The President's Identity Theft Task Force

COMBATING IDENTITY THEFT

A STRATEGIC PLAN

Exhibit I

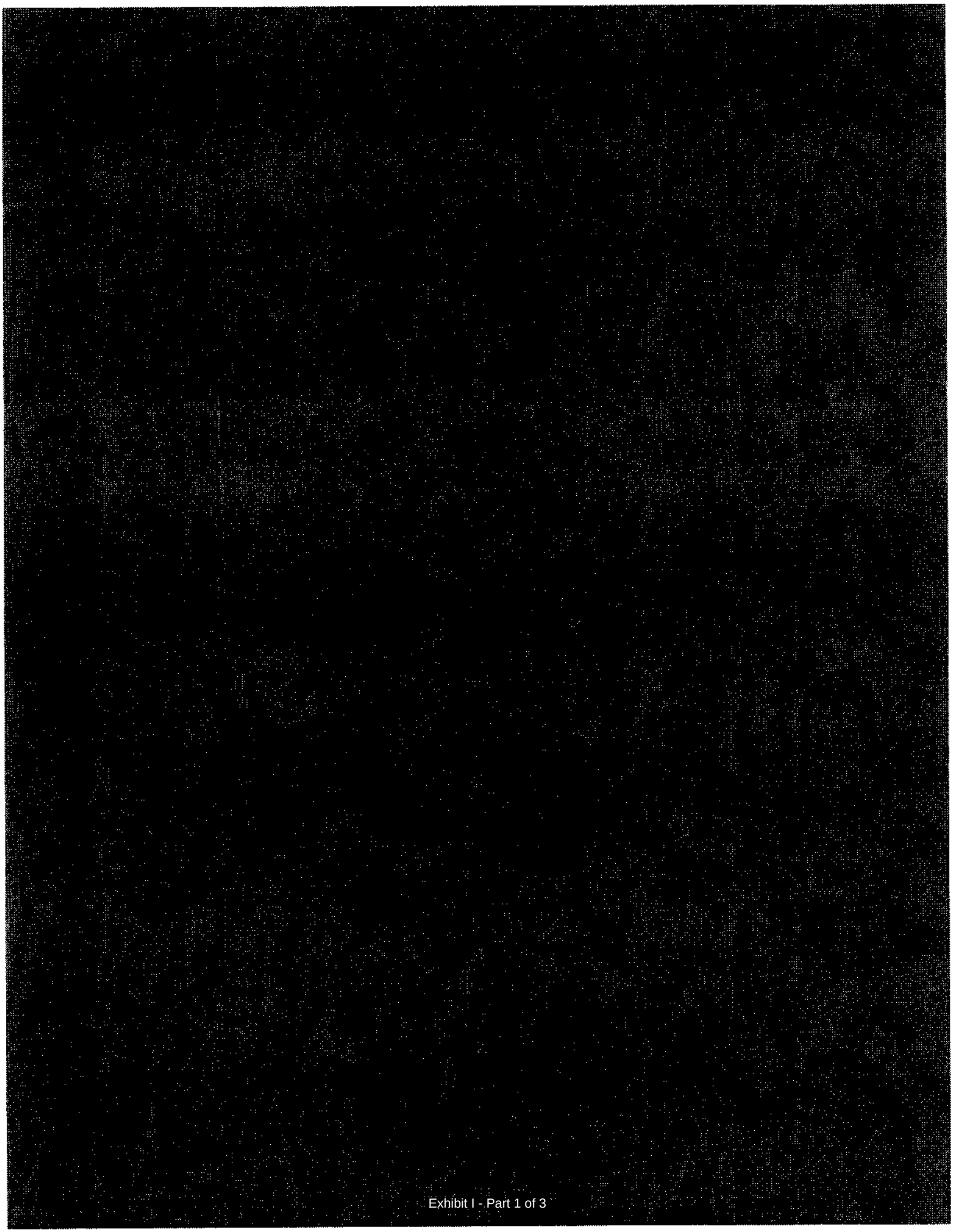


Exhibit I - Part 1 of 3

Table of Contents

APPENDICES

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

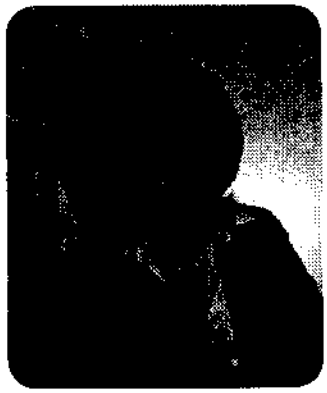
JoAnn Johnson
National Credit Union Administration

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

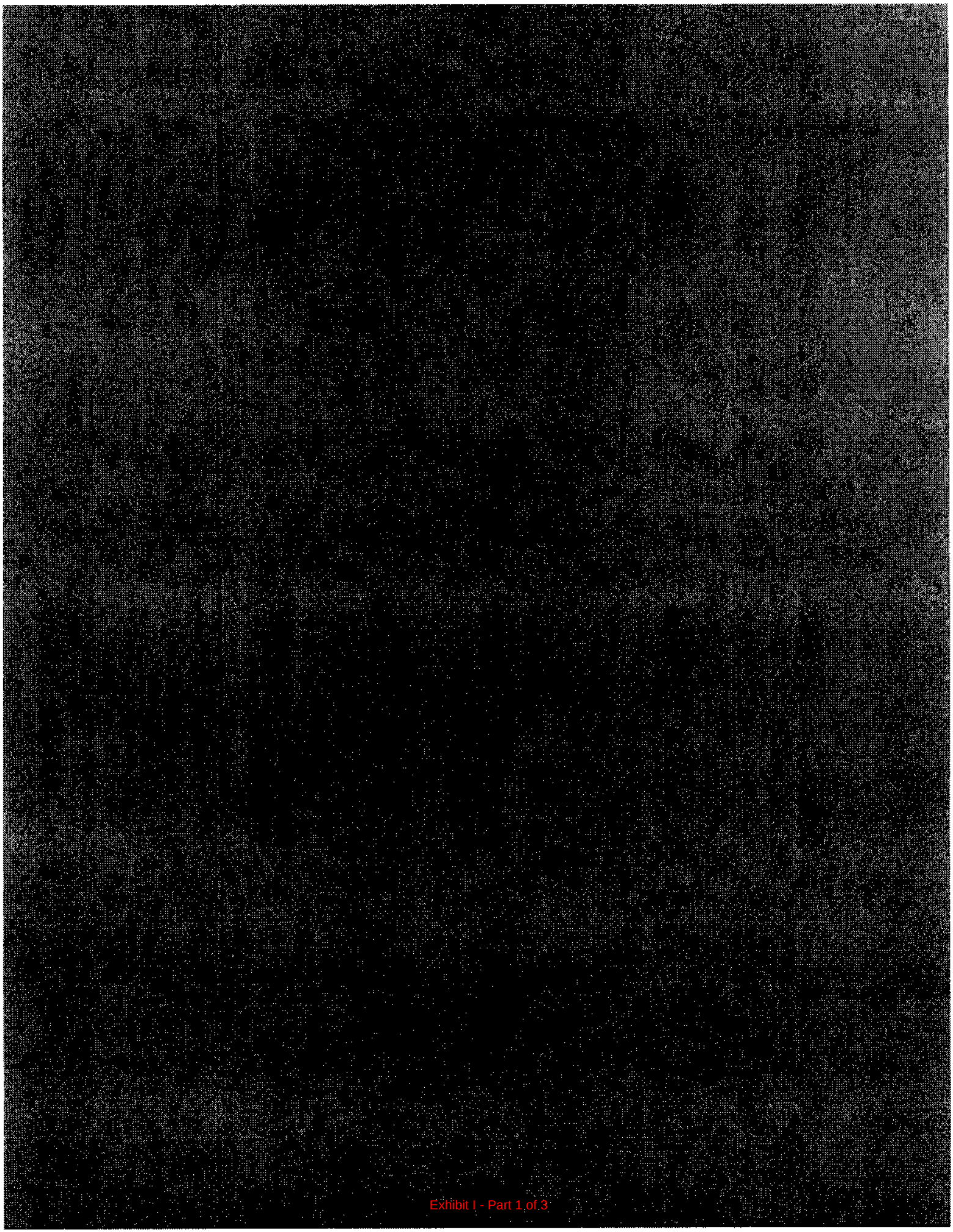


Exhibit I - Part 1 of 3

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.

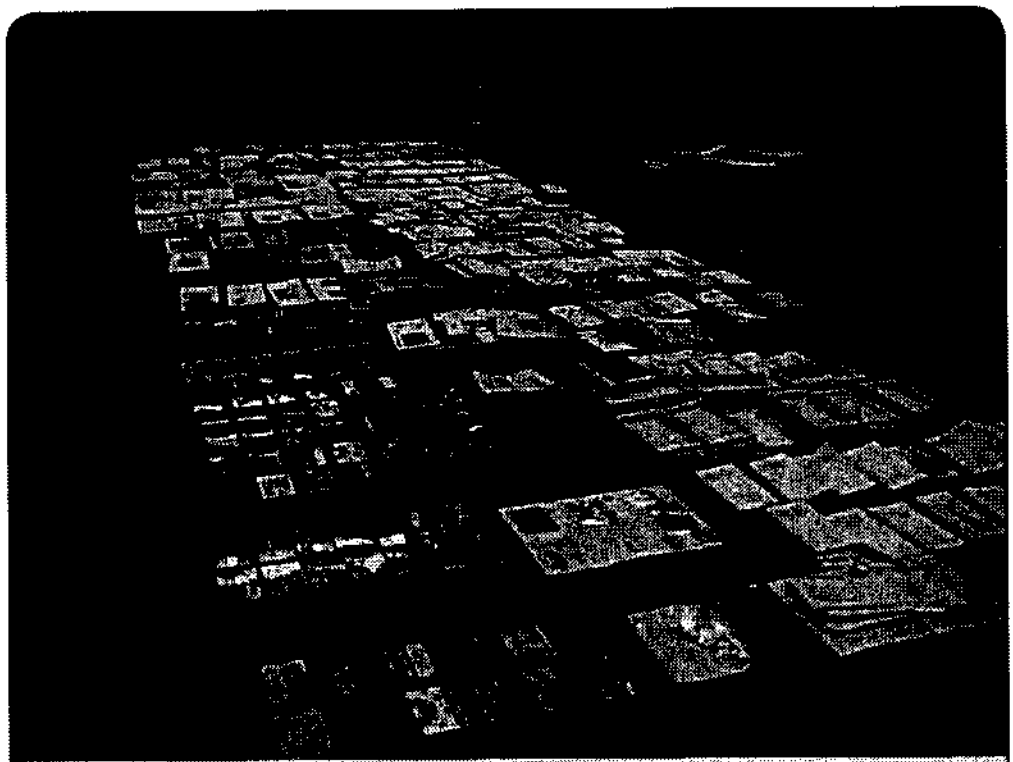
thieves use more technologically-advanced means to extract information from computers, including malicious-code programs that secretly log information or give criminals access to it.

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.