the identity theft offense. The language of the proposed amendment is in Appendix C. DOJ transmitted the proposed amendment to Congress on October 4, 2006.

RECOMMENDATION: EXPLORE THE DEVELOPMENT OF A NATIONAL PROGRAM ALLOWING IDENTITY THEFT VICTIMS TO OBTAIN AN IDENTIFICATION DOCUMENT FOR AUTHENTICATION PURPOSES

One of the problems faced by identity theft victims is proving that they are who they say they are. Indeed, some identity theft victims have been mistaken for the criminal who stole their identity, and have been arrested based on warrants issued for the thief who stole their personal data. To give identity theft victims a means to authenticate their identities in such a situation, several states have developed identification documents, or "passports," that authenticate identity theft victims. These voluntary mechanisms are designed to prevent the misuse of the victim's name in the

criminal justice system when, for example, an identity thief uses his victim's name when arrested. These documents often use multiple factors for authentication, such as biometric data and a password. The FBI has established a similar system through the National Crime Information Center, allowing identity theft victims to place their name in an "Identity File." This program, too, is limited in scope. Beginning in 2007, the Task Force member agencies should lead an effort to study the feasibility of developing a nationwide system allowing identity theft victims to obtain a document that they can use to avoid being mistaken for the suspect who has misused their identity. The system should build on the programs already used by several states and the FBI.

3. GATHERING BETTER INFORMATION ON THE EFFECTIVENESS OF VICTIM RECOVERY MEASURES

Identity theft victims have been granted many new rights in recent years. Gathering reliable information about the utility of these new rights is critical to evaluating whether they are working well or need to be modified. Additionally, because some states have measures in place to assist identity theft victims that have no federal counterpart, it is important to assess the success of those measures to determine whether they should be adopted more widely. Building a record of victims' experiences in exercising their rights is therefore crucial to ensuring that any strategy to fight identity theft is well-supported.

RECOMMENDATION: ASSESS EFFICACY OF TOOLS AVAILABLE TO VICTIMS

The Task Force recommends the following surveys or assessments:

- **Conduct Assessment of FACT Act Remedies Under FCRA.** The FCRA is among the federal laws that enable victims to restore their good name. The FACT Act amendments to the FCRA provide several new rights and tools for actual or potential identity theft victims, including the availability of credit file fraud alerts; the blocking of fraudulent trade lines on credit reports; the right to have creditors cease furnishing information relating to fraudulent accounts to credit reporting agencies; and the right to obtain business records relating to fraudulent accounts. Many of these rights have been in effect for a short time. Accordingly, the Task Force recommends that the agencies with enforcement authority for these statutory provisions assess their impact and effectiveness through appropriate surveys. Agencies should report on the results in calendar year 2008.

- **Conduct Assessment of State Credit Freeze Laws.** Among the state-enacted remedies without a federal counterpart is one granting consumers the right to obtain a credit freeze. Credit freezes make a consumer's credit report inaccessible when, for example, an identity thief attempts to open an account in the victim's name. State laws differ in several respects, including whether all consumers can obtain a freeze or only identity theft victims; whether credit reporting agencies can charge the consumer for unfreezing a file (which would be necessary when applying for credit); and the time allowed to the credit reporting agencies to unfreeze a file. These provisions are relatively new, and there is no "track record" to show how effective they are, what costs they may impose on consumers and businesses, and what features are most beneficial to consumers. An assessment of how these measures have been implemented and how effective they have been would help policy makers in considering whether a federal credit freeze law would be appropriate. Accordingly, the Task Force recommends that the FTC, with support from the Task Force member agencies, assess the impact and effectiveness of credit freeze laws, and report on the results in the first quarter of 2008.

D. LAW ENFORCEMENT: PROSECUTING AND PUNISHING IDENTITY THIEVES

The two keys to preventing identity theft are (1) preventing access to sensitive consumer information through better data security and increased education, and (2) preventing the misuse of information that may be obtained by would-be identity thieves. Should those mechanisms fail, strong criminal law enforcement is necessary to both punish and deter identity thieves.

In September 2006, the Michigan Attorney General won the conviction of a prison inmate who had orchestrated an elaborate scheme to claim tax refunds owed to low income renters through the state's homestead property tax program. Using thousands of identities, the defendant and his cohorts were detected by alert U.S. Postal carriers who were suspicious of the large number of Treasury checks mailed to certain addresses.

The increased awareness about identity theft in recent years has made it necessary for many law enforcement agencies at all levels of government to devote additional resources to investigating identity theft-related crimes. The principal federal law enforcement agencies that investigate identity theft are the FBI, the United States Secret Service, the United States Postal Inspection Service, SSA OIG, and ICE. Other agencies, as well as other federal Inspectors General, also may become involved in identity theft investigations.

In investigating identity theft, law enforcement agencies use a wide range of techniques, from physical surveillance to financial analysis to computer forensics. Identity theft investigations are labor-intensive, and because no single investigator can possess all of the skill sets needed to handle each of these functions, the investigations often require multiple detectives, analysts, and agents. In addition, when a suspected identity

theft involves large numbers of potential victims, investigative agencies may need additional personnel to handle victim-witness coordination and information issues.

During the last several years, federal and state agencies have aggressively enforced the laws that prohibit the theft of identities. All 50 states and the District of Columbia have some form of legislation that prohibits identity theft, and in all those jurisdictions, except Maine, identity theft can be a felony. See Volume II, Part H, for a description of state criminal law enforcement efforts. In the federal system, a wide range of statutory provisions is used to investigate and prosecute identity theft including, most notably, the aggravated identity theft statute[75] enacted in 2004, which carries a mandatory two-year prison sentence. Since then, DOJ has made increasing use of the aggravated identity theft statute: in Fiscal Year 2006, DOJ charged 507 defendants with aggravated identity theft, up from 226 defendants charged with aggravated identity theft in Fiscal Year 2005. In many of these cases, the courts have imposed substantial sentences. See Volume II, Part I, for a description of sentencing in federal identity theft prosecutions.

The Department of Justice also has initiated many special identity theft initiatives in recent years. The first of these, in May 2002, involved 73 criminal prosecutions by U.S. Attorney's Offices against 135 individuals in 24 federal districts. Since then, identity theft has played an integral part in several initiatives that DOJ and other agencies have directed at online economic crime. For example, "Operation Cyber Sweep," a November 2003 initiative targeting Internet-related economic crime, resulted in the arrest or conviction of more than 125 individuals and the return of indictments against more than 70 people involved in various types of Internet-related fraud and economic crime. See Volume II, Part J, for a description of special enforcement and prosecution initiatives.

In a "Operation Firewall," the Secret Service was responsible for the first-ever takedown of a large illegal online bazaar. Using the website www.shadowcrew.com, the Shadowcrew organization had thousands of members engaged in the online trafficking of stolen identity information and documents, such as drivers' licenses, passports, and Social Security cards, as well as stolen credit card, debit card, and bank account numbers. The Shadowcrew members trafficked in at least 1.7 million stolen credit card numbers and caused total losses in excess of $4 million. The Secret Service successfully shut down the website following a year-long undercover investigation, which resulted in the arrests of 21 individuals in the United States on criminal charges in October 2004. Additionally, law enforcement officers in six foreign countries arrested or searched eight individuals.

1. COORDINATION AND INTELLIGENCE/INFORMATION SHARING

Federal law enforcement agencies have recognized the importance of coordination among agencies and of information sharing between law enforcement and the private sector. Coordination has been challenging, however, for several reasons: identity theft data currently reside in numerous databases; there is no standard reporting form for all identity theft complaints; and many law enforcement agencies have limited resources. Given these challenges, law enforcement has responded to the need for greater cooperation by, among other things, forming interagency task forces and developing formal intelligence-sharing mechanisms. Law enforcement also has worked to develop methods of facilitating the timely receipt and analysis of identity theft complaint data and other intelligence.

a. Sources of Identity Theft Information

Currently, federal law enforcement has a number of sources of information about identity theft. The primary source of direct consumer complaint data is the FTC, which, through its Identity Theft Clearinghouse, makes available to law enforcement through a secure website the complaints it receives. Internet-related identity theft complaints also are received by the Internet Crime Complaint Center (IC3), a joint venture of the FBI and National White Collar Crime Center. The IC3 develops case leads from the complaints it receives and sends them to law enforcement throughout the country. Additionally, a special component of the FBI that works closely with the IC3 is the Cyber Initiative and Resource Fusion Unit (CIRFU). The CIRFU, based in Pittsburgh, facilitates the operation of the National Cyber Forensic Training Alliance (NCFTA), a public/private alliance and fusion center, by maximizing intelligence development and analytical resources from law enforcement and critical industry partners. The U.S. Postal Inspection Service also hosts its Financial Crimes Database, a web-based national database available to U.S. Postal Service inspectors for use in analyzing mail theft and identity theft complaints received from various sources. These are but a few of the sources of identity theft data for law enforcement. See Volume II, Part K, for a description of how law enforcement obtains and analyzes identity theft data.

Private sector entities—including the financial services industry and credit reporting agencies—also are important sources of identity theft information for law enforcement agencies. They often are best positioned to identify early anomalies in various components of the e-commerce environment in which their businesses interact, which may represent the earliest indicators of an identity theft scenario. For this reason and others, federal law enforcement has undertaken numerous public- and private-sector collaborations in recent years to improve information sharing. For example, corporations have placed analysts and investigators with IC3 in support of initiatives and investigations. In addition, ITAC, the cooperative initiative of the financial services industry, shares information with law enforcement and the FTC to help catch and convict the criminals responsible for identity theft. See Volume II, Part K, for a description of other private sector sources of identity theft data. Such alliances enable critical industry experts and law enforcement agencies to work together to more expeditiously receive and process information and intelligence vital both to early identification of identity theft schemes and rapid development of aggressive investigations and mitigation strategies, such as public service advisories. At the same time, however, law enforcement agencies report that they have encountered obstacles in obtaining support and assistance from key private-sector stakeholders in some cases, absent legal process, such as subpoenas, to obtain information.

One barrier to more complete coordination is that identity theft information resides in multiple databases, even within individual law enforcement agencies. A single instance of identity theft may result in information being posted at federal, state, and local law enforcement agencies, credit reporting agencies, credit issuers, financial institutions, telecommunications companies, and regulatory agencies. This, in turn, leads to the inefficient "stove-piping" of relevant data and intelligence. Additionally, in many cases, agencies do not or cannot share information with other agencies, making it difficult to determine whether an identity theft complaint is related to a single incident or a series of incidents. This problem may be even more pronounced at the state and local levels.

b. Format for Sharing Information and Intelligence

A related issue is the inability of the primary law enforcement agencies to communicate electronically using a standard format, which greatly impedes the sharing of criminal law enforcement information. When data collection systems use different formats to describe the same event or fact, at least one of the systems must be reprogrammed to fit the other program's terms. Where several hundred variables are involved, the programming resources required to connect the two databases can be an insurmountable barrier to data exchange.

To address that concern, several law enforcement organizations, including the International Association of Chiefs of Police's (IACP) Private Sector Liaison Committee and the Major Cities' Chiefs (MCC), have recommended developing a standard electronic identity theft police report form. Reports that use a standard format could be shared among law enforcement agencies and stored in a national repository for investigatory purposes.

c. Mechanisms for Sharing Information

Law enforcement uses a variety of mechanisms to facilitate information sharing and intelligence analysis in identity-theft investigations. See Volume II, Part L, for a description of federal law enforcement outreach efforts. As just one example, the Regional Information Sharing Systems (RISS) Program is a long-standing, federally-funded program to support regional law enforcement efforts to combat identity theft and other crimes. Within that program, law enforcement has established intelligence-sharing systems. These include, for example, the Regional Identity Theft Network (RITNET), created to provide Internet-accessible identity theft information for federal, state, and local law enforcement agencies within the Eastern District of Pennsylvania. RITNET is designed to include data from the FTC, law enforcement agencies, and the banking industry, and allow investigators to connect crimes committed in various jurisdictions

and link investigators. It also will collect information on all reported frauds, regardless of size, thereby eliminating the advantage identity thieves have in keeping theft amounts low.

Multi-agency working groups and task forces are another successful investigative approach, allowing different agencies to marshal resources, share intelligence, and coordinate activities. Federal authorities lead or co-lead over 90 task forces and working groups devoted (in whole or in part) to identity theft. See Volume II, Part M, for a description of interagency working groups and task forces.

Despite these efforts, coordination among agencies can be improved. Better coordination would help law enforcement officers "connect the dots" in investigations and pool limited resources.

RECOMMENDATION: ESTABLISH A NATIONAL IDENTITY THEFT LAW ENFORCEMENT CENTER

The Task Force recommends that the federal government establish, as resources permit, an interagency National Identity Theft Law Enforcement Center to better consolidate, analyze, and share identity theft information among law enforcement agencies, regulatory agencies, and the private sector. This effort should be led by the Department of Justice and include representatives of federal law enforcement agencies, including the FBI, the Secret Service, the U.S. Postal Inspection Service, the SSA OIG, and the FTC. Leveraging existing resources, increased emphasis should be placed on the analysis of identity theft complaint data and other information and intelligence related to identity theft from public and private sources, including from identity theft investigations. This information should be made available to appropriate law enforcement at all levels to aid in the investigation, prosecution, and prevention of identity theft crimes, including to target organized groups of identity thieves and the most serious offenders operating both in the United States and abroad. Effective mechanisms that enable law enforcement officers from around the country to share, access, and search appropriate law enforcement information around-the-clock, including through remote access, should also be developed. As an example, intelligence from documents seized during investigations could help facilitate the ability of agents and officers to "connect the dots" between various investigations around the country.

In a case prosecuted by the United States Attorney's Office for the Eastern District of Pennsylvania, a gang purchased 180 properties using false or stolen names. The thieves colluded to procure inflated appraisals for the properties, obtained financing, and drained the excess profits for their own benefit, resulting in harm to the identity theft victims and to the neighborhood when most of the properties went into foreclosure.

RECOMMENDATION: DEVELOP AND PROMOTE THE ACCEPTANCE OF A UNIVERSAL IDENTITY THEFT REPORT FORM

The Task Force recommended in its interim recommendations that the federal government, led by the FTC, develop and promote a universal police report like that recommended by the IACP and MCC—a standard document that an identity theft victim could complete, print, and take to any local law enforcement agency for verification and incorporation into the police department's report system. This would make it easier for victims to obtain these reports, facilitate entry of the information into a central database that could be used by law enforcement to analyze patterns and trends, and initiate more investigations of identity theft.

Criminal law enforcers, the FTC, and representatives of financial institutions, the consumer data industry, and consumer advocacy groups have worked together to develop a standard form that meets this need and captures essential information. The resulting Identity Theft Complaint ("Complaint") form was made available in October 2006 via the FTC's Identity Theft website, ***www.ftc.gov/idtheft***. Consumers can print copies of their completed Complaint and take it to their police station, where it can be used as the basis for a police report. The Complaint provides much greater specificity about the details of the crime than would a typical police report, so consumers will be able to submit it to credit reporting agencies and creditors to assist in resolving their identity theft-related problems. Further, the information they enter into the Complaint will be collected in the FTC's Identity Theft Data Clearinghouse, thus enriching this source of consumer complaints for law enforcement. This system also relieves the burden on local law enforcement because consumers are completing the detailed Complaint before filing their police report.

RECOMMENDATION: ENHANCE INFORMATION SHARING BETWEEN LAW ENFORCEMENT AND THE PRIVATE SECTOR

Because the private sector in general, and financial institutions in particular, are an important source of identity theft-related information for law enforcement, the Task Force recommends the following steps to enhance information sharing between law enforcement and the private sector:

- **Enhance Ability of Law Enforcement to Receive Information From Financial Institutions.** Section 609(e) of the Fair Credit Reporting Act enables identity theft victims to receive identity theft-related documents and to designate law enforcement agencies to receive the documents on their behalf. Despite that fact, law enforcement agencies have sometimes encountered difficulties in obtaining such information without a subpoena. By the second quarter of 2007, DOJ should initiate discussions with the financial sector to ensure greater compliance with this law, and should include other law enforcement agencies in these discussions. DOJ, on an ongoing basis, should compile any recommendations that may result from those discussions and, where appropriate, relay those recommendations to the appropriate private or public sector entity for action.

- **Initiate Discussions With the Financial Services Industry on Countermeasures to Identity Thieves.** Federal law enforcement agencies, led by the U.S. Postal Inspection Service, should continue discussions with the financial services industry as early as the second quarter of 2007 to develop more effective fraud prevention measures to deter identity thieves who acquire data through mail theft. Discussions should include use of the Postal Inspection Service's current Financial Industry Mail Security Initiative. The Postal Inspection Service, on an ongoing basis, should compile any recommendations that may result from those discussions and, where appropriate, relay those recommendations to the appropriate private or public sector entity for action.

- **Initiate Discussions With Credit Reporting Agencies On Preventing Identity Theft.** By the second quarter of 2007, DOJ should initiate discussions with the credit reporting agencies on possible measures that would make it more difficult for identity thieves to obtain credit based on access to a victim's credit report. The discussions should include other law enforcement agencies, including the FTC. DOJ, on an ongoing basis, should compile any recommendations that may result from the discussions and, where appropriate, relay the recommendations to the appropriate private or public sector entity for action.

2. COORDINATION WITH FOREIGN LAW ENFORCEMENT

Federal enforcement agencies have found that a significant portion of the identity theft committed in the United States originates in other countries. Therefore, coordination and cooperation with foreign law enforcement is essential. A positive step by the United States in ensuring

such coordination was the ratification of the Convention on Cybercrime (2001). The Cybercrime Convention is the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks, including offenses that relate to the stealing of personal information and the exploitation of that information to commit fraud. The Cybercrime Convention requires parties to establish laws against these offenses, to ensure that domestic laws give law enforcement officials the necessary legal authority to gather electronic evidence, and to provide international cooperation to other parties in the fight against computer-related crime. The United States participated in the drafting of the Convention and, in November 2001, was an early signatory.

Because of the international nature of many forms of identity theft, providing assistance to, and receiving assistance from, foreign law enforcement on identity theft is critical for U.S. enforcement agencies. Under current law, the United States generally is able to provide such assistance, which fulfills our obligations under various treaties and enhances our ability to obtain reciprocal assistance from foreign agencies. Indeed, there are numerous examples of collaborations between U.S. and foreign law enforcement in identity theft investigations.

Nevertheless, law enforcement faces several impediments in their ability to coordinate efforts with foreign counterparts. First, even though federal law enforcement agencies have successfully identified numerous foreign suspects trafficking in stolen consumer information, their ability to arrest and prosecute these criminals is very limited. Many countries do not have laws directly addressing identity theft, or have general fraud laws that do not parallel those in the United States. Thus, investigators in the United States may be able to prove violations of American identity theft statutes, yet be unable to show violations of the foreign country's law. This can impact cooperation on extradition or collection of evidence necessary to prosecute offenders in the United States. Additionally, some foreign governments are unwilling to cooperate fully with American law enforcement representatives, or may cooperate but fail to aggressively prosecute offenders or seize criminal assets.

Second, certain statutes governing foreign requests for electronic and other evidence—specifically, 18 U.S.C. § 2703 and 28 U.S.C. § 1782—fail to make clear whether, how, and in which court certain requests can be fulfilled. This jurisdictional uncertainty has impeded the ability of American law enforcement officers to assist their counterparts in other countries who are conducting identity theft investigations.

The FBI Legal Attache in Bucharest recently contributed to the development and launch of **www.efrauda.ro**, a Romanian government website for the collection of fraud complaints based on the IC3 model. The IC3 also provided this Legal Attache with complaints received by U.S. victims who were targets of a Romanian Internet crime ring. The complaint forms provided to Romanian authorities via the Legal Attache assisted the Romanian police and Ministry of Justice with the prosecution of Romanian subjects.

RECOMMENDATION: ENCOURAGE OTHER COUNTRIES TO ENACT SUITABLE DOMESTIC LEGISLATION CRIMINALIZING IDENTITY THEFT

The Department of Justice, after consulting with the Department of State, should formally encourage other countries to enact suitable domestic legislation criminalizing identity theft. A number of countries already have adopted, or are considering adopting, criminal identity-theft offenses. In addition, since 2005, the United Nations Crime Commission (UNCC) has convened an international Expert Group to examine the worldwide problem of fraud and identity theft. That Expert Group is drafting a report to the UNCC (for presentation in 2007) that is expected to describe the major trends in fraud and identity theft in numerous countries and to offer recommendations on best practices by governments and the private sector to combat fraud and identity theft. DOJ should provide input to the Expert Group concerning the need for the criminalization of identity theft worldwide.

RECOMMENDATION: FACILITATE INVESTIGATION AND PROSECUTION OF INTERNATIONAL IDENTITY THEFT BY ENCOURAGING OTHER NATIONS TO ACCEDE TO THE CONVENTION ON CYBERCRIME, OR TO ENSURE THAT THEIR LAWS AND PROCEDURES ARE AT LEAST AS COMPREHENSIVE

Global acceptance of the Convention on Cybercrime will help to assure that all countries have the legal authority to collect electronic evidence and the ability to cooperate in trans-border identity theft investigations that involve electronic data. The U.S. government should continue its efforts to promote universal accession to the Convention and assist other countries in bringing their laws into compliance with the Convention's standards. The Department of State, in close coordination with the Department of Justice and Department of Homeland Security, should lead this effort through appropriate bilateral and multilateral outreach mechanisms. Other agencies, including the Department of Commerce and the FTC, should participate in these outreach efforts as appropriate. This outreach effort began years ago in a number of international settings, and should continue until broad international acceptance of the Convention on Cybercrime is achieved.

RECOMMENDATION: IDENTIFY COUNTRIES THAT HAVE BECOME SAFE HAVENS FOR PERPETRATORS OF IDENTITY THEFT AND TARGET THEM FOR DIPLOMATIC AND ENFORCEMENT INITIATIVES FORMULATED TO CHANGE THEIR PRACTICES.

Safe havens for perpetrators of identity theft and individuals who aid and abet such illegal activities should not exist. However, the inaction of law enforcement agencies in some countries has turned those countries into breeding grounds for sophisticated criminal networks devoted to identity theft. Countries that tolerate the existence of such criminal networks encourage their growth and embolden perpetrators to expand their operations. In 2007, the U.S. law enforcement community, with input from the international law enforcement community, should identify the countries that are safe havens for identity thieves. Once identified, the U.S. government should use appropriate diplomatic measures and any suitable enforcement mechanisms to encourage those countries to change their practices.

RECOMMENDATION: ENHANCE THE U.S. GOVERNMENT'S ABILITY TO RESPOND TO APPROPRIATE FOREIGN REQUESTS FOR EVIDENCE IN CRIMINAL CASES INVOLVING IDENTITY THEFT

The Task Force recommends that Congress clarify which courts can respond to appropriate foreign requests for electronic and other evidence in criminal investigations, so that the United States can better provide prompt assistance to foreign law enforcement in identity theft cases. This clarification can be accomplished by amending 18 U.S.C. § 2703 and making accompanying amendments to 18 U.S.C. §§ 2711 and 3127, and by enacting a new statute, 18 U.S.C. § 3512, which would supplement the foreign assistance authority of 28 U.S.C. § 1782. Proposed language for these legislative changes is available in Appendix D (text of amendments to 18 U.S.C. §§ 2703, 2711, and 3127, and text of new language for 18 U.S.C. § 3512).

RECOMMENDATION: ASSIST, TRAIN, AND SUPPORT FOREIGN LAW ENFORCEMENT

Because the investigation of major identity theft rings increasingly will require foreign cooperation, federal law enforcement agencies, led by DOJ, FBI, Secret Service, USPIS, and ICE, should assist, train, and support foreign law enforcement through the use of Internet intelligence-collection entities, including IC3 and CIRFU, and continue to make it a priority to work with other countries in joint investigations targeting identity theft. This work should begin in the third quarter of 2007.

3. PROSECUTION APPROACHES AND INITIATIVES

As part of its effort to prosecute identity theft aggressively, DOJ, since 2002, has conducted a number of enforcement initiatives that have focused, in whole or in part, on identity theft. In addition to broader enforcement initiatives led by DOJ, various individual U.S. Attorney's Offices have undertaken their own identity theft efforts. For example, the U.S. Attorney's Office in the District of Oregon has an identity theft "fast track" program that requires eligible defendants to plead guilty to aggravated identity theft and agree, without litigation, to a 24-month minimum mandatory sentence. Under this program, it is contemplated that defendants will plead guilty and be sentenced on the same day, without the need for a pre-sentence report to be completed prior to the guilty plea, and waive all appellate and post-conviction remedies. In exchange for their pleas of guilty, defendants are not charged with the predicate offense, such as bank fraud or mail theft, which would otherwise result in a consecutive sentence under the United States Sentencing Guidelines. In addition, two U.S. Attorney's Offices have collaborated on a special initiative to combat passport fraud, known as Operation Checkmate. See Volume II, Part J.

Notwithstanding these efforts, challenges remain for federal law enforcement. Because of limited resources and a shortage of prosecutors, many U.S. Attorney's Offices have monetary thresholds—i.e., requirements that a certain amount of monetary loss must have been suffered by the victims—before the U.S. Attorney's Office will open an identity theft case. When a U.S. Attorney's Office declines to open a case based on a monetary threshold, investigative agents cannot obtain additional information through grand jury subpoenas that could help to uncover more substantial monetary losses to the victims.

RECOMMENDATION: INCREASE PROSECUTIONS OF IDENTITY THEFT

The Task Force recommends that, to further increase the number of prosecutions of identity thieves, the following steps should be taken:

- **Designate An Identity Theft Coordinator for Each United States Attorney's Office To Design a Specific Identity Theft Program for Each District.** DOJ should direct that each U.S. Attorney's Office, by June 2007, designate one Assistant U.S. Attorney who should serve as a point of contact and source of expertise within that office for other prosecutors and agents. That Assistant U.S. Attorney also should assist each U.S. Attorney in making a district-specific determination about the areas on which to focus to best address the problem of identity theft. For example, in some southwest border districts, identity theft may be best addressed by stepping up efforts to prosecute immigration fraud. In other districts, identity theft may be best addressed by increasing prosecutions of bank fraud schemes or by making an effort to add identity theft violations to the charges that are brought against those who commit wire/mail/bank fraud schemes through the misappropriation of identities.

- **Evaluate Monetary Thresholds for Prosecution.** By June 2007, the investigative agencies and U.S. Attorney's Offices should re-evaluate current monetary thresholds for initiating identity theft cases and, specifically, should consider whether monetary thresholds for accepting such cases for prosecution should be lowered in light of the fact that investigations often reveal additional loss and additional victims, that monetary loss may not always adequately reflect the harm suffered, and that the aggravated identity theft statute makes it possible for the government to obtain significant sentences even in cases where precisely calculating the monetary loss is difficult or impossible.

- **Encourage State Prosecution of Identity Theft.** DOJ should explore ways to increase resources and training for local investigators and prosecutors handling identity theft cases. Moreover, each U.S. Attorney, by June 2007, should engage in discussions with state and local prosecutors in his or her district to encourage those prosecutors to accept cases that do not meet appropriately-set thresholds for federal prosecution, with the understanding that these cases need not always be brought as identity theft cases.

- **Create Working Groups and Task Forces.** By the end of 2007, U.S. Attorneys and investigative agencies should create or make increased use of interagency working groups and task forces devoted to identity theft. Where funds for a task force are unavailable, consideration should be given to forming working groups with non-dedicated personnel.

RECOMMENDATION: CONDUCT TARGETED ENFORCEMENT INITIATIVES

Law enforcement agencies should continue to conduct enforcement initiatives that focus exclusively or primarily on identity theft. The initiatives should pursue the following:

- **Unfair or Deceptive Means to Make SSNs Available for Sale.** Beginning immediately, law enforcement should more aggressively target the community of businesses on the Internet that sell individuals' SSNs or other sensitive information to anyone who provides them with the individual's name and other limited information. The SSA OIG and other agencies also should continue or initiate investigations of entities that use unlawful means to make SSNs and other sensitive personal information available for sale.
- **Identity Theft Related to the Health Care System.** HHS should continue to investigate identity theft related to Medicare fraud. As part of this effort, HHS should begin to work with state authorities immediately to provide for stronger state licensure and certification of providers, practitioners, and suppliers. Schemes to defraud Medicare may involve the theft of beneficiaries' and providers' identities and identification numbers, the opening of bank accounts in individuals' names, and the submission of fraudulent Medicare claims. Medicare payment is linked to state licensure and certification of providers, practitioners, and suppliers as business entities. Lack of state licensure and certification laws and/or laws that do not require identification and location information of owners and officers of providers, practitioners and suppliers, can hamper the ability of HHS to stop identity theft related to fraudulent billing of the Medicare program.
- **Identity Theft By Illegal Aliens.** Law enforcement agencies, particularly the Department of Homeland Security, should conduct targeted enforcement initiatives directed at illegal aliens who use stolen identities to enter or stay in the United States.

RECOMMENDATION: REVIEW CIVIL MONETARY PENALTY PROGRAMS

By the fourth quarter of 2007, federal agencies, including the SEC, the federal bank regulatory agencies, and the Department of Treasury, should review their civil monetary penalty programs to assess whether they adequately address identity theft. If they do not, analysis should be done as to what, if any, remedies, including legislation, would be appropriate, and any such legislation should be proposed by the first quarter of 2008. If a federal agency does not have a civil monetary penalty program, the establishment of such a program with respect to identity theft should be considered.

4. STATUTES CRIMINALIZING IDENTITY-THEFT RELATED OFFENSES: THE GAPS

Federal law enforcement has successfully investigated and prosecuted identity theft under a variety of criminal statutes. Effective prosecution can be hindered in some cases, however, as a result of certain gaps in those statutes. At the same time, a gap in one aspect of the U.S. Sentencing Guidelines has precluded some courts from enhancing the sentences for some identity thieves whose conduct affected multiple victims. See Volume II, Part N, for an additional description of federal criminal statutes used to prosecute identity theft.

a. The Identity Theft Statutes

The two federal statutes that directly criminalize identity theft are the identity theft statute (18 U.S.C. § 1028(a)(7)) and the aggravated identity theft statute (18 U.S.C. § 1028A(a)). The identity theft statute generally prohibits the possession or use of a means of identification of a person in connection with any unlawful activity that either constitutes a violation of federal law or that constitutes a felony under state or local law.[76] Similarly, the aggravated identity theft statute generally prohibits the possession or use of a means of identification of another person during the commission of, or in relation to, any of several enumerated federal felonies, and provides for enhanced penalties in those situations.

There are two gaps in these statutes, however. First, because both statutes are limited to the illegal use of a means of identification of "a person," it is unclear whether the government can prosecute an identity thief who misuses the means of identification of a corporation or organization, such as the name, logo, trademark, or employer identification number of a legitimate business. This gap means that federal prosecutors cannot use those statutes to charge identity thieves who, for example, create and use

counterfeit documents or checks in the name of a corporation, or who engage in phishing schemes that use an organization's name. Second, the enumerated felonies in the aggravated identity theft statute do not include certain crimes that recur in identity theft and fraud cases, such as mail theft, uttering counterfeit securities, tax fraud, and conspiracy to commit certain offenses.

b. Computer-Related Identity Theft Statutes

Two of the federal statutes that apply to computer-related identity theft have similar limitations that preclude their use in certain important circumstances. First, 18 U.S.C. § 1030(a)(2) criminalizes the theft of information from a computer. However, federal courts only have jurisdiction if the thief uses an interstate communication to access the computer (unless the computer belongs to the federal government or a financial institution). As a result, the theft of personal information either by a corporate insider using the company's internal local networks, or by a thief intruding into a wireless network, generally would not involve an interstate communication and could not be prosecuted under this statute. In one case in North Carolina, for instance, an individual broke into a hospital computer's wireless network and thereby obtained patient information. State investigators and the victim asked the United States Attorney's Office to support the investigation and charge the criminal. Because the communications occurred wholly intrastate, however, no federal law criminalized the conduct.

A second limitation is found in 18 U.S.C. § 1030(a)(5), which criminalizes actions that cause "damage" to computers, i.e., that impair the "integrity or availability" of data or computer systems.[77] Absent special circumstances, the loss caused by the criminal conduct must exceed $5,000 to constitute a federal crime. Many identity thieves obtain personal information by installing malicious spyware, such as keyloggers, on many individuals' computers. Whether the programs succeed in obtaining the unsuspecting computer owner's financial data, these sorts of programs harm the "integrity" of the computer and data. Nevertheless, it is often difficult or impossible to measure the loss this damage causes to each computer owner, or to prove that the total value of these many small losses exceeds $5,000.

c. Cyber-Extortion Statute

Another federal criminal statute that may apply in some computer-related identity theft cases is the "cyber-extortion" provision of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(7). This provision, which prohibits the transmission of a threat "to cause damage to a protected computer,"[78] is used to prosecute criminals who threaten to delete data,

crash computers, or knock computers off of the Internet using a denial of service attack. Some cyber-criminals extort companies, however, without explicitly threatening to cause damage to computers. Instead, they steal confidential data and then threaten to make it public if their demands are not met. In other cases, the criminal causes the damage first—such as by accessing a corporate computer without authority and encrypting critical data—and then threatens not to correct the problem unless the victim pays. Thus, the requirement in section 1030(a)(7) that the defendant must explicitly "threaten to cause damage" can preclude successful prosecutions for cyber-extortion under this statute under certain circumstances.

d. Sentencing Guidelines Governing Identity Theft

In recent years, the courts have created some uncertainty about the applicability of the "multiple victim enhancement" provision of the U.S. Sentencing Guidelines in identity theft cases. This provision allows courts to increase the sentence for an identity thief who victimizes more than one person. It is unclear, however, whether this sentencing enhancement applies when the victims have not sustained actual monetary loss. For example, in some jurisdictions, when a financial institution indemnifies 20 victims of unauthorized charges to their credit cards, the courts consider the financial institution to be the only victim. In such cases, the identity thief therefore may not be penalized for having engaged in conduct that harmed 20 people, simply because those 20 people were later indemnified. This interpretation of the Sentencing Guidelines conflicts with a primary purpose of the Identity Theft and Assumption Deterrence Act of 1998: to vindicate the interests of individual identity theft victims.[79]

RECOMMENDATION: CLOSE THE GAPS IN FEDERAL CRIMINAL STATUTES USED TO PROSECUTE IDENTITY-THEFT RELATED OFFENSES TO ENSURE INCREASED FEDERAL PROSECUTION OF THESE CRIMES

The Task Force recommends that Congress take the following legislative actions:

- **Amend the Identity Theft and Aggravated Identity Theft Statutes to Ensure That Identity Thieves Who Misappropriate Information Belonging to Corporations and Organizations Can Be Prosecuted.** Proposed amendments to 18 U.S.C. §§ 1028 and 1028A are available in Appendix E.

- **Add Several New Crimes to the List of Predicate Offenses for Aggravated Identity Theft Offenses.** The aggravated identity theft statute, 18 U.S.C. § 1028A, should include other federal offenses that recur in various identity-theft and fraud cases—mail theft, uttering counterfeit securities, and tax fraud, as well as conspiracy to commit specified felonies already listed in 18 U.S.C. § 1028A—in the statutory list of predicate offenses for that offense. Proposed additions to 18 U.S.C. § 1028A are contained in Appendix E.

- **Amend the Statute That Criminalizes the Theft of Electronic Data By Eliminating the Current Requirement That the Information Must Have Been Stolen Through Interstate Communications.** The proposed amendment to 18 U.S.C. § 1030(a)(2) is available in Appendix F.

- **Penalize Malicious Spyware and Keyloggers.** The statutory provisions in 18 U.S.C. § 1030(a)(5) should be amended to penalize appropriately the use of malicious spyware and keyloggers, by eliminating the current requirement that the defendant's action must cause "damage" to computers and that the loss caused by the conduct must exceed $5,000. Proposed amendments to 18 U.S.C. §§ 1030(a)(5), (c), and (g), and the accompanying amendment to 18 U.S.C. § 2332b(g), are included in Appendix G.

- **Amend the Cyber-Extortion Statute to Cover Additional, Alternate Types of Cyber-Extortion.** The proposed amendment to 18 U.S.C. § 1030(a)(7) is available in Appendix H.

RECOMMENDATION: ENSURE THAT AN IDENTITY THIEF'S SENTENCE CAN BE ENHANCED WHEN THE CRIMINAL CONDUCT AFFECTS MORE THAN ONE VICTIM

The Sentencing Commission should amend the definition of "victim," as that term is used under United States Sentencing Guideline section 2B1.1, to state clearly that a victim need not have sustained an actual monetary loss. This amendment will ensure that courts can enhance the sentences imposed on identity thieves who cause harm to multiple victims, even when that harm does not result in any monetary loss to the victims. The proposed amendment to United States Sentencing Guideline section 2B1.1 is available in Appendix I.

5. TRAINING OF LAW ENFORCEMENT OFFICERS AND PROSECUTORS

Training can be the key to effective investigations and prosecutions, and much has been done in recent years to ensure that investigators and prosecutors have been trained on topics relating to identity theft. In addition to ongoing training by U.S. Attorney's Offices, for example, several federal law enforcement agencies—including DOJ, the Postal Inspection Service, the Secret Service, the FTC, and the FBI—along with the American Association of Motor Vehicle Administrators (AAMVA) have sponsored jointly over 20 regional, one-day training seminars on identity fraud for state and local law enforcement agencies across the country. See Volume II, Part O, for a description of training by and for investigators and prosecutors.

Nonetheless, the amount, focus, and coordination of law enforcement training should be expanded. Identity theft investigations and prosecutions involve particular challenges—including the need to coordinate with foreign authorities, some difficulties with the application of the Sentencing Guidelines, and the challenges that arise from the inevitable gap in time between the commission of the identity theft and the reporting of the identity theft—that warrant more specialized training at all levels of law enforcement.

RECOMMENDATION: ENHANCE TRAINING FOR LAW ENFORCEMENT OFFICERS AND PROSECUTORS

- **Develop Course at National Advocacy Center (NAC) Focused Solely on Investigation and Prosecution of Identity Theft**. By the third quarter of 2007, DOJ's Office of Legal Education should complete the development of a course specifically focused on identity theft for prosecutors. The identity theft course should include, among other things: a review of the scope of the problem; a review of applicable statutes, forfeiture and sentencing guideline applications; an outline of investigative and case presentation techniques; training on addressing the unique needs of identity theft victims; and a review of programs for better utilizing collective resources (working groups, task forces, and any "model programs"— fast track programs, etc.).
- **Increase Number of Regional Identity Theft Seminars.** In 2006, the federal agencies and the AAMVA held a number of regional identity theft seminars for state and local law enforcement officers. In 2007, the number of seminars should be increased. Additionally, the participating entities should coordinate with the Task Force to provide the most complete, targeted, and up-to-date training materials.

- **Increase Resources for Law Enforcement Available on the Internet.** The identity theft clearinghouse site, ***www.idtheft.gov***, should be used as the portal for law enforcement agencies to gain access to additional educational materials on investigating identity theft and responding to victims.

- **Review Curricula to Enhance Basic and Advanced Training on Identity Theft.** By the fourth quarter of 2007, federal investigative agencies should review their own training curricula, and curricula of the Federal Law Enforcement Training Center, to ensure that they are providing the most useful training on identity theft.

6. MEASURING SUCCESS OF LAW ENFORCEMENT EFFORTS

One shortcoming in the federal government's ability to understand and respond effectively to identity theft is the lack of comprehensive statistical data about the success of law enforcement efforts to combat identity theft. Specifically, there are few benchmarks that measure the activities of the various components of the criminal justice system in their response to identity thefts occurring within their jurisdictions, little data on state and local enforcement, and little information on how identity theft incidents are being processed in state courts.

Addressing these questions requires benchmarks and periodic data collection. The Bureau of Justice Statistics (BJS) has platforms in place, as well as the tools to create new platforms, to obtain information about identity theft from victims and the response to identity theft from law enforcement agencies, state and federal prosecutors, and courts.

RECOMMENDATION: ENHANCE THE GATHERING OF STATISTICAL DATA MEASURING THE CRIMINAL JUSTICE SYSTEM'S RESPONSE TO IDENTITY THEFT

- **Gather and Analyze Statistically Reliable Data from Identity Theft Victims.** The BJS and FTC should continue to gather and analyze statistically reliable data from identity theft victims. The BJS should conduct its surveys in collaboration with subject matter experts from the FTC. BJS should add additional questions on identity theft to the household portion of its National Crime Victimization Survey (NCVS), and conduct periodic supplements to gather more in-depth information. The FTC should conduct a general identity theft survey approximately every three years, independently or in conjunction with BJS or other government agencies. The FTC also should conduct surveys focused more narrowly on issues related to the effectiveness of and compliance with the identity theft-related provisions of the consumer protection laws it enforces.

- **Expand Scope of National Crime Victimization Survey (NCVS).** The scope of the annual NCVS should be expanded to collect information about the characteristics, consequences, and extent of identity theft for individuals ages 12 and older. Currently, information on identity theft is collected only from the household respondent and does not capture data on multiple victims in the household or multiple episodes of identity theft.

- **Review of Sentencing Commission Data.** DOJ and the FTC should systematically review and analyze U.S. Sentencing Commission identity theft-related case files every two to four years, and should begin in the third quarter of 2007.

- **Track Prosecutions of Identity Theft and the Amount of Resources Spent.** In order to better track resources spent on identity theft cases, DOJ should, by the second quarter of 2007, create an "Identity Theft" category on the monthly report that is completed by all Assistant United States Attorneys, and should revise its departmental case tracking application to allow for the reporting of offenses by individual subsections of section 1028. Additionally, BJS should incorporate additional questions in the National Survey of Prosecutors to better understand the impact identity theft is having on prosecutorial resources.

- **Conduct Targeted Surveys.** In order to expand law enforcement knowledge of the identity theft response and prevention activities of state and local police, BJS should undertake new data collections in specified areas. Proposed details of those surveys are included in Appendix J.

IV. Conclusion: The Way Forward

There is no magic bullet that will eradicate identity theft. To successfully combat identity theft and its effects, we must keep personal information out of the hands of thieves; take steps to prevent an identity thief from misusing any data that may end up in his hands; prosecute him vigorously if he succeeds in committing the crime; and do all we can to help the victims recover.

Only a comprehensive and fully coordinated strategy to combat identity theft—one that encompasses effective prevention, public awareness and education, victim assistance, and law enforcement measures, and that fully engages federal, state, and local authorities and the private sector—will have any chance of solving the problem. This proposed strategic plan strives to set out such a comprehensive approach to combating identity theft, but it is only the beginning. Each of the stakeholders—consumers, business and government—must fully and actively participate in this fight for us to succeed, and must stay attuned to emerging trends in order to adapt and respond to developing threats to consumer well being.

Appendices

APPENDIX A

Identity Theft Task Force's Guidance Memorandum on Data Breach Protocol

September 19, 2006

MEMORANDUM FROM THE IDENTITY THEFT TASK FORCE

Chair, Attorney General Alberto R. Gonzales ag
Co-Chair, Federal Trade Commission Chairman Deborah Platt Majoras DPM

SUBJECT: Identity Theft Related Data Security Breach Notification Guidance

The Identity Theft Task Force ("Task Force") has considered the steps that a Department or agency should take in responding to a theft, loss, or unauthorized acquisition of personal information that poses a risk of subsequent identity theft. This memorandum reports the Task Force's recommended approach to such situations, without addressing other notification issues that may arise under the Privacy Act or other federal statutes when the data loss involves sensitive information that does not pose an identity theft risk.

I. Background

Identity theft, a pernicious crime that harms consumers and our economy, occurs when individuals' identifying information is used without authorization in an attempt to commit fraud or other crimes.[1] There are two primary forms of identity theft. First, identity thieves can use financial account identifiers, such as credit card or bank account numbers, to commandeer an individual's existing accounts to make unauthorized charges or withdraw money. Second, thieves can use accepted identifiers like social security numbers ("SSNs") to open new financial accounts and incur charges and credit in an individual's name, but without that person's knowledge.

This memorandum describes three related recommendations: (1) Agencies should immediately identify a core response group that can be convened in the event of a breach; (2) If an incident occurs, the core response group should engage in a risk analysis to determine whether the incident poses problems related to identity theft; (3) If it is determined that an identity theft risk is present, the agency should tailor its response (which may include advice to those potentially affected, services the agency may provide to those affected, and public notice) to the nature and scope of the risk presented. The memorandum provides a menu of steps for an agency to consider, so that it may pursue such a risk-based, tailored response. Ultimately, the precise steps to take must be decided in light of the particular facts presented, as there is no single response for all breaches. This memorandum is intended simply to assist those confronting such issues in developing an appropriate response.

---

[1]Federal laws define "identifying information" broadly. *See, e.g.*, The 1998 Identity Theft Assumption and Deterrence Act (Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028)) and the Fair and Accurate Credit Transactions Act (15 U.S.C. §§ 1681-1681x, as amended). This memorandum focuses on the type of identifying information generally used to commit identity theft.

II. Data Breach Planning

Given the volume of personal information appropriately collected to carry out myriad government functions, it is almost inevitable that some agencies will, on occasion, lose control of such information. Thus, an important first step in responding to a breach is for agencies to engage in advance planning for this contingency. We therefore recommend that each agency identify in advance a core management group that will be convened upon the identification of a potential loss of personal information. This core group would initially evaluate the situation to help guide any further response. Our experience suggests that such a core group should include, at minimum, an agency's chief information officer, chief legal officer, chief privacy officer (or their designees), a senior management official from the agency, and the agency's inspector general (or equivalent or designee). Such a group should ensure that the agency has brought together many of the basic competencies needed to respond, including expertise in information technology, legal authorities, the Privacy Act, and law enforcement. We recommend that this core group convene at least annually to review this memorandum and discuss likely actions should an incident occur.

III. Identifying an Incident That Presents Identity Theft Risk and the Level of Risk Involved

A loss of control over personal information, may, but need not necessarily, present a risk of identity theft. For example, a data report showing the name "John Smith," with little or no further identifying information related to John Smith, presents little or no risk of identity theft. Thus, the first steps in considering whether there is a risk of identity theft, and hence whether an "identity theft response" is necessary, are understanding the kind of information most typically used to commit identity theft and then determining whether that kind of information has been potentially compromised in the incident being examined. Because circumstances will differ from case to case, agencies should draw upon law enforcement expertise, including that of the agency Inspector General, in assessing the risk of identity theft from a data compromise and the likelihood that the incident is the result of or could lead to criminal activity.

An SSN standing alone can generate identity theft. Combinations of information can have the same effect. With a name, address, or telephone number, identity theft becomes possible, for instance, with any of the following: (1) any government-issued identification number (such as a driver's license number if the thief cannot obtain the SSN); (2) a biometric record; (3) a financial account number, together with a PIN or security code, if a PIN or security code is necessary to access the account; or (4) any additional, specific factor that adds to the personally identifying profile of a specific individual, such as a relationship with a specific financial institution or membership in a club. For further purposes of this memorandum, information posing a risk of identity theft will be described as "covered information." If a particular data loss or breach does not involve this type of information, the identity theft risk is minimal, and it is unlikely that further steps

designed to address identity theft risks are necessary.[2]

Even where covered information has been compromised, various other factors should be considered in determining whether the information accessed could result in identity theft. Our experience suggests that in determining the level of risk of identity theft, the agency should consider not simply the data that was compromised, but all of the circumstances of the data loss, including

- how easy or difficult it would be for an unauthorized person to access the covered information in light of the manner in which the covered information was protected;[3]
- the means by which the loss occurred, including whether the incident might be the result of a criminal act or is likely to result in criminal activity;[4]
- the ability of the agency to mitigate the identity theft;[5] and
- evidence that the compromised information is actually being used to commit identity theft.

Considering these factors together should permit the agency to develop an overall sense of where

---

[2]OMB has promulgated guidance requiring certain notifications within the government, most notably to the United States Computer Emergency Readiness Team (US-CERT), whenever personal information is compromised, and which applies even where there is no identity theft risk. That reporting guidance remains in full effect.

[3]For example, information on a computer laptop that is adequately protected by encryption is less likely to be accessed, while "hard copies" of printed-out data are essentially unprotected.

[4]For example, as a general matter, the risk of identity theft is greater if the covered information was stolen by a thief who was targeting the data (such as a computer hacker) than if the information was inadvertently left unprotected in a public location, such as in a briefcase in a hotel lobby. Similarly, in some cases of theft, the circumstances might indicate that the data-storage device, such as a computer left in a car, rather than the information itself, was the target of the theft. An opportunistic criminal, of course, may exploit information once it comes into his possession, and this possibility must be considered when fashioning an agency response, along with the recognition that risks vary with the circumstances under which incidents occur. In making this assessment, it is crucial that federal law enforcement (which may include the agency's Inspector General) be consulted.

[5]The ability of an agency or other affected entities to monitor for and prevent attempts to misuse the covered information can be a factor in determining the risk of identity theft. For example, if the compromised information relates to disability beneficiaries, the agency can monitor its beneficiary database for requests for change of address, which may signal attempts to misuse the information, and take steps to prevent the fraud. Likewise, alerting financial institutions in cases of a data breach involving financial account information can allow them to monitor for fraud or close the compromised accounts.

-3-

along the continuum of identity-theft risk the risk created by the particular incident falls. That assessment, in turn, should guide the agency's further actions.

IV. Reducing Risk After Disclosure

While assessing the level of risk in a given situation, the agency should simultaneously consider options for attenuating that risk. It is important in this regard for the agency to understand certain standard options available to agencies and individuals to help protect potential victims:

A. Actions that Individuals Can Routinely Take

The steps that individuals can take to protect themselves will depend on the type of information that is compromised. In notifying the potentially affected individuals about steps they can take following a data breach, agencies should focus on the steps that are relevant to those individuals' particular circumstances, which may include the following:

- Contact their financial institution to determine whether their account(s) should be closed. This option is relevant only when financial account information is part of the breach.
- Monitor their financial account statements and immediately report any suspicious or unusual activity to their financial institution.
- Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. It might take a few months for most signs of fraudulent accounts to appear on the credit report, and this option is most useful when the data breach involves information that can be used to open new accounts. Consumers are entitled by law to obtain one free credit report per year from each of the three major credit bureaus – Equifax, Experian, and TransUnion – for a total of three reports every year. The annual free credit report can be used by individuals, along with the free report provided when placing a fraud alert (which is discussed below), to self-monitor for identity theft. The annual report also can be used as an alternative for those individuals who want to check their credit report, but do not want to place a fraud alert. Contact information for the credit bureaus should be provided, which can be found on the FTC's website.
- Place an initial fraud alert[6] on credit reports maintained by the three major credit bureaus noted above. This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. After placing an initial fraud alert, individuals are entitled to a free credit report, which they should

---

[6]A fraud alert is a mechanism that signals to credit issuers who obtain credit reports on a consumer that they must take reasonable steps to verify the consumer's identity before issuing credit, making it harder for identity thieves to secure new credit lines. It should be noted that, although fraud alerts can help prevent fraudulent credit accounts from being opened in an individual's name, they also can delay that individual's own legitimate attempts to secure credit.

obtain beginning a few months after the breach and review for signs of suspicious activity.

- For residents of states in which state law authorizes a credit freeze, consider placing a credit freeze on their credit file.[7] This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. A credit freeze cuts off third party access to a consumer's credit report, thereby effectively preventing the issuance of new credit in the consumer's name.
- For deployed members of the military, consider placing an active duty alert on their credit file.[8] This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. Such active duty alerts serve a similar function as initial fraud alerts, causing creditors to be more cautious in extending new credit. However, unlike initial fraud alerts, they last for one year instead of 90 days. In addition, active duty alerts do not entitle the individual to a free credit report. Therefore, those placing an active duty alert should combine this option with a request for obtaining the annual free credit reports to which all individuals are entitled.
- Review resources provided on the FTC identity theft website, www.ftc.gov/idtheft. The FTC maintains a variety of consumer publications providing comprehensive information on breaches and identity theft.
- Be aware that the public announcement of the breach could itself cause criminals engaged in fraud, under the guise of providing legitimate assistance, to use various techniques, including email or the telephone, to deceive individuals affected by the breach into disclosing their credit card numbers, bank account information, SSNs, passwords, or other sensitive personal information. One common such technique is "phishing," a scam involving an email that appears to come from a bank or other organization that asks the individual to verify account information, and then directs him to a fake website whose only purpose is to trick the victim into divulging his personal information. Advice on avoiding such frauds is available on the FTC's web site http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt166.htm.

---

[7]State laws vary with respect to usability and cost issues, which individuals will need to consider before deciding to place a credit freeze.

[8]A variety of factors may influence a service member's decision to place an active duty alert–for example, if there are stateside family members who need easy credit access, the alert would likely be counterproductive.

-5-

B. Actions that Agencies Can Take

If the breach involves government-authorized credit cards, the agency should notify the issuing bank promptly. If the breach involves individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit payment, the agency should notify the bank or other entity that handles that particular transaction for the agency.

Agencies may take two other significant steps that can offer additional measures of protection – especially for incidents where the compromised information presents a risk of new accounts being opened – but which will involve additional agency expense. First, in recent years, some companies have developed technologies to analyze whether a particular data loss appears to be resulting in identity theft. This data breach analysis may be a useful intermediate protective action, especially where the agency is uncertain about whether the identity-theft risk warrants implementing more costly additional steps such as credit monitoring (see below) or where the risk is such that agencies wish to do more than rely on the individual action(s) identified above.

For two reasons, such technology may be useful for incidents involving data for large numbers of individuals. First, the cost of implementing credit monitoring (and the potential to have spent large sums unnecessarily if no identity theft materializes) can be substantial for large incidents because the cost of credit monitoring generally is a function of the number of individuals for whom credit monitoring is being provided. Second, subsequent to any large data breach that is reported publicly, it is likely that an agency will get reports of identity theft directly from individuals in the affected class. Yet, agencies should be aware that approximately 3.6% of the adult population reports itself annually as the victim of some form of identity theft. Thus, for any large breach, it is statistically predictable that a certain number of the potential victim class will be victims of identity theft through events *other than* the data security breach in question. Data-breach monitoring of the type described here can assist an agency in determining whether the particular incident it has suffered is truly a source of identity theft, or whether, instead, any such reports are the normal by-product of the routine incidence of identity theft.

Second, and typically at great expense, agencies may wish to provide credit-monitoring services. Credit monitoring is a commercial service that can assist individuals in early detection of instances of identity theft, thereby allowing them to take steps to minimize the harm (although credit monitoring cannot guarantee that identity theft will not occur). A credit-monitoring service typically notifies individuals of changes that appear in their credit report, such as creation of a new account or new inquiries to the file.[9]

---

[9]Various credit-monitoring services provide different features and their offerings are constantly evolving. Therefore, agencies may wish to consult with OMB or the FTC concerning the most current, available options.

In deciding whether to offer credit monitoring services and of what type and length, agencies should consider the seriousness of the risk of identity theft arising from the data breach. Particularly important are whether incidents have already been detected and the cost of providing the service. Such costs can be substantial, although rates are often subject to negotiation; bulk purchase discounts have been offered in many cases of large data breaches.[10] The length of time for which the service is provided may have an impact on cost as well. In addition, the agency should consider the characteristics of the affected individuals. Some affected populations may have more difficulty in taking the self-protective steps described earlier. For example, there may be groups who, because of their duties or their location, may warrant special protection from the distraction or effort of self-monitoring for identity theft.

Agencies should also be aware that, to assist the timely implementation of either data breach analysis or credit monitoring, the General Services Administration (GSA) is putting in place several government-wide contracting methods to provide these services if needed. Thus, an agency's contract officer, working with GSA, should be able promptly to secure such services and to develop cost estimates associated with such services.

Finally, it is important to note that notification to law enforcement is an important way for an agency to mitigate the risks faced by the potentially affected individuals. Because an agency data breach may be related to other breaches or other criminal activity, the agency's Inspector General should coordinate with appropriate federal law enforcement agencies to enable the government to look for potential links and to effectively investigate and punish criminal activity that may result from, or be connected to, the breach.

V. Implementing a Response Plan: Notice to Those Affected

Having identified the level of risk and bearing in mind the steps that can be taken by the agency or individual to limit that risk, the agency should then move to implement a response plan that incorporates elements of the above. Agencies should bear in mind that notice and the response it can generate from individuals is not "costless," a consideration that can be especially important where the risk of identity theft is low. The costs can include the financial expense and inconvenience that can arise from canceling credit cards, closing bank accounts, placing fraud alerts on credit files, and/or obtaining new identity documents. The private sector and other government agencies also incur costs in servicing these consumer actions. Moreover, frequent public notices of such incidents may be counterproductive, running the risk of injuring the public and, by making it more difficult to distinguish between serious and minor threats, causing citizens to ignore all notices, even of incidents that truly warrant heightened vigilance. Thus, weighing all the facts available, the risks to consumers caused by the data security breach warrant notice when notice would facilitate appropriate remedial action that is likely to be justified given the risk.

---

[10]In some instances, monitoring services may even be provided at no cost. Agencies should check the GSA contract schedule.

Assuming that an agency has made the decision to provide notice to those put at risk, agencies should incorporate the following elements into that notification process:

1. ***Timing***: The notice should be provided in a timely manner, but without compounding the harm from the initial incident through premature announcement based on incomplete facts or in a manner likely to make identity theft more likely to occur as a result of the announcement. While it is important to notify promptly those who may be affected so that they can take protective steps quickly, false alarms or inaccurate alarms are counterproductive. In addition, sometimes an investigation of the incident (such as a theft) can be impeded if information is made public prematurely. For example, an individual who has stolen a password-protected laptop in order to resell it may be completely unaware of the nature and value of the information the laptop contains. In such a case, public announcement may actually alert the thief to what he possesses, increasing risk that the information will be misused. Thus, officials should consult with those law enforcement officials investigating the incident (which could include the agency's Inspector General) regarding the timing and content of any announcement, before making any public disclosures about the incident. Indeed, even when the decision has been made to notify affected individuals, under certain circumstances, law enforcement may need a temporary delay before such notice is given to ensure that a criminal investigation can be conducted effectively or for national security reasons. Similarly, if the data breach resulted from a failure in a security or information system, that system should be repaired and tested before disclosing details related to the incident.[11]

2. ***Source***: Given the serious security and privacy concerns raised by data breaches, notification to individuals affected by the data loss should be issued by a responsible official of the agency, or, in those instances in which the breach involves a publicly known component of an agency, a responsible official of the component.

There may be some instances in which notice of a breach may appropriately come from an entity other than the actual agency that suffered the loss. For example, when the data security breach involves a federal contractor operating a system of records on behalf of the agency or a public-private partnership (for example, a federal agency/private-sector agreement to operate a program that requires the collection of covered information on members of the public), the responsibility for complying with these notification procedures should be established with the contractor or partner prior to entering the business relationship. Additionally, a federal agency that suffers a breach involving personal information may wish to determine, in conjunction with the regulated entity from which it obtained the information, whether notice is more appropriately given by the agency or by the regulated entity. Whenever possible, to avoid creating confusion and anxiety, the actual notice

---

[11] There may be other reasons related to law enforcement or national security that dictate that notice not be given to those who are affected. For example, if an agency suffers a breach of a database containing law enforcement sensitive data, immediate notification to potentially affected individuals may be inappropriate – even if the risk of identity theft resulting from that breach is significant – as such notification may result in the disclosure of law enforcement-sensitive or counter-terrorism data.

should come from the entity which the affected individuals are reasonably likely to perceive as the entity with which they have a relationship. In all instances, the agency is responsible for ensuring that its contractor or partner promptly notifies the agency of any data loss it suffers.

3. ***Contents***: The substance of the notice should be reduced to a stand-alone document and written in clear, concise, and easy-to-understand language, capable of individual distribution and/or posting on the agency's website and other information sites. The notice should include the following elements:

- a brief description of what happened;
- to the extent possible, a description of the types of personal information that were involved in the data security breach (e.g., full name, SSN, date of birth, home address, account number, disability code, etc.);
- a brief description of what the agency is doing to investigate the breach, to mitigate losses, and to protect against any further breaches;
- contact procedures for those wishing to ask questions or learn additional information, including a toll-free telephone number, website, and/or postal address;
- steps individuals should take to protect themselves from the risk of identity theft (see above for the steps available), including steps to take advantage of any credit monitoring or other service the agency intends to offer and contact information for the FTC website, including specific publications.

Given the amount of information needed to give meaningful notice, an agency may want to consider providing the most important information up front, with the additional details in a Frequently Asked Questions (FAQ) format or on its website. If an agency has knowledge that the affected individuals are not English speaking, notice should also be provided in the appropriate language(s).

4. ***Method of Notification***: Notification should occur in a manner calibrated to ensure that the individuals affected receive actual notice of the incident and the steps they should take. First-class mail notification to the last known mailing address of the individual should be the primary means by which the agency provides notification. Even when an agency has reason to doubt the continued accuracy of such an address or lacks an address, mailed notice may still be effective. The United States Postal Service (USPS) will forward mail to a new address for up to one year, or will provide an updated address via established processes.[12] Moreover, certain agencies, such as the Social Security Administration and the Internal Revenue Service, may sometimes possess address information that can be used to facilitate effective mailing. The notice should be

---

[12]Agencies may receive updated addresses as a mailer by becoming a direct licensee of the Postal Service or by using a USPS licensed NCOA Link service provider. A current list of service providers is available at http://ribbs.usps.gov/files/ncoalink/CERTIFIED%5FLICENSEES/. For information on address-update and delivery-validation services, contact the USPS at 1-800-589-5766.

sent separately from any other mailing so that it stands out to the recipient. If using another agency to facilitate mailing as referenced above, agencies should take care that the agency that suffered the loss is identified as the sender, not the facilitating agency.

Substitute means of notice such as broad public announcement through the media, website announcements, and distribution to public service and other membership organizations likely to have access to the affected individual class, should be employed to supplement direct mail notification or if the agency cannot obtain a valid mailing address. Email notification is discouraged, as the affected individuals could encounter difficulties in distinguishing the agency's email from a "phishing" email.

The agency also should give special consideration in providing notice to individuals who are visually or hearing impaired consistent with Section 504 of the Rehabilitation Act of 1973. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on the agency's web site.

5. ***Preparing for follow-on inquiries***: Those notified can experience considerable frustration if, in the wake of an initial public announcement, they are unable to find sources of additional accurate information. Agencies should be aware that the GSA has a stand-by capability through its "USA Services" operation to quickly put in place a 1-800-FedInfo call center staffed by trained personnel and capable of handling individual inquiries for circumstances in which the number of inquiries is likely to exceed the agency's native capacity. Thus, agencies may wish to consider briefly delaying a public announcement to allow them to implement a consolidated announcement strategy, as opposed to a hasty public announcement without any detailed guidance on steps to take. Such a strategy will permit public statements, website postings, and a call center staffed with individuals prepared to answer the most frequently asked questions all to be made simultaneously available.

6. ***Prepare counterpart entities that may receive a surge in inquiries***: Depending on the nature of the incident, certain entities, such as the credit-reporting agencies or the FTC, may experience a surge in inquiries also. For example, in incidents involving a substantial number of SSNs (e.g., more than 10,000), notifying the three major credit bureaus allows them to prepare to respond to requests from the affected individuals for fraud alerts and/or their credit reports. Thus, especially for large incidents, an agency should inform the credit bureaus and the FTC of the timing and distribution of any notices, as well as the number of affected individuals, in order to prepare.

APPENDIX B

Proposed Routine Use Language

Subsection (b)(3) of the Privacy Act provides that information from an agency's system of records may be disclosed without a subject individual's consent if the disclosure is "for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section." 5 U.S.C. § 552a(b)(3). Subsection (a)(7) of the Act states that "the term 'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." 5 U.S.C. § 552a(a)(7). The Office of Management and Budget, which pursuant to subsection (v) of the Privacy Act has guidance and oversight responsibility for the implementation of the Act by federal agencies, has advised that the compatibility concept encompasses (1) functionally equivalent uses, and (2) other uses that are necessary and proper. 52 Fed. Reg. 12,990, 12,993 (Apr. 20, 1987). In recognition of and in accordance with the Act's legislative history, OMB in its initial Privacy Act guidance stated that "[t]he term routine use . . . recognizes that there are corollary purposes 'compatible with the purpose for which [the information] was collected' that are appropriate and necessary for the efficient conduct of government and in the best interest of both the individual and the public." 40 Fed. Reg. 28,948, 28,953 (July 9, 1975). A routine use to provide for disclosure in connection with response and remedial efforts in the event of a breach of federal data would certainly qualify as such a necessary and proper use of information—a use that is in the best interest of both the individual and the public.

Subsection (e)(4)(D) of the Privacy Act requires that agencies publish notification in the Federal Register of "each routine use of the records contained in the system, including the categories of users and the purpose of such use." 5 U.S.C. § 552a(e)(4)(D). The Department of Justice has developed the following routine use that it plans to apply to its Privacy Act systems of records, and which allows for disclosure as follows:[80]

> To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Agencies should already have a published system of records notice for each of their Privacy Act systems of records. To add a new routine use to an agency's existing systems of records, an agency must simply publish a notice in the Federal Register amending its existing systems of records to include the new routine use.

Subsection (e)(11) of the Privacy Act requires that agencies publish a Federal Register notice of any new routine use at least 30 days prior to its use and "provide an opportunity for interested persons to submit written data, views, or arguments to the agency." 5 U.S.C. § 552a(e)(11). Additionally, subsection (r) of the Act requires that an agency provide Congress and OMB with "adequate advance notice" of any proposal to make a "significant change in a system of records." 5 U.S.C. § 552a(r). OMB has stated that the addition of a routine use qualifies as a significant change that must be reported to Congress and OMB and that such notice is to be provided at least 40 days prior to the alteration. *See* Appendix I to OMB Circular No. A-130—Federal Agency Responsibilities for Maintaining Records About Individuals, 61 Fed. Reg. 6435, 6437 (Feb. 20, 1996). Once a notice is prepared for publication, the agency would send it to the Federal Register, OMB, and Congress, usually simultaneously, and the proposed change to the system (i.e., the new routine use) would become effective 40 days thereafter. *See id*. at 6438 (regarding timing of systems of records reports and noting that notice and comment period for routine uses and period for OMB and congressional review may run concurrently). Recognizing that each agency likely will receive different types of comments in response to its notice, the Task Force recommends that OMB work to ensure accuracy and consistency across the range of agency responses to public comments.

APPENDIX C

Text of Amendments to 18 U.S.C. §§ 3663(b) and 3663A(b)

Proposed Language:

(a) Section 3663 of Title 18, United States Code, is amended by:

(1) Deleting "and" at the end of paragraph (4) of subsection (b);

(2) Deleting the period at the end of paragraph (5) of subsection (b) and inserting in lieu thereof "; and"; and

(3) Adding the following after paragraph (5) of subsection (b):

"(6) in the case of an offense under sections 1028(a)(7) or 1028A(a) of this title, pay an amount equal to the value of the victim's time reasonably spent in an attempt to remediate intended or actual harm incurred from the offense.".

Make conforming changes to the following:

(b) Section 3663A of Title 18, United States Code, is amended by:

(1) Adding the following after Section 3663A(b)(4)

"(5) in the case of an offense under this title, section 1028(a)(7) or 1028A(a), pay an amount equal to the value of the victim's time reasonably spent in an attempt to remediate intended or actual harm incurred from the offense.".

Section Analysis

These new subsections provide that defendants may be ordered to pay restitution to victims of identity theft and aggravated identity theft for the value of the victim's time spent remediating the actual or intended harm of the offense. Restitution could therefore include an amount equal to the value of the victim's time spent clearing a victim's credit report or resolving charges made by the perpetrator for which the victim has been made responsible.

New subsections 3663(b)(6) and 3663A(b)(5) of Title 18 would make clear that restitution orders may include an amount equal to the value of the victim's time spent remediating the actual or intended harm of the identity theft or aggravated identity theft offense. The federal courts of appeals have interpreted the existing provisions of Section 3663 in such a way that would likely preclude the recovery of such amounts, absent explicit statutory authorization. For example, in *United States v. Arvanitis*, 902 F.3d 489 (7th Cir. 1990), the court held that restitution ordered for offenses resulting in loss of property must be limited to recovery of property which is the subject of the offenses, and may not include consequential damages. Similarly, in *United States v. Husky*, 924 F.2d 223 (11th Cir. 1991), the Eleventh Circuit held

that the list of compensable expenses in a restitution statute is exclusive, and thus the district court did not have the authority to order the defendant to pay restitution to compensate the victim for mental anguish and suffering. Finally, in *United States v. Schinnell*, 80 F.3d 1064 (5th Cir. 1996), the court held that restitution was not allowed for consequential damages involved in determining the amount of loss or in recovering those funds; thus, a victim of wire fraud was not entitled to restitution for accounting fees and costs to reconstruct bank statements for the time period during which the defendant perpetuated the scheme, for the cost of temporary employees to reconstruct monthly bank statements, and for the costs incurred in borrowing funds to replace stolen funds. These new subsections will provide statutory authority for inclusion of amounts equal to the value of the victim's time reasonably spent remediating the harm incurred as a result of the identity theft offense.

APPENDIX D

Text of Amendments to 18 U.S.C. §§ 2703, 2711 and 3127, and Text of New Language for 18 U.S.C. § 3512

The basis for these proposals is set forth in Section III.2 of the strategic plan, which describes coordination with foreign law enforcement.

Proposed Language:

§ 2703. Required disclosure of customer communications or records

(a) **Contents of wire or electronic communications in electronic storage.**—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ~~by a court with jurisdiction over the offense under investigation~~ ***by a court of competent jurisdiction*** or an equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) **Contents of wire or electronic communications in a remote computing service.**—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ~~by a court with jurisdiction over the offense under investigation~~ ***by a court of competent jurisdiction*** or equivalent State warrant; ***or***

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(c) **Records concerning electronic communication service or remote computing service.**—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ~~by a court with jurisdiction over the offense under investigation~~ ***by a court of competent jurisdiction*** or equivalent State warrant;

§ 2711. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system; and

(3) the term "court of competent jurisdiction" ~~has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation~~ ***means***—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that–

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or

(iii) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants.

§ 3127. Definitions for chapter

As used in this chapter—

(1) the terms "wire communication", "electronic communication", "electronic communication service", and "contents" have the meanings set forth for such terms in section 2510 of this title;

(2) the term "court of competent jurisdiction" means—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals ~~having jurisdiction over the offense being investigated~~ ***that~~***–

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of electronic communication service is located;

(iii) is in or for a district in which a landlord, custodian, or other person subject to 3124(a) or (b) is located; or

(iv) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

§ 3512. Foreign requests for assistance in criminal investigations and prosecutions:

(a) Upon application of an attorney for the government, a Federal judge may issue such orders as may be necessary to execute a request from a foreign authority for assistance in the investigation or prosecution of criminal offenses, or in proceedings related to the prosecution of criminal offenses including but not limited to proceedings regarding forfeiture, sentencing, and restitution. Such orders may include the issuance of a search warrant as provided under Rule 41 of the Federal Rules of Criminal Procedure, a warrant or order for contents of stored wire or electronic communications or for records related thereto as provided under 18 U.S.C. § 2703, an order for a pen register or trap and trace device as provided under 18 U.S.C. § 3123, or an order requiring the appearance of a person for the purpose of providing testimony or a statement, or requiring the production of documents or other things, or both.

(b) In response to an application for execution of a request from a foreign authority as described in subsection (a) , a Federal judge may also issue an order appointing a person to direct the taking of testimony or statements or of the production of documents or other things, or both. A person so appointed may be authorized to –

(1) issue orders requiring the appearance of a person, or the production of documents or other things, or both;

(2) administer any necessary oath; and

(3) take testimony or statements and receive documents or other things.

(c) Except as provided in subsection (d), an application for execution of a request from a foreign authority under this section may be filed –

(1) in the district in which a person who may be required to appear resides or is located or in which the documents or things to be produced are located;

(2) in cases in which the request seeks the appearance of persons or production of documents or things that may be located in multiple districts, in any one of the districts in which such a person, documents or things may be located; or

(3) in any case, the district in which a related Federal criminal investigation or prosecution is being conducted, or in the District of Columbia.

(d) An application for a search warrant under this section, other than an application for a warrant issued as provided under 18 U.S.C. § 2703, must be filed in the district in which the place or person to be searched is located.

(e) A search warrant may be issued under this section only if the foreign offense for which the evidence is sought involves conduct that, if committed in the United States, would be considered an offense punishable by imprisonment for more than one year under federal or state law.

(f) Except as provided in subsection (d), an order or warrant issued pursuant to this section may be served or executed in any place in the United States.

(g) This section does not preclude any foreign authority or an interested person from obtaining assistance in a criminal investigation or prosecution pursuant to 28 U.S.C. § 1782.

(h) As used in this section –

(1) the term "foreign authority" means a foreign judicial authority, a foreign authority responsible for the investigation or prosecution of criminal offenses or for proceedings related to the prosecution of criminal offenses, or an authority designated as a competent authority or central authority for the purpose of making requests for assistance pursuant to an agreement or treaty with the United States regarding assistance in criminal matters; and

(2) the terms "Federal judge" and "attorney for the Government" have the meaning given such terms for the purposes of the Federal Rules of Criminal Procedure.

APPENDIX E

Text of Amendments to 18 U.S.C. §§ 1028 and 1028A

The basis for these proposed amendments is set forth in Section III.D.4.a of the strategic plan, which describes gaps in the identity theft statutes.

Proposed Amendment to Aggravated Identity Theft Statute to Add Predicate Offenses

Congress should amend the aggravated identity theft offense (18 U.S.C. § 1028A) to include other federal offenses that recur in various identity-theft and fraud cases, specifically, mail theft (18 U.S.C. § 1708), uttering counterfeit securities (18 U.S.C. § 513), and tax fraud (26 U.S.C. §§ 7201, 7206, and 7207), as well as conspiracy to commit specified felonies already listed in section 1028A—in the statutory list of predicate offenses for that offense (18 U.S.C. § 1028A(c)).

Proposed Additions to Both Statutes to Include Misuse of Identifying Information of Organizations

(a) Section 1028(a) of Title 18, United States Code, is amended by inserting in paragraph (7) the phrase "(including an organization as defined in Section 18 of this Title)" after the word "person".

Section 1028A(a) of Title 18, United States Code, is amended by inserting in paragraph (1) the phrase "(including an organization as defined in Section 18 of this Title)" after the word "person".

(b) Section 1028(d)(7) of Title 18, United States Code, is amended by inserting in paragraph (7) the phrase "or other person" after the word "individual".

Rationale:

Corporate identity theft whereby criminals assume the identity of corporate entities to cloak fraudulent schemes in a misleading and deceptive air of legitimacy have become rampant. Criminals routinely engage in unauthorized "appropriation" of legitimate companies' names and logos in a variety of contexts: misrepresenting themselves as officers or employees of a corporation, sending forged or counterfeit documents or financial instruments to victims to improve their aura of legitimacy, and offering nonexistent benefits (e.g., loans and credit cards) in the names of companies.

One egregious example of corporate identity theft is represented on the Internet by the practice commonly known as "phishing," whereby criminals electronically assume the identity of a corporation in order to defraud unsuspecting recipients of email solicitations to voluntarily disclose identifying and financial account information. This personal information is then used to further the underlying criminal scheme—for example, to

scavenge the bank and credit card accounts of these unwitting consumer victims. Phishing is just one example of how criminals in mass-marketing fraud schemes incorporate corporate identity theft into their schemes, though phishing also is designed with individual identity theft in mind.

Phishing has become so routine in many major fraud schemes that no particular corporation can be easily singled out as having suffered a special "horror story" which stands above the rest. In August 2005, the "Anti-Phishing Working Group" determined in just that month alone, there were 5,259 unique phishing websites around the world. By December 2005, that number had increased to 7,197, and there were 15,244 unique phishing reports. It was also reported in August 2005, that 84 corporate entities' names (and even logos and web content) were "hijacked" (i.e., misused) in phishing attacks, though only 3 of these corporate brands accounted for 80 percent of phishing campaigns. By December 2005 the number of victimized corporate entities had increased to 120. The financial sector is and has been the most heavily targeted industry sector in phishing schemes, accounting for nearly 85 percent of all phishing attacks. *See*, *e.g.* ***http://antiphishing.org/apwg_phishing_activity_report_august_05.pdf***.

In addition, major companies have reported to the Department of Justice that their corporate names, logos, and marks are often being misused in other types of fraud schemes. These include telemarketing fraud schemes in which communications purport to come from legitimate banks or companies or offer products or services from legitimate banks and companies, and West African fraud schemes that misuse legitimate banks and companies' names in communications with victims or in counterfeit checks.

Uncertainty has arisen as to whether Congress intended Sections 1028(a)(7) and 1028A(a) of Title 18, United States Code to apply only to "natural" persons or to also protect corporate entities. These two amendments would clarify that Congress intended that these statute apply broadly and may be used against phishing directed against victim corporate entities.

APPENDIX F

Text of Amendment to 18 U.S.C. § 1030(a)(2)

The basis for this proposed amendment is set forth in Section III.D.4.b of the strategic plan, which describes gaps in the computer-related identity theft statutes.

Proposed Language:

1030(a) Whoever—

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains–

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer ~~if the conduct involved an interstate or foreign communication~~;

APPENDIX G

Text of Amendments to 18 U.S.C. §§ 1030(a)(5), (c), and (g), and to 18 U.S.C. § 2332b

The basis for these proposed amendments is set forth in Section III.D.4.b of the strategic plan, which describes gaps in the computer-related identity theft statutes.

Proposed Language:

18 U.S.C. § 1030

(a) Whoever—

(5)

(A) ~~(i)~~ knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) ~~(ii)~~ intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) ~~(iii)~~ intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; ~~and~~

~~(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—~~

~~(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;~~

~~(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;~~

~~(iii) physical injury to any person;~~

~~(iv) a threat to public health or safety; or~~

~~(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;~~

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(2) (A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), ~~(a)(5)(A)(iii)~~, or (a)(6) of this

section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3) ...(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), ~~(a)(5)(A)(iii)~~, or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

~~(4) (A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;~~

~~(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;~~

~~(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and~~

~~(5) (A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and~~

~~(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.~~

(4) (A) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety;

(v) damage affecting a computer used by or for a government entity in furtherance of the administration of justice, national defense, or national security; or

(vi) damage affecting ten or more protected computers during any 1-year period;

or an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (c)(4)(D) and (c)(4)(E), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subparagraphs (c)(4)(A)(i) through (vi), or an attempt to commit an offense punishable under this subparagraph;

(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5) that occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(D) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title or imprisonment for not more than 20 years, or both;

(E) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title or imprisonment for any term of years or for life, or both; or

(F) a fine under this title, imprisonment for not more than one year, or both, for any other offense under subsection (a)(5), or an attempt to commit an offense punishable under this subparagraph.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) ~~of subsection (a)(5)(B)~~ ***subparagraph (c)(4)(A)***. Damages for a violation involving only conduct described in ~~subsection (a)(5)(B)(i)~~ ***subparagraph (c)(4)(A)(i)*** are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

18 U.S.C. § 2332b(g)(5)(B)(I)

...1030(a)(5)(A)~~(i)~~ resulting in damage as defined in ~~1030(a)(5)(B)(ii) through (v)~~ ***1030(c)(4)(A)(ii) through (vi)*** (relating to protection of computers)...

APPENDIX H

Text of Amendments to 18 U.S.C. § 1030(a)(7)

The basis for this proposed amendment is set forth in Section III.D.4.c of the strategic plan, which describes gaps in the cyber-extortion statute.

Proposed Language:

18 U.S.C. § 1030(a)(7)

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any –

(a) threat to cause damage to a protected computer***;***

(b) ***threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or***

(c) ***demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;***

APPENDIX I

Text of Amendment to United States Sentencing Guideline § 2B1.1

The basis for this proposed amendment is set forth in Section III.D.4.d of the strategic plan, which describes the Sentencing Guidelines provision governing identity theft.

Proposed language for United States Sentencing Guidelines § 2B1.1, comment.(n.1):

"Victim" means (A) any person who sustained any harm, whether monetary or non-monetary, as a result of the offense. Harm is intended to be an inclusive term, and includes bodily injury, non-monetary loss such as the theft of a means of identification, invasion of privacy, reputational damage, and inconvenience. "Person" includes individuals, corporations, companies, associations, firms, partnerships, societies, and joint stock companies.

APPENDIX J

Description of Proposed Surveys

In order to expand law enforcement knowledge of the identity theft response and prevention activities of state and local police, the Bureau of Justice Statistics (BJS) should undertake new data collections in three areas: (1) a survey of law enforcement agencies focused on the response to identity theft; (2) enhancements to the existing Law Enforcement Management and Administrative Statistics (LEMAS) survey platform; and (3) enhancements to the existing training academy survey platform. Specifically, BJS should undertake to do the following:

- **New survey of state and local law enforcement agencies.** A new study focused on state and local law enforcement responses to identity theft should seek to document agency personnel, operations, workload, and policies and programs related to the handling of this crime. Detail on the organizational structure, if any, associated with identity theft response should be included (for example, the use of special units devoted to identity theft). The study should inquire about participation in regional identity theft task forces, community outreach and education efforts, as well as identity theft prevention programs. Information collected should also include several summary measures of identity theft in the agencies' jurisdictions (offenses known, arrests, referrals, outcomes), with the goal of producing some standardized metrics with which to compare jurisdictions.
- **Enhancement to existing LEMAS survey.** BJS should develop a special battery of questions for the existing LEMAS survey platform. The LEMAS survey, conducted roughly every three years since 1987, collects detailed administrative information from a nationally representative sample of about 3,000 agencies. The sample includes all agencies with 100 or more officers, and a stratified random sample of smaller agencies as well as campus law enforcement agencies. Information collected should include whether agencies presently enforce identity theft laws, utilize special units, have designated personnel, participate in regional identity theft task forces, and have policies and procedures in place related to the processing of identity theft incidents. The survey should also inquire whether agencies collect summary measures of identity theft in their jurisdictions, including offenses known, arrests, referrals, and any outcome measures. Finally, this study should also collect information on whether agencies are engaged in community outreach, education, and prevention activities related to identity theft.
- **Enhancement to existing law enforcement training academy survey.** BJS should develop a special battery of questions for the existing law enforcement training academy survey platform. A section of the data collection instrument should be devoted to the types of training, if any,

being provided by basic academies across the country in the area of identity theft. BJS should subsequently provide statistics on the number of recruits who receive training on identity theft, as well as the nature and content of the training. In-service training provided to active-duty officers should also be covered.

- **The Bureau of Justice Statistics should revise both the State Court Processing Statistics (SCPS) and National Judicial Reporting Program (NJRP) programs so that they are capable of distinguishing identity theft from other felony offenses.** In addition, the scope of these surveys should be expanded to include misdemeanor identity theft offenders. If SCPS and NJRP were able to follow identity theft offenders, then a variety of different types of court-specific information could be collected. These include how many offenders are charged with identity theft in the Nation's courts, what percentage of these offenders are released at pretrial, and how are the courts adjudicating (e.g., convicting or dismissing) identity theft offenders. Among those convicted identity theft offenders, data should be collected on how many are being sentenced to prison, jail, or probation. These projects should also illuminate the prior criminal histories or rap sheets of identity theft offenders. Both projects should also allow for the post conviction tracking of identity theft offenders for the purposes of examining their overall recidivism rates.
- BJS should ensure that other state court studies that it funds are reconfigured to analyze the problem of identity theft. For example, State Court Organization (SCO) currently surveys the organizational structure of the Nation's state courts. This survey could be supplemented with additional questionnaires that measure whether special courts similar to gun, drug, or domestic violence courts are being created for identity theft offenders. Also, SCO should examine whether courts are training or funding staff equipped to handle identity theft offenders.
- BJS should ensure that the Civil Justice Survey of State Courts, which examines civil trial litigation in a sample of the Nation's state courts, is broadened to identify and track various civil enforcement procedures and their utilization against identity thieves.

ENDNOTES

1. Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998). The Identity Theft Assumption and Deterrence Act provides an expansive definition of identity theft. It includes the misuse of any identifying information, which could include name, SSN, account number, password, or other information linked to an individual, to commit a violation of federal or state law. The definition thus covers misuse of existing accounts as well as creation of new accounts.

2. The federal financial regulatory agencies include the banking and securities regulators, namely, the Federal Deposit Insurance Corporation, the Federal Reserve Board, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Commodity Futures Trading Commission, and the Securities and Exchange Commission.

3. The public comments are available at ***www.idtheft.gov.***

4. Testimony of John M. Harrison, June 19, 2003, Senate Banking Committee, "The Growing Problem of Identity Theft and its Relationship to the Fair Credit Reporting Act."

5. *See* U.S. Attorney's Office, Western District of Michigan, Press Release (July 5, 2006), available at ***http://www.usdoj.gov/usao/miw/press/JMiller_Others10172006.html***.

6. Javelin Strategy and Research, *2007 Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance Necessary* (Feb 2007), summary available at ***http://www.javelinstrategy.com***; Bureau of Justice Statistics (DOJ) (2004), available at ***http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf***; Gartner, Inc. (2003), available at ***http://www.gartner.com/5_about/press_releases/pr21july2003a.jsp***; FTC 2003 Survey Report (2003), available at ***http://www.consumer.gov/idtheft/pdf/synovate_report.pdf***.

7. *See* Business Software Alliance, *Consumer Confidence in Online Shopping Buoyed by Security Software Protection, BSA Survey Suggests* (Jan. 12, 2006), available at ***http://www.bsacybersafety.com/news/2005-Online-Shopping-Confidence.cfm***.

8. *See* Cyber Security Industry Alliance, *Internet Security Voter Survey* (June 2005) at 9, available at ***https://www.csialliance.org/publications/surveys_and_polls/CSIA_Internet_Security_Survey_June_2005.pdf***.

9. *See* U.S. Attorney's Office, Southern District of Florida, Press Release (July 19, 2006), available at ***http://www.usdoj.gov/usao/fls/PressReleases/060719-01.html***.

10. *See*, *e.g.*, John Leland, *Meth Users, Attuned to Detail, Add Another Habit: ID Theft*, New York Times, July 11, 2006, available at ***http://www.nytimes.com/2006/07/11/us/11meth.html?ex=1153540800&en=7b6c7773afa880be&ei=5070***; Byron Acohido and Jon Swartz, ***Meth addicts' other habit: Online Theft***, USA Today, December 14, 2005, available at ***http://www.usatoday.com/tech/news/internetprivacy/2005-12-14-meth-online-theft_x.htm***.

11. Bob Mims, *Id Theft Is the No. 1 Runaway U.S. Crime*, The Salt Lake Tribune, May 3, 2006, available at 2006 WLNR 7592526.

12. Dennis Tomboy, *Meth Addicts Stealing Mail*, Deseret Morning News, April 28, 2005, ***http://deseretnews.com/dn/view/0,1249,600129714,00.html.***

13. Stephen Mihm, *Dumpster-Diving for Your Identity*, New York Times Magazine, December 21, 2003, available at ***http://www.nytimes.com/2003/12/21/magazine/21IDENTITY.html?ex=1387342800&en=b693eef01223bc3b&ei=5007&partner=USERLAND***.

14. Pub. L. No. 108-159, 117 Stat. 1952.

15. The FACT Act required merchants to comply with this truncation provision within three years of the Act's passage with respect to any cash register or device that was in use before January 1, 2005, and within one year of the Act's passage with respect to any cash register or device that was first put into use on or after January 1, 2005. 15 U.S.C. § 1681c(g)(3).

16. *Overview of Attack Trends*, CERT Coordination Center 2002, available at ***http://www.cert.org/archive/pdf/attack_trends.pdf.***

17. Lanowitz, T., Gartner Research ID Number G00127407: December 1, 2005.

18. *"Vishing" Is Latest Twist In Identity Theft Scam,* Consumer Affairs, July 24, 2006, available at ***http://www.consumeraffairs.com/news04/2006/07/scam_vishing.html***.

19. Fraudsters have recently used pretexting techniques to obtain phone records, *see*, *e.g.*, Jonathan Krim, *Online Data Gets Personal: Cell Phone Records For Sale*, Washington Post, July 13, 2005, available at 2005 WLNR 10979279, and the FTC is pursuing enforcement actions against them. *See* ***http://www.ftc.gov/opa/2006/05/phonerecords.htm***.

20. The FTC brought three cases after sting operations against financial pretexters. Information on the settlement of those cases is available at ***http://www.ftc.gov/opa/2002/03/pretextingsettlements.htm***.

21. *See*, *e.g.*, *Computers Stolen with Data on 72,000 Medicaid Recipients*, Cincinnati Enquirer, June 3, 2006.

22. 15 U.S.C. § 1681e; 15 U.S.C. § 6802(a).

23. Although the FACT Act amendments to the Fair Credit Reporting Act require merchants to truncate credit account numbers, allowing only the final five digits to appear on an electronically generated receipt, 15 U.S.C. § 1618c(g), manually created receipts might still contain the full account number.

24. *See* ***http://www.bizjournals.com/philadelphia/stories/2006/07/24/daily30.html***. *See also* Identity Theft Resource Center, Fact Sheet 126: *Checking Account Takeover and Check Fraud*, ***http://www.idtheftcenter.org/vg126.shtml***.

25. For example, the Securities and Exchange Commission instituted proceedings against a 19-year-old internet hacker after the hacker illicitly accessed an investor's online brokerage account. His bogus transactions saved the hacker approximately $37,000 in trading losses. The SEC also obtained an emergency asset freeze to halt an Estonia-based "account intrusion" scheme that targeted online brokerage accounts in the U.S. to manipulate the markets. *See* Litigation Release No. 19949 (Dec. 19, 2006), available at ***http://www.sec.gov/litigation/litreleases/2006/lr19949.htm***.

26. For unauthorized credit card charges, the Fair Credit Billing Act limits consumer liability to a maximum of $50 per account. 15 U.S.C. § 1643. For bank account fraud, different laws determine consumers' legal remedies based on the type of fraud that occurred. For example, applicable state laws protect consumers against fraud committed by a thief using paper documents, like stolen or counterfeit checks. If, however, the thief used an electronic fund transfer, federal law applies. The Electronic Fund Transfer Act limits consumer liability for unauthorized transactions involving an ATM or debit card, depending on how quickly the consumer reports the loss or theft of his card: (1) if reported within two business days of discovery, the consumer's losses are limited to a maximum of $50; (2) if reported more than two business days after discovery, but within 60 days of the transmittal date of the account statement containing unauthorized transactions, he could lose up to $500; and (3) if reported more than 60 days after the transmittal date of the account statement containing unauthorized transactions, he could face unlimited liability. 15 U.S.C. § 1693g. As a matter of policy, some credit and debit card companies waive liability under some circumstances, freeing the consumer from fraudulent use of his credit or debit card.

27. *See* John Leland, *Some ID Theft Is Not For Profit, But to Get a Job*, N.Y. Times, Sept. 4, 2006.

28. *See* World Privacy Forum, *Medical Identity Theft: The Information Crime That Can Kill You* (May 3, 2006), available at ***worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf***.

29. *See* ***http://www.idanalytics.com/news_and_events/20051208.htm***. Some other organizations have begun conducting statistical analyses to determine the link between data breaches and identity theft. These efforts are still in their early stages, however.

30. Government Accounting Office, *Social Security Numbers: Government Could Do More to Reduce Display in Public Records and On Identity Cards* (November 2004), at 2, available at ***http://www.gao.gov/new.items/d0559.pdf***.

31. 15 U.S.C. §§ 6801 et seq.; 42 U.S.C. §§ 1320d et seq.; 18 U.S.C. §§ 2721 et seq.

32. 5 U.S.C. § 552a.

33. *See*, *e.g.*, Ariz. Rev. Stat. § 44-1373.

34. *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, Yet Gaps Remain*, GAO - 05-1016T, September 15, 2005.

35. *See, e.g.*, ***www.wpsic.com/edi/comm_sub_p.shtml?mm=3***, *Non-SSN Member Numbers to Be Assigned for Privacy Protection*.

36. Except where expressly noted, all references to years in this strategic plan are intended to refer to calendar years, rather than fiscal years.

37. The federal government's overall information privacy program derives primarily from five statutes that assign OMB policy and oversight responsibilities, and agencies responsibility for implementation. The Privacy Act of 1974 (5 U.S.C. § 552a) sets collection, maintenance, and disclosure conditions; access and amendment rights and notice and record-keeping requirements with respect to personally identifiable information retrieved by name or personal identifier. The Computer Matching and Privacy Protection Act of 1988 (5 U.S.C. § 552a note) amended the Privacy Act to provide a framework for the electronic comparison of personnel and benefits-related information systems. The Paperwork Reduction Act of 1995 (44 U.S.C. § 3501 et seq.) and the Information Technology Management Reform Act of 1996 (also known as Clinger-Cohen Act; 41 U.S.C. § 251 note) linked agency privacy activities to information technology and information resources management, and assigned to agency Chief Information Officers (CIO) the responsibility to ensure implementation of privacy programs within their respective agencies. Finally, Section 208 of the E-Government Act of 2002 (44 U.S.C. § 3501 note) included provisions requiring agencies to conduct privacy impact assessments on new or substantially altered information technology systems and electronic information collections, and post web privacy policies at major entry points to their Internet sites. These provisions are discussed in OMB memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002."

38. *See Protection of Sensitive Agency Information*, Memorandum from Clay Johnson III, Deputy Director for Management, OMB, to Heads of Departments and Agencies, M-06-16 (June 23, 2006).

39. The United States Computer Emergency Readiness Team (US-CERT) has played an important role in public sector data security. US-CERT is a partnership between DHS and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. The organization interacts with federal agencies, state and local governments, industry professionals, and others to improve information sharing and incident response coordination and to reduce cyber threats and vulnerabilities. US-CERT provides the following support: (1) cyber security event monitoring; (2) advanced warning on emerging threats; (3) incident response capabilities for federal and state agencies; (4) malware analysis and recovery support; (5) trends and analysis reporting tools; and (6) other support services in the area of cyber security. US-CERT also provides consumer and business education on Internet and information security.

40. *See* ***http://www.whitehouse.gov/results/agenda/scorecard.html.***

41. The proposed routine use language set forth in Appendix B differs slightly from that included in the Task Force's interim recommendations in that it further clarifies, among other things, the categories of users and the circumstances under which disclosure would be "necessary and proper" in accordance with the OMB's guidance on this issue.

42. 15 U.S.C. §§ 6801-09; 16 C.F.R. Part 313 (FTC); 12 C.F.R. Part 30, App. B (OCC, national banks); 12 C.F.R. Part 208, App. D-2 and Part 225, App. F (FRB, state member banks and holding companies); 12 C.F.R. Part 364, App. B (FDIC, state non-member banks); 12 C.F.R. Part 570, App. B (OTS, savings associations); 12 C.F.R. Part 748, App. A (NCUA, credit unions); 16 C.F.R. Part 314 (FTC, financial institutions that are not regulated by the FRB, FDIC, OCC, OTS, NCUA, CFTC, or SEC); 17 C.F.R. Part 248.30 (SEC); 17 C.F.R. Part 160.30 (CFTC).

43. 15 U.S.C. § 45(a). Further, the federal bank regulatory agencies have authority to enforce Section 5 of the FTC Act against entities over which they have jurisdiction. *See* 15 U.S.C. §§ 6801-09.

44. 15 U.S.C. §§ 1681-1681x, as amended.

45. Pub. L. No. 108-159, 117 Stat. 1952.

46. 42 U.S.C. §§ 1320d et seq.

47. 31 U.S.C. § 5318(l).

48. 18 U.S.C. §§ 2721 et seq.

49. ***http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm***.

50. ***http://www.bbb.org/securityandprivacy/SecurityPrivacyMadeSimpler.pdf***;***www.staysafeonline.org/basics/company/basic_tips.html***; *The Financial Services Roundtable, Voluntary Guidelines for Consumer Confidence in Online Financial Services*, available at ***www.bitsinfo.org/downloads/Publications%20Page/bitsconscon.pdf***; ***www.realtor.org/realtororg.nsf/files/NARInternetSecurityGuide.pdf/$FILE/NARInternetSecurityGuide.pdf***; ***www.antiphishing.org/reports/bestpracticesforisps.pdf***; ***www.uschamber.com/sb/security/default.htm***; ***www.truste.org/pdf/SecurityGuidelines.pdf***; ***www.the-dma.org/privacy/informationsecurity.shtml***; ***http://www.staysafeonline.org/basics/company/basic_tips.html***.

51. These changes may be attributable to requirements contained in the regulations implementing Title V of the GLB Act. *See* 12 C.F.R. Part 30, App. B (national banks); 12 C.F.R. Part 208, App. D-2 and Part 225, App. 5 (state member banks and holding companies); 12 C.F.R. Part 364, App. B (state non-member banks); 12 C.F.R. Part 570, App. B (savings associations); 12 C.F.R. Part 748, App. A and B, and 12 C.F.R. Part 717 (credit unions); 16 C.F.R. Part 314 (financial institutions that are not regulated by the FDIC, FRB, NCUA, OCC, or OTS).

52. *See*, *e.g.*, ***http://www.truste.org/pdf/SecurityGuidelines.pdf***; ***http://www.the-dma.org/privacy/informationsecurity.shtml***.

53. Deloitte Financial Services, *2006 Global Security Survey*, available at ***http://singe.rucus.net/blog/archives/756-Deloitte-Security-Surveys.html.***

54. Datalink, *Data Storage Security Study*, March 2006, available at ***www.datalink.com/security/.***

55. *Id*.

56. *See* Small Business Technology Institute, *Small Business Information Security Readiness* (July 2005).

57. *See*, *e.g.*, California (Cal. Civ. Code § 1798.82 (2006)); Illinois (815 Ill. Comp. Stat 530/5 (2005)); Louisiana (La. Rev. Stat. 51:3074 (2006)); Rhode Island (R.I. Gen. Laws § 11-49.2.3 (2006)).

58. *See*, *e.g.*, Colorado (Colo. Rev. Stat. § 6-1-716 (2006)); Florida (Fla. Stat. § 817.5681 (2005)); New York (NY CLS Gen. Bus. § 889-aa (2006)); Ohio (Ohio Rev. Code Ann. § 1349.19 (2006)).

59. Ponemon Institute LLC, *Benchmark Study of European and U.S. Corporate Privacy Practices*, p. 16 (Apr. 26, 2006).

60. *Id.*

61. Ponemon Institute, LLC, 2005 *Benchmark Study of Corporate Privacy Practices* (July 11, 2005).

62. MultiChannel Merchant, *Retailers Need to Provide Greater Data Security, Survey Says* (Dec. 1, 2005), available at ***http://multichannelmerchant.com/opsandfulfillment/advisor/retailers_data_security_1201/index.html***.

63. *See* Information Technology Examination Handbook's Information Security Booklet, available at ***http://www.ffiec.gov/guides.htm***.

64. *See*, *e.g.*, ***http://www.pvkansas.com/police/crime/iden_theft.shtml*** (Prairie Village, Kansas), ***http://phoenix.gov//POLICE/dcd1.html*** (Phoenix, Arizona); ***www.co.arapahoe.co.us/departments/SH/index.asp*** (Arapahoe County, Colorado).

65. *Colleges Are Textbook Cases of Cybersecurity Breaches*, USA TODAY, August 1, 2006.

66. Examples of this outreach include a wide-scale effort at the University of Michigan which launched Identity Web, a comprehensive site based on the recommendations of a graduate class in fall of 2003. The State University of New York's Orange County Community College offers identity theft seminars, the result of a student who fell victim to a scam. A video at student orientation sessions at Drexel University in Philadelphia warns students of the dangers of identity theft on social networking sites. Bowling Green State University in Kentucky emails campus-wide "fraud alerts" when it suspects that a scam is being targeted to its students. In recent years, more colleges and universities have hired chief privacy officers, focusing greater attention on the harms that can result from the misuse of students' information.

67. *See* 31 C.F.R. § 103.121 (banks, savings associations, credit unions, and certain non-federally regulated banks); 31 C.F.R. § 103.122 (broker-dealers); 17 C.F.R. § 270.0-11, 31 C.F.R. § 103.131 (mutual funds); and 31 C.F.R. § 103.123 (futures commission merchants and introducing brokers).

68. *See* ***http://www.dhs.gov/xprevprot/laws/gc_1172765386179.shtm***.

69. A primary reason criminals use other people's identities to commit identity theft is to enable them to operate with anonymity. However, in committing identity theft, the suspects often leave telltale signs that should trigger concern for alert businesses. Section 114 of the FACT Act seeks to take advantage of businesses' awareness of these patterns, and requires the federal bank regulatory agencies and the FTC to develop regulations and guidelines for financial institutions and creditors addressing identity theft. In developing the guidelines, the agencies must identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. 15 U.S.C. § 1681m.

    Those agencies have issued a set of proposed regulations that would require each financial institution and creditor to develop and implement an identity theft prevention program that includes policies and procedures for detecting, preventing, and mitigating identity theft in connection with account openings and existing accounts. The proposed regulations include guidelines listing patterns, practices, and specific forms of activity that should raise a "red flag" signaling a possible risk of identity theft. Recognizing these "red flags" can enable businesses to detect identity theft at its early stages before too much harm is done. *See* 71 Fed. Reg. 40786 (July 18, 2006) to be codified at 12 C.F.R. Parts 41 (OCC), 222 (FRB), 334 and 364 (FDIC), 571 (OTS), 717 (NCUA), and 16 C.F.R. Part 681 (FTC), available at ***http://www.occ.gov/fr/fedregister/71fr40786.pdf***.

70. USB token devices are typically small vehicles for storing data. They are difficult to duplicate and are tamper-resistant. The USB token is plugged directly into the USB port of a computer, avoiding the need for any special hardware on the user's computer. However, a login and password are still required to access the information contained on the device. Smart cards resemble a credit card and contain a microprocessor that allows them to store and retain information. Smart cards are inserted into a compatible reader and, if recognized, may require a password to perform a transaction. Finally, the common token system involves a device that generates a one-time password at predetermined intervals. Typically, this password would be used in conjunction with other login information such as a PIN to allow access to a computer network. This system is frequently used to allow for remote access to a work station for a telecommuter.

71. Biometrics are automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics. Biometrics commonly implemented or studied include: fingerprint, face, iris, voice, signature, and hand geometry. Many other modalities are in various stages of development and assessment. Additional information on biometric technologies, federal biometric programs, and associated privacy considerations can be found at ***www.biometrics.gov***.

72. *See Authentication in an Internet Banking Environment* (October 12, 2005), available at ***http://www.ffiec.gov/pdf/authentication_guidance.pdf***.

73. *See* FFIEC Frequently Asked Questions on *FFIEC Guidance on Authentication in an Internet Banking Environment* (August 15, 2006), available at ***http://www.ffiec.gov/pdf/authentication_faq.pdf***.

74. *See* Kristin Davis and Jessica Anderson, *But Officer, That Isn't Me*, Kiplinger's Personal Finance (October 2005); Bob Sullivan, *The Darkest Side of ID Theft*, MSNBC.com (Dec. 1, 2003); David Brietkopf, *State of Va. Creates Special Cards for Crime Victims*, The American Banker (Nov. 18, 2003).

75. 18 U.S.C. § 1028A.

76. 18 U.S.C. § 1028(d)(7).

77. *See* 18 U.S.C. § 1030(e)(8).

78. 18 U.S.C. § 1030(a)(7).

79. S. Rep. No. 105-274, at 9 (1998).

80. As this Task Force has been charged with considering the federal response to identity theft, this routine use notice does not include all possible triggers, such as embarrassment or harm to reputation. However, after consideration of the Strategic Plan and the work of other groups charged with assessing Privacy Act considerations, OMB may determine that a routine use that takes into account other possible triggers may be preferable.