The President's Identity Theft Task Force

Combating Identity Theft

Volume II: Supplemental Information

April 2007

Table of Contents

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

PART A

FEDERAL LAWS AND REGULATIONS RELATED TO DATA SECURITY

Although there is no single comprehensive federal data security law, a number of federal laws, regulations, and guidelines relate to and protect consumer information. Each of these laws and regulations provides specific remedies that can be sought by the agencies with enforcement authority. Significant examples include:

TITLE V OF THE GRAMM-LEACH-BLILEY ACT (GLB Act), 15 U.S.C. §§ 6801-09

The GLB Act addresses privacy and security obligations of "financial institutions." Financial institutions are defined broadly as those entities engaged in "financial activities" such as banking, lending, insurance, loan brokering, and credit reporting. 12 C.F.R. §§ 225.28, 225.86. The GLB Act addresses two distinct types of protection for personal information: protection of security and protection of privacy. Various federal agencies, including the federal bank regulatory agencies, the Federal Trade Commission (FTC), and the Securities and Exchange Commission (SEC), have issued regulations or guidelines addressing both the security and privacy provisions of the GLB Act. The security provisions require the agencies to write standards for financial institutions regarding appropriate physical, technical, and procedural safeguards to ensure the security and confidentiality of customer records and information, and to protect against anticipated threats and unauthorized access to such information. The privacy provisions require financial institutions to give notice to their customers of their information-sharing practices and provide customers with an opportunity to opt out of information-sharing with certain unaffiliated third parties in certain circumstances.

REMEDIES: The specific remedies available to each agency are listed below.

▶ Interagency Guidelines Establishing Information Security Standards ("Interagency Security Guidelines")

The Interagency Security Guidelines, jointly issued by the federal bank regulatory agencies in 2001, require each financial institution under their jurisdiction to have a written information security program designed to meet the statutory objectives of Title V of the GLB Act and Section 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) regarding disposal of consumer information derived from consumer reports.[1] *See* 12 C.F.R. Part 30, App. B (national banks); 12 C.F.R. Part 208, App. D-2 and Part 225, App. F (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 (credit unions). Under the guidelines, the institution's board of directors must approve the program and oversee its

development, implementation, and maintenance. The institution also must assess the risks to its customer information, identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure or misuse of its customer information, and assess the likelihood and potential damage of these threats, taking into account the institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. Each of the requirements in the guidelines regarding proper disposal of customer information also applies to the disposal of consumer information.

The institution must then design its information security program to control the identified risks. The guidelines stipulate certain minimum specific security measures that should be considered and adopted if appropriate to the institution's risk profile. These measures include access controls on customer information systems, encryption of electronic customer information, monitoring systems to detect actual and attempted attacks on customer information systems, and response programs that specify actions to be taken when an institution suspects or detects unauthorized access to customer information.

Each institution must also train staff to implement the program and oversee its arrangements with service providers that have access to its customer information. This includes using due diligence in selecting service providers, requiring by contract that service providers implement appropriate safeguard measures that satisfy the guidelines, and monitoring the activities of service providers, where necessary, to control the risks the institution has identified that may be posed by the service provider's access to the institution's customer information.

An institution's information security program must be dynamic. Institutions must routinely test their systems and address any weaknesses they discover. Institutions must adjust their programs to address new threats to customer information, changes in technology, and new business arrangements.

REMEDIES: The federal bank regulatory agencies have comprehensive supervision and examination authority over banks, savings associations, and credit unions, and are well positioned to detect violations of law, ensure compliance, and apply sanctions appropriate to the nature and severity of any violation of law or regulation. The bank regulatory agencies have a well-established arsenal of enforcement tools under sections 8 and 39 of the Federal Deposit Insurance Act (FDI Act) and sections 206 and 216 of the Federal Credit Union Act (FCU Act), ranging from informal to formal actions. Depending on the level of severity of a violation, an agency may choose to cite an institution for a violation, but forego formal action where management quickly remedies the situation. In other circumstances, formal, public actions are warranted and the regulators may seek civil penalties, restitution, and cease and desist orders.

▶ Interagency Guidance on Authentication in an Internet Banking Environment ("Interagency Authentication Guidance")

The Interagency Authentication Guidance, jointly issued by the federal bank regulatory agencies in 2005, states that financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services. In the guidance, the federal bank regulatory agencies state that financial institutions should use effective risk-based methods to authenticate the identity of customers using their products and services. Single-factor authentication, as the only control mechanism, is considered inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Financial institutions are encouraged to implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

REMEDIES: The guidance describes practices that the federal bank regulatory agencies consider to be safe and sound. The agencies may take enforcement action under section 8 of the FDI Act and section 206 of the FCU Act against an institution that engages in unsafe and unsound conduct.

▶ FTC Standards for Safeguarding Customer Information ("Safeguards Rule"), 16 C.F.R. Part 314

The FTC's Safeguards Rule applies to a wide variety of "financial institutions" that are not subject to the jurisdiction of other federal or state authorities under the GLB Act. Among the institutions that fall under the Safeguards Rule are non-bank mortgage lenders, loan brokers, some state-regulated financial or investment advisers, tax preparers, providers of real estate settlement services, and debt collectors. The FTC's regulation applies only to companies that are "significantly engaged" in such financial activities.

Like the Interagency Security Guidelines, the Safeguards Rule requires financial institutions to develop a written information security plan that describes their procedures to protect customer information. Further, the Rule requires covered entities to take certain procedural steps, including: (1) assigning employees to oversee the program; (2) conducting a risk assessment; (3) designing and implementing an information safeguards program; (4) contractually requiring service providers to protect customers' information; and (5) evaluating and adjusting the program in light of relevant circumstances. However, given the wide variety of entities (large and small) that are covered, the Rule mandates a data security plan that accounts for each entity's particular circumstances, including its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

REMEDIES: The FTC can seek injunctive relief and other equitable remedies, including consumer redress or disgorgement in appropriate cases.

▶ SEC Regulation S-P, 17 C.F.R. Part 248

In June 2000, the SEC adopted Regulation S-P, which implements the GLB Act's Title V information privacy and safeguarding requirements for securities brokers and dealers, investment companies, and SEC-registered investment advisers. *See* 65 Fed. Reg. 40334 (June 29, 2000). Regulation S-P contains rules of general applicability that are substantively similar to the financial privacy rules adopted by the FTC and the federal bank regulatory agencies. In addition to providing general guidance, Regulation S-P contains numerous examples specific to the securities industry to provide more meaningful guidance to help firms implement its requirements. It also includes a section regarding procedures to safeguard information, including the disposal of consumer report information. *See* 17 CFR 248.30. This section requires securities firms to adopt written policies and procedures that address administrative, technical, and physical safeguards that are reasonably designed to: (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security and integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

In a public statement released in September 2004, the SEC stated that in large and complex organizations, with thousands of employees and multiple offices, written policies and procedures to safeguard customers' records and information generally address procedures at several levels, going from an organization-wide policy statement down to detailed procedures addressing particular controls. *See* Disposal of Consumer Report Information, Release Nos. 34-50361, IA-2293, IC-26596 (Sept. 14, 2004). More specifically, the SEC stated that at one level, the highest levels of management approve an organization-wide policy statement. At another level, more specific policies and procedures address separate areas of safeguarding risk. At a final level, detailed procedures set out the controls, management checks and balances, audit trail functions, and other actions needed to ensure that the firm's safeguarding program is reasonably effective and verifiable by senior management. These written policies and procedures also generally designate a specialized staff of information security professionals to manage the organization's day-to-day safeguarding operations, and an information security governance framework, to ensure that the information security policy is adequately supported throughout the enterprise. Finally, these written policies and procedures generally make provision for measures to verify the safeguarding program's effectiveness, including risk assessments, independent audits and penetration tests, as well as active monitoring, surveillance, and detection programs. The SEC stated that this comprehensive approach to safeguarding is consistent with widely accepted standards adopted by

government and private sector standard-setting bodies and professional literature and generally leads to reasonable written policies and procedures.

REMEDIES: A violation of Regulation S-P can result in supervisory action, such as a deficiency letter. In addition, the Commission has authority to initiate enforcement proceedings for violations of Regulation S-P under the Securities Exchange Act of 1934, the Investment Company Act of 1940, and the Investment Advisers Act of 1940. Violations of regulations under these acts can result in injunctive relief, civil penalties, or in some cases, imprisonment. Failure to honor a commitment to a customer also may constitute a violation of a rule of a self-regulatory organization, such as National Association of Securities Dealers (NASD) Rule 2110, which requires adherence to "high standards of commercial honor and just and equitable principles of trade."

▶ Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("Incident Response Guidance")

In 2005, the federal bank regulatory agencies also issued guidance for banks, savings associations, and credit unions, relating to breach notification. *See* 12 C.F.R. Part 30, Supp. A to App. B (national banks); 12 C.F.R. Part 208, Supp. A to App. D-2 and Part 225, Supp. A to App. F (state member banks and holding companies); 12 C.F.R. Part 364, Supp. A to App. B (state non-member banks); 12 C.F.R. Part 570, Supp. A to App. B (savings associations); 12 C.F.R. 748, App. B (credit unions). The guidance states that each of these financial institutions should develop and implement a response program to address incidents of unauthorized access to or use of customer information maintained by or on behalf of the institution as part of the information security program required by the Interagency Security Guidelines. The program must contain procedures for: (1) assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused; (2) notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information; (3) notifying appropriate law enforcement authorities, in addition to filing a timely Suspicious Activities Report, in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing; (4) taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and (5) notifying customers when warranted.

The Incident Response Guidance also describes when and how a financial institution should provide notice to customers affected by unauthorized access or misuse of sensitive customer information. In particular, it indicates that

once the institution becomes aware of an incident of unauthorized access to "sensitive customer information" as defined in the guidance, it should conduct a reasonable investigation to determine promptly the likelihood that the information has been or will be misused. If the institution determines that misuse of customer information has occurred or is reasonably possible, it should notify any affected customer as soon as possible.

Such notice should be given in a clear and conspicuous manner, and it should include a description of the incident, the type of customer information affected, the steps taken to protect the customers' information from further unauthorized access, a telephone number that customers can call for further information and assistance, and other information as appropriate to the situation. The guidance also makes clear that an institution remains responsible for protecting customer information in the hands of a service provider and that it, by contract, should require the service provider to take appropriate actions to address incidents of unauthorized access to the institution's customer information, including notifying the institution of security breaches involving the institution's customer information.

REMEDIES: The guidance represents the federal bank regulatory agencies' interpretation of the standards set out in the Interagency Security Guidelines described above. Remedies for breaches are discussed in that section. In addition, the guidance describes practices that the federal bank regulatory agencies consider to be safe and sound. The agencies may take enforcement action under section 8 of the FDI Act and section 206 of the FCU Act against an institution that engages in unsafe and unsound conduct.

▶ Privacy of Consumer Financial Information ("Privacy Rule")

The Privacy Rule, issued by the federal bank regulatory agencies and the FTC, implements the privacy provisions of the GLB Act with respect to financial institutions under their respective jurisdictions. 16 C.F.R. Part 313 (FTC); 12 C.F.R. Parts 40 (OCC), 216 (FRB), 332 (FDIC), 573 (OTS), and 716 (NCUA). Subject to certain exceptions, it prohibits financial institutions from disclosing nonpublic personal information to non-affiliated third parties without first providing consumers with notice and the opportunity to opt out of the disclosure. The notice and opt out must be provided no later than when a customer relationship arises and annually for the duration of that relationship, or at a reasonable time before the disclosure in the case of non-customers. The notice must be "a clear and conspicuous notice that accurately reflects [the financial institution's] privacy policies and practices" including policies and practices related to security.

REMEDIES: Pursuant to the FTC Act, the FTC can seek injunctive relief, as well as consumer redress or disgorgement in appropriate cases. The GLB Act provides that the regulations may be enforced by the federal bank regulatory agencies under section 8 of the FDI Act and section 206 of the FCU Act, which are discussed in detail above under "Interagency Security Guidelines."

FAIR CREDIT REPORTING ACT (FCRA), 15 U.S.C. §§ 1681-1681X, as amended by the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), Pub. L. No. 108-159, 117 Stat. 1952

The FCRA contains requirements designed to protect the privacy of consumer report information, which includes account, credit history, and employment information. Under the FCRA, consumer reporting agencies are prohibited from distributing consumer reports except for specified "permissible purposes." These entities must maintain reasonable procedures to ensure that they provide consumer reports only for such purposes, such as by verifying the identities of persons obtaining consumer reports and their intended use of the information. The FACT Act amendments to the FCRA added a number of new requirements, many of which have been or are being implemented through rulemaking. Several of these new requirements are intended to prevent identity theft or assist victims in the recovery process. The rules most relevant to data security are discussed below.[2]

REMEDIES: The FCRA allows for both monetary relief, including civil penalties, and injunctive relief for violations of the Act, 15 U.S.C. § 1681s, and provides for criminal sanctions against those who infringe on consumer privacy by unlawfully obtaining consumer reports. The FCRA and its implementing regulations may be enforced by the federal bank regulatory agencies under section 8 of the FDI Act and section 206 of the FCU Act, which are discussed in detail above under "Interagency Security Guidelines."

▶ Disposal of Consumer Report Information and Record Rule ("Disposal Rule")

The FACT Act amended the FCRA to include a number of provisions designed to increase the protection of sensitive consumer information. One such provision required the financial regulatory agencies and the FTC to promulgate a coordinated rule designed to prevent unauthorized access to consumer report information by requiring all users of such information to have reasonable procedures to dispose of it properly. This Disposal Rule took effect on June 1, 2005.

The Rule applies to any entity that maintains consumer reports or information derived from consumer reports. The Rule does not address *when* entities must dispose of such information, but rather *how* they must dispose of it: by using disposal practices that are reasonable and appropriate to prevent the unauthorized access to or use of information in a consumer report. The standard is flexible and allows the organizations and individuals covered by the Rule to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology. For the federal bank regulatory agencies, these requirements are included in their Interagency Security Guidelines. The SEC's disposal rule requirements are included in the SEC's Regulation S-P (17 C.F.R. § 248.30(b)).

REMEDIES: All remedies available under the FCRA (see above) and remedies available for violation of the SEC's Regulation S-P (see above).

▶ Identity Theft Red Flags and Address Discrepancies Rule under the FACT Act ("Red Flags Rule"), Pub. L. No. 108-159, 117 Stat. 1952, Sections 114 and 315. (Proposed)

On July 18, 2006, the financial regulatory agencies and the FTC issued a notice of proposed rulemaking for the Red Flags Rule, a new regulation designed to reduce identity theft. The regulations would require every financial institution and creditor to develop and implement a written 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 program must be risk-based and tailored to the size and complexity of each financial institution or creditor and the nature and scope of its activities. Credit card and debit card issuers must develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card.

In addition, as required by statute, the proposed regulations require users of consumer reports to develop reasonable policies and procedures regarding notices of address discrepancies they receive from a consumer reporting agency (CRA). If a user of a consumer report receives notice from a CRA that the address a consumer has provided to obtain the report "substantially differs" from the consumer's address in the CRA's file, the user must reasonably confirm as accurate an address for the consumer and provide it to the CRA.

REMEDIES: All remedies available under the FCRA. (See above.)

FEDERAL TRADE COMMISSION ACT (FTC Act), 15 U.S.C. § 45(a)

The FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce" and gives the FTC broad jurisdiction over a wide variety of entities and individuals operating in commerce. Prohibited deceptive practices include making false or misleading claims about the privacy and security provided for consumer information. The FTC Act also prohibits unfair practices, including unfair practices affecting consumer data. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition. The FTC has used this authority to challenge a variety of injurious practices, including companies' failure to provide reasonable and appropriate security for sensitive consumer data such as Social Security numbers (SSNs) and financial account information. (*See* discussion of enforcement actions below.) The federal bank regulatory agencies have also enforced Section 5 of the FTC Act against financial institutions under their jurisdiction.

REMEDIES: Injunctive relief, affirmative conduct requirements, and consumer redress or disgorgement of ill-gotten gains in appropriate cases. The FTC Act may be enforced by the federal bank regulatory agencies under section 8 of the FDI Act and section 206 of the FCU Act, which are discussed in detail above under "Interagency Security Guidelines."

CUSTOMER IDENTIFICATION PROGRAM RULES Implementing Section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) , 31 U.S.C. § 5318(l)

Banks, savings associations, credit unions, broker-dealers, mutual funds, and futures commission merchants are required to follow verification procedures under rules issued by the federal bank regulatory agencies, the Department of Treasury, the CFTC, and the SEC under section 326 of the USA PATRIOT Act. The implementing rules require every covered entity to design and implement a customer identification program (CIP) that includes policies and procedures for verifying the identity of a person opening a new account. While the primary purpose of the regulations implementing the USA PATRIOT Act was to deter terrorist financing and money laundering, the CIP regulations also play a role in preventing identity theft.

REMEDIES: The Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) has authority to assess penalties against financial institutions that violate this regulation. The regulation also is enforced by the federal bank regulatory agencies under section 8 of the FDI Act and section 206 of the FCU Act, which are discussed in detail above under "Interagency Security Guidelines." The SEC examines mutual funds, and the SEC and relevant self-regulatory organizations examine broker-dealers, for compliance with the regulation and may also bring enforcement actions depending on the circumstances. The CFTC has similar authority for futures commission merchants.

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA), 42 U.S.C. § 1320d et seq.

HIPAA and the implementing Privacy Rule prohibit covered entities (including health plans, healthcare clearinghouses, and certain healthcare providers) from disclosing to third parties an individual's protected health information without prior authorization, subject to some exceptions, such as the disclosure of patient records by covered entities for purposes of routine treatment, insurance, payment or, in limited circumstances, credit reporting relating to account information. 45 C.F.R. Part 160 and Subparts A and E of Part 164 ("HIPAA Privacy Rule"). Like the GLB Act Safeguards Rule, the

HIPAA Privacy Rule requires covered entities under its jurisdiction to have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c). The HIPAA Security Rule similarly seeks to protect the confidentiality, integrity, and availability of electronic protected health information by specifying a series of administrative, technical, and physical security procedures for covered entities to use to assure the security and confidentiality of electronic protected health information. 45 C.F.R. Part 160 and Subparts A and C of Part 164 ("HIPAA Security Rule").

REMEDIES: HIPAA allows for civil monetary penalties and criminal sanctions for violations under some circumstances.

THE DRIVERS PRIVACY PROTECTION ACT OF 1994 (DPPA), 18 U.S.C. §§ 2721-2725

The DPPA prohibits the disclosure of a driver's personal information (i.e., individual photograph, SSN, and driver identification number) obtained in connection with a motor vehicle record. The DPPA contains exceptions that allow for certain disclosures of such information, such as for use by an insurer or to provide notice to the owners of towed or impounded vehicles. The DPPA also prohibits an individual from knowingly obtaining a driver's personal information for a use not permitted under the Act, and from making a false representation to obtain any such information.

REMEDIES: For violations of the Act, the DPPA provides for criminal fines against individuals and/or State Departments of Motor Vehicles, civil penalties for violations by State Departments of Motor Vehicles, and a private right of action for individuals.

THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA), 20 U.S.C. § 1232g; 34 C.F.R. Part 99

FERPA protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records; these rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Under FERPA, a parent or an eligible student has the right to inspect and review the student's education records maintained by the school and to request that a school correct records that the parent or eligible student believes to be inaccurate or misleading. Furthermore, schools generally must have written permission from the parent or eligible student to release any information from a student's education record, subject to certain exceptions, such as disclosures to appropriate parties in connection with financial aid

to a student. Schools may disclose "directory" release information–including a student's name, address, telephone number, and date and place of birth–but must provide advance notice to parents and eligible students and allow them a reasonable amount of time to opt out of the disclosure.

REMEDIES: Institutions in violation of FERPA can be denied federal educational funding.

DEPARTMENT OF VETERANS AFFAIRS INFORMATION SECURITY ACT OF 2006, 38 U.S.C. §§ 5721-28

The Department of Veterans Affairs Information Security Enhancement Act of 2006 establishes a comprehensive information security program for the Department of Veterans Affairs (VA) and outlines requirements for the VA's response to data breaches. The Act provides that if it appears that VA sensitive information may have been compromised, and an independent data breach analysis determines that a reasonable risk of potential misuse exists, then the VA must offer credit protection services to the record subjects. The following credit protection services must be prescribed in VA regulations: notification of the record subjects, data mining, fraud alerts, data breach analyses, credit monitoring, identity theft insurance, and credit protection services. In addition, the VA must comply with Congressional notification requirements regarding data breaches. The Act requires all VA contracts in which the contractor will have access to VA sensitive information to contain provisions prohibiting the contractor from sharing the information with other entities except to perform the contract, requiring the contractor to report any data breaches to the agency, and requiring the contractor to pay liquidated damages to the VA for any data breach involving sensitive VA information.

PART B

ENFORCEMENT ACTIONS RELATING TO DATA SECURITY

Many federal agencies have taken aggressive enforcement actions in response to data security failures. Some of those actions are listed below.

Federal Bank Regulatory Agencies

The federal bank regulatory agencies have taken numerous enforcement actions against institutions for failure to have adequate programs to safeguard customer information. The FDIC took 17 formal enforcement actions between the beginning of 2002 and the end of 2006; the FRB has taken 14 formal enforcement actions in the past five years; the OCC has taken 18 formal actions since 2002; and the OTS has taken 8 formal enforcement actions in the past five years.

The following are just a few examples of the formal and informal actions taken by those agencies in recent years:

- A federal bank regulatory agency assessed civil money penalties against a subsidiary of a bank for improperly disposing of customer records.
- A federal bank regulatory agency issued a cease and desist order against a California-based financial institution, requiring, among other things, that the institution notify customers of security breaches, after the federal regulator's investigation revealed that the institution's service provider improperly disposed of hundreds of customer loan files. The regulator also issued a cease and desist order against the financial institution's service provider, and assessed hundreds of thousands of dollars in civil penalties against the financial institution and its service provider.
- A federal bank regulatory agency, after investigating allegations of a data compromise by a financial institution employee, directed a retail credit card bank to notify customers whose accounts or information may have been compromised. The regulator was able to determine that the information was used for nefarious purposes, after working collaboratively with the FTC to review complaints of identity theft made to the FTC through its Identity Theft Data Clearinghouse, with which the regulator is an information-sharing member. The financial regulator imposed on the employee a lifetime prohibition order from the banking industry and ordered him to pay a $25,000 civil penalty.
- A federal bank regulatory agency directed a large financial institution to improve its employee screening policies, procedures, systems, and controls after the regulator determined that the financial institution's employee screening practices had inadvertently permitted a convicted felon, who engaged in identity theft-related crimes, to gain employment

at the financial institution. Deficiencies in the institution's screening practices came to light through the regulator's review of the former employee's activities.

- In 2004, a federal bank regulatory agency's examination of a state-chartered bank disclosed significant computer system deficiencies and inadequate controls to prevent unauthorized access to customer information. The financial institution regulator issued an order directing the bank to develop and implement an information security program meeting the requirements of the Guidelines Establishing Information Security Standards. More specifically, the order required the bank to perform a formal risk assessment of internal and external threats that could result in unauthorized access to customer information, review computer user access levels to ensure that access was restricted to only those individuals with a legitimate business need to access the customer information, and review all other security controls to manage and control the risks to customer information.

The federal bank regulatory agencies also have taken dozens of enforcement actions against financial institution insiders who breached their duty of trust to customers, were engaged in identity theft-related activities, or were otherwise involved in serious breaches, compromises, or the misuse of customer information. These enforcement actions have included, for example, prohibiting individuals from working in the financial services industry, personal cease and desist orders restricting the use of customer information, the assessment of significant civil money penalties, and orders requiring restitution.

Securities and Exchange Commission (SEC)

Pursuant to the Regulation S-P standards, the SEC's staff has actively examined securities firms to determine whether they have policies and procedures reasonably designed to protect their customers from identity theft. Specifically, the SEC, along with the NASD and the New York Stock Exchange (NYSE), examines registered firms for Regulation S-P compliance by examining their operations and reviewing customer complaints, and the SEC is the primary regulator of investment companies and investment advisers registered with the SEC. The SEC also evaluates the quality of NASD and NYSE oversight in enforcing their members' compliance with federal securities laws, including compliance with Regulation S-P. The most common Regulation S-P deficiencies have been failure to provide privacy notices, lack of or inadequate privacy policies, and lack of or inadequate policies and procedures for safeguarding customer information. The SEC has not yet found any deficiencies during its examinations that warranted formal enforcement actions; instead, the SEC thus far has dealt with Regulation S-P compliance as a supervisory matter and has required registrants to resolve deficiencies without taking formal action.

The SEC has conducted two separate examination sweep programs reviewing securities firms' policies and procedures to protect their customers from identity theft. The first was conducted in 2002 and 2003, and the second is ongoing. In the first program, the SEC focused on large firms where a significant security breach could implicate large numbers of customers. The program included broker-dealers with more than half of all brokerage accounts and fund complexes with approximately a third of all mutual fund assets. In the second program, the SEC selected firms for review based on a number of factors including the extent to which their business model is dependent on the Internet, recent complaints, and certain affiliations. In both sweep programs, the overall goal has been to assess the reasonableness of securities firms' policies and procedures to protect their customers from identity theft. These sweep programs supplement the SEC's regular examination program, which includes examining securities firms' compliance with the SEC's requirements for safeguarding customer records and information.

At the SEC, consideration is being given to the possibility of adding provisions to the SEC's financial privacy rules to provide more detailed guidance.

Federal Trade Commission

The FTC has brought 14 cases against firms that allegedly failed to maintain reasonable procedures to protect the sensitive consumer data they collected.

> ***In the Matter of Guidance Software, Inc.,***
> FTC File No. 062-3057 (November 16, 2006) (consent order)
> ***http://www.ftc.gov/opa/2006/11/guidance.htm***

The FTC charged that Guidance, a seller of software for use in responding to computer breaches and other security incidents, failed to take reasonable security measures to protect sensitive customer data despite promises made on its website. The complaint alleged that Guidance's failure to protect the sensitive data as promised constituted a deceptive practice under Section 5 of the FTC Act. The matter was settled through a consent agreement in which Guidance agreed to implement a comprehensive information-security program and obtain audits by an independent third-party security professional every other year for 10 years.

> ***In the Matter of Card Systems Solutions, Inc. and Solidus Networks, Inc., d/b/a Pay by Touch Solutions***,
> FTC File No. 052-3148 (Sept. 8, 2006) (consent order)
> ***http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html***

The FTC charged that CardSystems, a processor of transactions for major credit cards, failed to provide reasonable security for sensitive consumer information, resulting in the breach of credit card information for tens of millions of card holders. The complaint alleged that this failure caused or was likely to cause substantial consumer injury and constituted an unfair practice under Section 5 of the FTC Act. The matter was resolved through a

settlement whereby CardSystems and its successor company agreed to implement a comprehensive information security program that must be certified by a qualified, independent, third-party professional every other year for 20 years.

> ***In the Matter of Nations Title Agency, Inc., Nations Holding Company, and Christopher M. Likens***, FTC Docket No. C-4161 (June 19, 2006) (consent order) ***http://www.ftc.gov/os/caselist/0523117/0523117.htm***
>
> ***In the Matter of Superior Mortgage Corp.***,
> FTC Docket No. C-4153 (Dec. 14, 2005) (consent order)
> ***http://www.ftc.gov/os/caselist/0523136/0523136.htm***
>
> ***In the Matter of Nationwide Mortgage Group, Inc., and John D. Eubank***,
> FTC Docket No. 9319 (April 12, 2005) (consent order)
> ***http://www.ftc.gov/os/adjpro/d9319/index.htm***
>
> ***In the Matter of Sunbelt Lending Services***,
> FTC Docket No. C-4129 (Jan. 3, 2005) (consent order)
> ***http://www.ftc.gov/os/caselist/0423153/04231513.htm***

In these cases, the FTC charged four companies in the real estate business with violating the GLB Safeguards Rule by failing to provide reasonable security to protect consumers' confidential financial information, including SSNs, bank and credit card account numbers, and credit histories. In the *Nationwide* and *Sunbelt* cases, the FTC charged that the companies violated the GLB Privacy Rule by failing to provide required privacy notices to consumers, and in the *Nationwide* and *Superior* cases, that the companies allegedly misrepresented their security procedures. In settling these cases, the companies agreed to comply with the various laws and regulations they allegedly violated and to implement a comprehensive security program and obtain periodic audits from an independent professional.

> ***In the Matter of DSW, Inc.***,
> FTC Docket No. C-4157 (March 14, 2006) (consent order)
> ***http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html***

Following a breach involving account information for 1.5 million credit card, debit card, and checking accounts, the FTC charged that shoe discounter DSW engaged in an unfair practice by failing to provide reasonable security for sensitive consumer information. In settling the case, as in other FTC data security orders, DSW agreed to implement a comprehensive information security program and obtain periodic audits.

> ***United States v. ChoicePoint, Inc.,***
> 1 06-CV-0198 (N.D. Ga. February 15, 2006)
> ***http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html***

Following a breach involving the sensitive information, including thousands of credit reports, of over 160,000 consumers, the FTC charged data broker ChoicePoint with failing to have reasonable procedures to screen prospective purchasers of their data products. According to the FTC complaint, ChoicePoint failed to detect obvious signs that certain purchasers were lying about their credentials, and as a result, ChoicePoint sold information to identity thieves posing as legitimate businesses. The FTC charged that ChoicePoint violated the FCRA by furnishing consumer reports to purchasers who did not have a permissible purpose to obtain them, and by failing to maintain reasonable procedures to verify purchasers' identities and purposes for obtaining the information. The agency also charged that ChoicePoint violated the FTC Act by engaging in unfair practices and by making false and misleading statements in its privacy policies about its credentialing procedures. The FTC alleged that ChoicePoint's practices led to at least 800 cases of identity theft at the time the complaint was filed. In its settlement with the FTC, ChoicePoint agreed to pay $10 million in civil penalties for its violations of the FCRA, and $5 million in redress to identity theft victims. The settlement also requires ChoicePoint to maintain reasonable procedures to prevent the provision of a consumer report to a party without a permissible purpose, including specific types of investigation and certification procedures.

In the Matter of BJ's Wholesale Club, Inc.,
FTC Docket No. C-4148 (Sept. 20, 2005) (consent order)
http://www.ftc.gov/opa/2005/06/bjswholesale.htm

Following a security breach involving account information for thousands of credit and debit cards, BJ's settled FTC charges that its failure to take appropriate security measures to protect the sensitive account information of its customers was an unfair practice. The FTC had alleged that an unauthorized person or persons made millions of dollars in fraudulent purchases using counterfeit copies of credit and debit cards that had been used at BJ's stores. In settling the case, as in other FTC data security orders, BJ's agreed to implement a comprehensive information security program and obtain periodic audits.

In the Matter of Petco Animal Supplies, Inc.,
FTC Docket No. C-4133 (March 4, 2005) (consent order)
http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html

Petco settled FTC charges that security flaws in its www.petco.com web site violated privacy promises it made to its customers and therefore was a deceptive practice in violation of the FTC Act. According to the FTC complaint, Petco made security claims on its website, for example, that customers' personal data was encrypted and "strictly shielded from unauthorized access." The FTC alleged that, in fact, Petco did not encrypt the data and failed to implement reasonable measures to protect sensitive consumer information from common attacks. As a result, a hacker allegedly

was able to penetrate the website and access credit card numbers stored in unencrypted clear text. The settlement prohibits Petco from misrepresenting the extent to which it maintains and protects sensitive consumer information and, as in other FTC data security orders, requires the company to implement a comprehensive information security program and obtain periodic audits.

> ***In the Matter of MTS Inc., d/b/a Tower Records/Books/Video***,
> FTC Docket No. C-4110 (May 28, 2004) (consent order)
> ***http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html***

Tower settled FTC charges that a security flaw in the Tower website exposed customers' personal information to other Internet users, in violation of Tower's claims in its privacy policy that it used "state-of-the-art" security technology. The settlement bars Tower from misrepresenting the extent to which it maintains and protects the privacy, confidentiality, or security of personal information collected from or about consumers. As in other FTC data security cases, Tower also agreed to implement a comprehensive information security program and obtain periodic audits.

> ***In the Matter of Guess?, Inc.***,
> FTC Docket No. C-4091(July 30, 2003) (consent order)
> ***http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html***

Guess settled FTC charges that it exposed consumers' personal information, including credit card numbers, to commonly known attacks by hackers, contrary to the company's claims that it would keep the information secure and protected. The complaint also alleged that Guess falsely claimed that the personal information was stored in an encrypted format. According to the complaint, a visitor to the website, using a common attack, was able to read, in clear text, credit card numbers stored in Guess' databases. The settlement, like those in the *Tower* and *Petco* cases, prohibits future misrepresentations and requires Guess to implement a comprehensive information security program and obtain periodic audits.

> ***In the Matter of Microsoft Corp.***,
> FTC Docket No. C-4069 (Dec. 20, 2002) (consent order)
> ***http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html***

Microsoft settled FTC charges that it made false representations about the security, confidentiality, and features of its "Passport" services, including claims that purchases made using the service were generally safer or more secure than purchases made without it. According to the FTC complaint, Microsoft failed to implement sufficient security procedures to maintain the high level of security it represented. The settlement, like those in *Tower, Petco,* and *Guess,* prohibits future misrepresentations and requires Microsoft to implement a comprehensive information security program and obtain periodic audits.

In the Matter of Eli Lilly & Co.,
FTC Docket No. C-4047 (May 8, 2002) (consent order)
http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html

Lilly settled FTC charges that it engaged in a deceptive practice when it made claims about the confidentiality of personal information it gathered on its websites, while failing to maintain measures to protect that information. These alleged failures led to the company's disclosure of the email addresses of 669 subscribers, which essentially revealed that they were users of Lilly's prescription drug Prozac. The settlement, like those in *Tower, Petco, Guess,* and *Microsoft*, prohibits future misrepresentations and requires Lilly to implement a comprehensive information security program and obtain periodic audits.

PART C

GUIDANCE FOR BUSINESSES ON SAFEGUARDING DATA

Federal Agency Guidance

While the enforcement efforts by the government are key to sending a message about the importance of securing data and preventing identity theft, education and outreach also can help to ensure that companies are aware of their legal obligations to protect the data they hold. Numerous federal agencies–including the FTC, the federal bank regulatory agencies, the National Institute of Standards and Technology (NIST), the Small Business Administration (SBA), and the Department of Health and Human Services (HHS)–provide guidance to the industries they regulate on the subject of data protection. This guidance is accessible through agency websites, written brochures, speeches, workshops, and conferences. They include the following:

Federal Trade Commission. The FTC's emphasis is on preventing breaches before they happen by encouraging businesses to make data security part of their regular operations and corporate culture. The agency recognizes that there is no one-size-fits-all data security "fix," and offers companies realistic advice about adapting old-school business practices to meet new-style threats. Its recommendations deal with employee management and training, appropriate information systems security, and detecting and managing system failures through constant monitoring and system updates. The FTC has numerous programs to inform organizations about their legal responsibilities to strengthen data security:

- **Publications.** Among the publications the FTC has produced for businesses are *Security Check: Reducing Risks to Your Computer Systems*, available at ***www.ftc.gov/bcp/conline/pubs/buspubs/security.htm***; *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, available at ***www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm***; *Disposing of Consumer Report Information? New Rule Tells How*, available at ***www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.htm***; and *Securing Your Wireless Network*, available at ***www.ftc.gov/bcp/conline/pubs/online/wireless.pdf***. The FTC has recently issued a new brochure on how entities can safeguard sensitive consumer information at ***www.ftc.gov/infosecurity***.
- OnGuard Online website, available at ***www.onguardonline.gov***. This website offers practical tips on guarding against Internet fraud, securing computers, and protecting personal information, as well as resources for companies in the event of a data breach, such as law enforcement and credit reporting agency contacts. The site has daily updates from the Department of Homeland Security

(DHS), as well as content developed by IT companies, industry associations, and other federal agencies.

- **Workshop on "*Technologies for Protecting Personal Information: The Consumer and Business Experiences*."** The FTC's efforts on data security took root in this workshop, which explored the challenges consumers and industry face in securing their computers. The workshop featured industry leaders, technologists, researchers on human behavior, and representatives from consumer and privacy groups to both identify challenges in safeguarding information and propose solutions, both technical and human. Information about this workshop is available at ***www.ftc.gov/bcp/workshops/technology*** and ***www.ftc.gov/bcp/workshops/technology/finalreport.pdf***.

- **The Division of Privacy and Identity Protection.** Recognizing the need to protect sensitive consumer information and fight against identity theft, in January 2006, the FTC created a new Division of Privacy and Identity Protection within its Bureau of Consumer Protection. This division addresses consumer privacy and data security matters through aggressive enforcement, rulemaking, policy development, and creative outreach to consumers and businesses.

Federal Bank Regulatory Agencies. The federal bank regulatory agencies also have been extremely active in issuing guidance for financial institutions relating to information security and identity theft, including the Federal Financial Institutions Examination Council ("FFIEC") Information Technology Examination Handbook's *Information Security Booklet*, available at ***http://www.ffiec.gov/guides.htm***; the FFIEC's guidance entitled *Authentication in an Internet Banking Environment*, available at ***http://www.fdic.gov/consumers/consumer/fightheft/index.html***; the *Interagency Informational Brochure on Internet Phishing Scams*, available at ***www.fdic.gov/consumers/consumer/fightheft/index.html***; and the bank regulatory agencies' letter entitled *Identity Theft and Pretext Calling*, available at ***http://www.federalreserve.gov/boarddocs/srletters/2001/sr0111.htm***.[3]

Securities and Exchange Commission. In June 2000, SEC adopted Regulation S-P, which implements the GLB Act's Title V information privacy and safeguarding requirements for securities brokers and dealers, investment companies, and SEC-registered investment advisers. In addition to providing general guidance, Regulation S-P contains numerous examples specific to the securities industry to provide more meaningful guidance to help firms implement its requirements. It also includes a section regarding procedures to safeguard information, including the disposal of consumer report information. In September 2004 the SEC released a public statement on Regulation S-P's

safeguarding requirements. *See* Disposal of Consumer Report Information, Release Nos. 34-50361, IA-2293, IC-26596 (Sept. 14, 2004).

National Credit Union Administration. The NCUA offers advice to credit unions on issues related to data security. It has issued numerous letters to credit unions that provide guidance on these issues (available at ***www.ncua.gov/letters/letters.html***), and representatives from the NCUA regularly speak on information security issues at credit union conferences.

Small Business Administration. The SBA offers information and data security guidance targeted towards small businesses. The SBA's website, ***www.sba.gov/beawareandprepare/cyber.html***, serves as a portal to private sector sites that offer information for safeguarding computers against cyber attacks, and directs users to NIST's Computer Security Division's Small Business Corner, which provides "Cyber Security Tips" on subjects including spyware, email hoaxes, employee awareness, and firewalls (available at ***sbc.nist.gov/cyber-security-tips/***). The SBA also offers workshops on small business computer security around the country, co-sponsored by the SBA and the Federal Bureau of Investigation (FBI), that allow participants to explore practical tools to assess and improve the security of their information.

Department of Health and Human Services. The Department of Health and Human Services provides entities with information to help their compliance with the Privacy and Security Rules of HIPAA. The Office for Civil Rights provides guidance and educational materials for entities required to comply with the Privacy Rule, and the Office of e-Health Standards and Services in the Centers for Medicare and Medicaid Services provides guidance and educational materials for entities required to comply with the Security Rule. The Privacy Rule sets standards that protect the privacy of health information, and the associated Security Rule sets standards to assure the confidentiality, integrity, and availability of electronic protected health information.

Private Sector Guidance

Private sector entities also provide guidance to businesses that addresses safeguarding sensitive data, usually targeted to entities based on their industry sector or size. A few examples include:

Financial Services Industry. The Financial Services Roundtable has developed voluntary guidelines to address data security concerns in the financial services industry, such as incorporating security awareness and education into corporate-wide training programs, encrypting some types of financial data and customer data when it is transported on unprotected networks or stored for aggregation-related processes, and using Secure Socket Layers (SSL) when obtaining data feeds for aggregation-related processes.[4] The financial services industry also has produced white papers and reports, which include advice about new account/application

review, "Know Your Employee" practices that are designed to screen criminals out of financial institutions, and using technology to identify and manage fraud and identity theft.[5]

The payment card segment of the financial services industry has adopted a single set of data security standards, the Payment Card Industry Data Security Standards (PCI Standards), for all merchants and service providers that store, process, or transmit cardholder data. These standards, which card companies have adopted voluntarily, resulted from a collaboration between Visa and MasterCard, and have been endorsed by other major U.S. card companies.[6] The PCI Standards are designed to ensure the proper handling and protection of cardholder account and transaction information. Major card companies have their own programs to ensure data security compliance in accordance with PCI standards, and each company enforces the standards via their individual programs. Visa, for example, instituted a program called Cardholder Information Security Program for this purpose; information about this program is available at ***http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html***. Under individual company programs, failure to comply with the standards may subject merchants and service providers to fines levied by the card company and possible revocation of the right to participate in the card company's network.

Real Estate Industry. Real estate associations also have issued information security guidelines that address how the industry collects, shares, and protects the consumer information it uses and receives. One set of guidelines issued by the National Association of Realtors (available at ***http://www.realtor.org/realtororg.nsf/files/NARInternetSecurityGuide.pdf/$FILE/NARInternetSecurityGuide.pdf***), consolidates best practices for real estate agents, multiple listing services, and associations to improve their security safeguards. The guidelines recommend setting policies for the acceptable use of information; creating management oversight, including setting up an information security management committee; setting up access controls on a "need to know" basis; implementing appropriate personnel screening and regular training; instituting physical controls including locks and appropriate disposal tactics; and using technology applications to secure data and detect problems (e.g., cryptographic controls, network intrusion detection).

Health Care Industry. The health care industry has applied significant resources towards improving the privacy and security of its business practices. Major industry organizations such as the American Hospital Association and the American Medical Association produce handbooks and toolkits, and partner with vendors to provide security and privacy guidance to their members. WEDI (Workgroup for Electronic Data Interchange), an industry nonprofit dedicated to improving health care through electronic commerce, has produced a series of white papers that

provide guidance on topics that include encryption, disaster recovery, policies and procedures, and evaluation, available at ***www.wedi.org***. Industry-sponsored conferences and seminars focused on implementing privacy and security protections for health information are commonplace. Providing the tools to enable compliance with the HIPAA Security and Privacy Rules has been the common goal of these efforts.

Internet Service and Electronic Mailbox Providers. Because of their unique position in the internet community, internet service providers (ISPs) and electronic mailbox providers pay particular attention to data security issues. Guidelines from the Anti-Phishing Working Group (APWG), available at ***www.antiphishing.org/reports/bestpracticesforisps.pdf***, focus on how ISPs and mailbox providers can prevent and mitigate the damage caused by phishing attacks. They recommend a number of practices, including using inbound and outbound filtration technology to prevent spam, monitoring bounced email messages to help determine when a phishing attack is underway, disabling hyperlinks in emails from sources that are not trusted, and providing customers relevant, accurate information about phishing and what to do following an attack.

Small Businesses. Organizations also have made available information on how to recognize and address identity theft and fraud directed toward small businesses. The U.S. Chamber of Commerce, for instance, offers a "Security Toolkit" for small businesses, available at ***www.uschamber.com/sb/security/default.htm***, that includes information about compliance with PCI standards, technology tips, a Microsoft Interactive Security Video, a sample security plan, and technical tools. The Chamber is conducting a series of seminars in 12 cities, featuring experts from Visa, that should help businesses that accept credit or debit card payments understand the basic requirements for handling sensitive customer data. Information about these seminars is available at ***www.uschamber.com/events/visatour***.

Other organizations, such as the Council of Better Business Bureaus and the National Cyber Security Alliance, provide guidelines that serve as primers for incorporating basic security and privacy practices into everyday business operations that are appropriately tailored for smaller companies. These guidelines, available at ***www.bbb.org/securityandprivacy/SecurityPrivacyMadeSimpler.pdf*** and ***www.staysafeonline.org/basics/company/basic_tips.html***, emphasize the importance of employee screening and training and the use of physical safeguards beyond electronic measures to prevent identity theft. They include tips on: recognizing attempts at theft and fraud; understanding the importance of offline and online security and privacy safeguards; developing security and privacy policies and communicating them to customers; training employees; handling and managing sensitive

information; managing employees as they interact with customers and their personal data; credit card/debit card security safeguards; physically safeguarding systems and accessories; using the latest technologies; instituting controls to prevent phishing; and conducting international transactions securely.

Nonprofit Organizations. Nonprofit organizations also have issued guidance to businesses. For example, one nonprofit organization focused on online privacy has guidelines available for companies drafting internal data security at ***www.truste.org/pdf/SecurityGuidelines.pdf***. The guidelines stress that reasonable security standards are not "one size fits all," and offer companies a non-technical high level overview of recommended security practices for consideration.

Some private sector entities also have developed standards and guidelines regarding specific issues that raise security concerns:

- **Contractual Arrangements with Service Providers.** The guidance from the private sector generally recognizes that entities have a responsibility to ensure that their security and privacy policies are implemented and enforced. Typically, private sector guidelines recognize the importance of contractually requiring all third party service vendors with access to an organization's sensitive data, such as outsourced IT or data management operations, to adhere to the contracting entity's security requirements.[7] These guidelines also address specific practices for contracting organizations, including conducting a site audit of a vendor's data center to determine the adequacy of the security infrastructure; requiring vendors to provide certification that they are in compliance with the contracting organization's privacy and data protection obligations; and performing periodic or random audits of vendors or outsourcers.[8]

- **Encryption.** Encryption is the process of converting plaintext into ciphertext to ensure that data can be read only by the intended recipient. Categories of information for encryption commonly include access passwords, email, files on laptops, stored data, and virtual private networks (VPNs), which use a public telecommunication infrastructure like the Internet to provide remote users with secure access to their organization's network. A number of industry groups are developing new policies that recommend the use of encryption to enhance internal data storage security.[9] In the wake of several highly publicized security breaches, encryption is being viewed as a tool for providing enhanced security for portable devices (laptops) and for media (backup tapes).[10]

- **Preventing Malware.** Malware is considered a growing threat to data privacy and security.[11] Spyware, a type of malware intended to violate a user's privacy, is becoming more widespread, and is leading organizations and computer users to take new precautions.[12] Some

businesses have adopted industry and government guidelines on how to detect and avoid malware, including guidelines developed by NIST. Although developed for use by federal agencies, the NIST guidelines have been adopted voluntarily by many businesses as well.[13] NIST's recommendations for improving an organization's malware incident prevention measures include: planning and implementing an approach to malware incident prevention based on the most likely attack points; ensuring that policies support the prevention of malware incidents and including provisions related to remote workers; and using appropriate techniques to prevent malware incidents (e.g., patch management, application of security configuration guides).[14]

- **Employee Data.** While some guidance to businesses is exclusively or primarily focused on providing advice about securing customer data, some organizations concentrate their efforts on guidelines and best practices for protecting the data of employees. For instance, the Society for Human Resource Management offers its members reports and toolkits related to identity theft, data security, and HIPAA privacy, including advice about compliance with federal and state privacy laws, on its website at ***www.shrm.org***.

State Guidance

Many state consumer protection agencies and Attorneys General have information and guidance for businesses to help them protect consumers' sensitive information. A few examples of states providing this type of guidance include:

California. California has created an Office of Privacy Protection to promote and protect consumers' rights. This office makes available numerous publications to assist businesses in complying with federal and state safeguards requirements as well as improving their general information security practices. In its publication, *A California Business Privacy Handbook* (available at ***www.privacyprotection.ca.gov/recommendations/ca_business_privacy_hb.pdf***), the state's Office of Privacy Protection describes basic techniques that companies can use to protect personal information and prevent identity theft, such as controlling access to personal information and securely disposing of materials containing sensitive consumer information. Likewise, in its *Recommended Practices for Protecting the Confidentiality of Social Security Numbers* (available at ***www.privacyprotection.ca.gov/recommendations/ssnrecommendations.pdf***), the state provides businesses with information on federal and state laws regarding the collection, use, and confidentiality of SSNs, as well as recommended practices like reducing the unnecessary collection of SSNs and eliminating the public display of SSNs.

New York. The New York State Office of Cyber Security and Critical Infrastructure Coordination has published *Best Practices and Assessment Tools to Promote Cyber Security Awareness*. This guide includes advice specifically directed at corporations and small businesses.

Wisconsin. Like California, Wisconsin has created an agency to address consumers' privacy rights, the Office of Privacy Protection within the Wisconsin Department of Agriculture, Trade and Consumer Protection division. This office provides guidance for small businesses through its website, available at ***www.privacy.wi.gov/business/business.jsp***, which recommends actions like limiting the collection of sensitive information, and screening and training employees.

PART D

GUIDANCE FOR BUSINESSES ON DATA BREACHES

Federal Guidance

In addition to providing guidance on safeguarding sensitive information, the federal government offers businesses guidance on what to do in the event of a data breach. The federal bank regulatory agencies (the FRB, FDIC, NCUA, OCC, and OTS), for example, have issued detailed guidance on financial institutions' response programs and customer notice, which is discussed in detail in Part A, above. The FTC offers businesses guidance on breach notifications in a booklet entitled *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, available at ***http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.htm***. The FTC recommends that when a data compromise could result in harm to a person or business, private entities should contact appropriate local law enforcement as soon as possible. The FTC also recommends that companies consider contacting other businesses that may be impacted by a data breach, such as banks or credit issuers, and if names and SSNs have been stolen, the major credit bureaus. Finally, when deciding if or when individual consumer notification is warranted, the FTC recommends that businesses consider the nature of the compromise, the type of information taken, the likelihood of misuse, and the potential damage arising from misuse. The FTC's booklet also contains a model letter for businesses notifying people whose names and SSNs have been stolen.

Private Sector Guidance

In light of recent high-profile data breaches, a number of private sector organizations also have developed guidance regarding how to respond to breaches and when to provide notice to consumers. Some of this guidance is designed to facilitate compliance with applicable laws, regulations, or industry standards. Examples of entities providing this guidance include:

- **The American Bankers Association (ABA).** The ABA sponsors conferences on regulatory compliance that address responding to information breaches; information about these conferences is available at ***www.aba.com/Events/NCS.htm***. The ABA also provides online information about establishing a response program and notifying customers on its website at ***www.aba.com/About+ABA/datasecuritynotification.htm***.
- **The Financial Services Roundtable.** The Financial Services Roundtable has developed guidelines to address breach response issues, available at ***www.bitsinfo.org/downloads/Publications%20Page/bitscons2005.pdf***.
- **The Payment Card Industry (PCI).** Members of the payment card industry also have issued guidance for businesses to respond to security

incidents in order to comply with the PCI standards. For instance, individual card companies have issued step-by-step instructions and workbooks for businesses responding to a security incident.[15] Businesses are encouraged to create an internal response plan that, among other things, confirms, analyzes, and documents events, and allows for a quick response to maintain and restore business continuity.[16] In the event of a suspected or confirmed security breach, merchants and service providers are advised to immediately contain the breach and limit possible exposure of consumer information while preserving logs and electronic evidence.[17] Affected companies are advised to contact their internal information security group and incident response team, merchant bank, card company, and the local office of the United States Secret Service (USSS).[18] Moreover, businesses are advised to conduct a forensic analysis of the event and maintain logs and evidence to assist law enforcement authorities in investigations.[19]

- **Nonprofit Organizations.** Nonprofit organizations that specialize in data security and privacy issues also have distributed guidance for businesses in the event of a data security breach. For instance, the National Cyber Security Alliance offers a guide on *Small Business Incident Recovery and Reporting*, available at ***www.staysafeonline.org/basics/recovery/recoveryandreporting.html***. This guide includes information about establishing an internal incident response team to respond to security incidents, and a formal written breach response plan and process for reporting and escalating incidents. The Identity Theft Resource Center (ITRC) provides similar guidance on its website at ***www.idtheftcenter.org/index.shtml***. In addition, the Council of Better Business Bureaus has created guidelines specifically targeted to small businesses, available at ***www.bbb.org/securityandprivacy/SecurityPrivacyMadeSimpler.pdf***. Although not all states require customer notification in the event of a breach, the guidance urges companies to consider the advantages of notifying those whose information has been compromised.

- Other organizations, including higher education associations,[20] professional associations,[21] and firms that offer consulting or policy development services related to data security,[22] have provided advice and guidance to businesses in the event of a data breach. The guidance relates to policies, procedures, technical tools, and notice to consumers for businesses responding to a security incident.

State Guidance

State consumer protection agencies and Attorneys General also offer guidance on responding to data breaches. Among states offering such guidance are:

- **California.** California's *Recommended Practices on Notice of Security Breach Involving Personal Information*, available at ***www.privacyprotection.ca.gov/recommendations/secbreach.pdf***, has information about the state's breach notification law, as well as recommended practices for protection and prevention, preparation for notification, and notification itself. This document offers guidance on developing an incident response plan, with instructions for developing written procedures for internal notification processes, designating an individual responsible for coordinating internal notification procedures, and responding to the breach by providing notice to consumers and law enforcement. The document also provides sample breach notice letters.

- **Wisconsin.** The Wisconsin Department of Agriculture, Trade and Consumer Protection, Office of Privacy Protection, publishes a fact sheet entitled *How Small Business Can Help in the Fight Against ID Theft*, (available at ***www.privacy.wi.gov./business/business.jsp***), which recommends that businesses create an action plan in advance for responding to data breaches. In the event of a breach, businesses are encouraged to investigate internally while devising a plan for notifying people that a breach has occurred.

- **Colorado.** The Colorado Attorney General's office provides information about data breach response plans to businesses on its website at ***www.ago.state.co.us/idtheft/clients.cfm***. It recommends that businesses have policies and procedures in place to isolate the information that has been compromised, promptly notify all affected customers of the breach, and promptly notify the appropriate law enforcement office of the breach.

PART E

FEDERAL CONSUMER EDUCATION EFFORTS

The federal government has produced, promoted, and distributed an extensive library of consumer education materials in print and electronic formats to help consumers learn about various aspects of identity theft. Listed below are titles and locations of each agency's identity theft consumer education materials.

FEDERAL TRADE COMMISSION (FTC)

www.ftc.gov

The FTC has played 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. (Spanish–***www.consumer.gov/idtheft/espanol.htm***.)

The FTC also recently implemented a national public awareness campaign centered around the themes of "Deter, Detect, and Defend." This campaign seeks to drive behavioral change in consumers that will reduce their risk of identity theft (Deter); encourage consumer monitoring of their credit reports and accounts to alert them of identity theft soon 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 material written for consumers about identity theft and material written for organizations, community leaders, and local law enforcement on how to communicate and educate their constituencies about identity theft. ***www.consumer.gov/idtheft/ddd/index.html***. (Spanish–***www.consumer.gov/idtheft/ddd/espanol.html***).

The Deter, Detect, and Defend materials have been adopted and distributed by hundreds of entities, both public and private, involved in the fight against identity theft. The National Council of Higher Education Loan Program, the Direct Marketing Association, the National Association of Realtors, the Internal Revenue Service (IRS), neighborhood associations, and over 500 local law enforcement agencies among others, are using the materials as part of their own consumer education efforts. The U.S. Department of Justice's Office for Victims of Crimes disseminated 4,600 Deter, Detect, Defend kits to the victim services field offices.

Other FTC publications include:

Fighting Back Against Identity Theft
www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.htm

ID Theft: What It's All About
www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.htm
In Spanish—***www.ftc.gov/bcp/conline/spanish/credit/s-idtheftmini.htm***

Take Charge: Fighting Back Against Identity Theft
www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm
In Spanish—*www.ftc.gov/bcp/conline/spanish/credit/s-idtheft.htm*

"Active Duty" Alerts Help Protect Military Personnel from Identity Theft
www.ftc.gov/bcp/conline/pubs/alerts/dutyalrt.htm

What To Do If Your Personal Information Has Been Compromised
www.ftc.gov/bcp/conline/pubs/alerts/infocompalrt.htm

Remedying the Effects of Identity Theft
www.ftc.gov/bcp/conline/pubs/credit/idtsummary.pdf
In Spanish—*www.ftc.gov/bcp/conline/spanish/credit/s-idtsummary.pdf*

Your Access to Free Credit Reports
www.ftc.gov/bcp/conline/pubs/credit/freereports.htm
In Spanish—*www.ftc.gov/bcp/conline/spanish/credit/s-freereports.htm*

How Not to Get Hooked by a Phishing Scam
www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm
In Spanish—*www.ftc.gov/bcp/conline/spanish/alerts/s-phishingalrt.htm*

Privacy Choices for Your Personal Financial Information
www.ftc.gov/bcp/conline/pubs/credit/privchoices.htm

Medicare Part D Solicitations: Words to the Wise About Fraud
www.ftc.gov/bcp/conline/pubs/alerts/meddalrt.htm

ID Theft Audio File **—Audio 1, Audio 2**
www.consumer.gov/idtheft/con_pubs.htm

ID Theft Video News Release **(Dial Up Version—56k)—Video 1, Video 2**
www.consumer.gov/idtheft/con_pubs.htm

ID Theft Video News Release **(Broadband Version)—Video 1, Video 2**
www.consumer.gov/idtheft/con_pubs.htm

U.S. DEPARTMENT OF JUSTICE (DOJ)
www.usdoj.gov

Bureau of Justice Assistance (BJA)
The Justice Department's BJA, together with the National Crime Prevention Council, created an identity theft booklet, *Preventing Identity Theft: a Guide for Consumers*,[23] and produced radio and television public service announcements about identity theft, featuring McGruff® the Crime Dog. Other publications include *Identity Theft and Fraud,* at ***www.usdoj.gov/criminal/fraud/idtheft.html***.

Office for Victims of Crime (OVC)

The Department of Justice's OVC has several web pages on identity theft,[24] and has provided funding to several identity theft-related initiatives, such as the Ohio Identity Theft Verification Passport program. Other publications include *Identity Theft*, at ***www.ojp.gov/ovc/help/it.htm***.

Office of Justice Programs (OJP)

The Department of Justice's OJP also has developed some identity theft resources, including the following publications:

Justice Resource Update
www.ncjrs.gov/jru/spring_2006/featured.html

Preventing Identity Theft: A Guide for Consumers
www.ncpc.org/cms/cms-upload/prevent/files/idtheftrev.pdf

Executive Office for United States Trustees

The Executive Office for the United States Trustees, a component of DOJ, has developed the following publication on identity theft: *Fraud/Identity Theft*, at ***www.usdoj.gov/ust/r16/fraud.htm***.

United States Attorney's Offices *(www.usdoj.gov/usao)*

Some United States Attorney's Offices also have their own identity theft web pages, for example: ***www.usdoj.gov/usao/gan/citizen/idtheft.html*** and ***www.usdoj.gov/usao/cac/idtheft/idtheft.html.***

U.S. DEPARTMENT OF THE TREASURY

www.treas.gov

Over 120,000 copies of the Department of the Treasury's DVD about identity theft, *Identity Theft: Outsmarting the Crooks*, have been distributed to the public. *See* ***www.treasury.gov/press/releases/js3083.htm***. In addition, the Department of the Treasury has developed Identity Theft Resource Page, which can be found at ***www.treas.gov/offices/domestic-finance/financial-institution/cip/identity-theft.shtml***.

The FACT Act established the Financial Literacy and Education Commission (the Commission), and appointed the Secretary of the Treasury as head. The Commission, composed of 19 other federal agencies and bureaus, launched a website and toll-free hotline for financial literacy in 2004, ***www.MyMoney.gov*** and 1–888–MY–MONEY, along with a free toolkit. These resources include consumer information (available in English and Spanish) about how to defend oneself against identity theft and what victims should do to set their records straight.

Separately, the Department of Treasury's Financial Management Service and the Federal Reserve Banks sponsor *Go Direct*, a campaign to motivate people who receive federal benefit checks to use direct deposit. Direct deposit is the

best way for people to get their Social Security and SSI payments because it eliminates the risk of stolen checks, reduces fraud, and gives them more control over their money. A simple action like enrolling in direct deposit can offer much-needed peace of mind to people who rely on federal benefits, most of whom are seniors and people with disabilities.

Office of the Comptroller of the Currency (*www.occ.treas.gov*)

The OCC has issued a number of publications on identity theft. Those include the following:

Fight Back: What You Can Do about Identity Theft
www.occ.gov/consumer/idtheft.htm

How to Avoid Becoming a Victim of Identity Theft
www.occ.treas.gov/idtheft.pdf

Internet Pirates Are Trying to Steal Your Personal Financial Information
www.occ.gov/consumer/phishing.htm

Check Fraud: A Guide to Avoiding Losses
www.occ.treas.gov/chckfrd/chckfrd.pdf

Office of Thrift Supervision (*www.ots.treas.gov*)

The OTS has issued a number of publications related to identity theft. These publications deal with topics including pretext calling, phishing and email scams, and customer/consumer education, and can be found on the OTS website.

Internal Revenue Service (*www.irs.gov*)

The IRS, another arm of the Treasury Department, has issued the following publication on identity theft:

Identity Theft and Your Tax Records
www.irs.gov/individuals/article/0,,id=136324,00.html

Treasury Inspector General for Tax Administration (*www.treas.gov/tigta*)

TIGTA has issued the following publication for taxpayers relating to identity theft:

Computer Security Bulletin—Phishing Scams
www.treas.gov/tigta/docs/phishing_alert_2006.pdf

U.S. SECRET SERVICE (USSS)

www.secretservice.gov

The USSS, a component of DHS, is active in the investigation of identity theft. In that role, it also has issued the following guidance on identity theft:

Financial Crimes Division
www.treas.gov/usss/financial_crimes.shtml

Frequently Asked Questions (FAQ): Protecting Yourself
www.treas.gov/usss/faq.shtml#identity

FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

www.fdic.gov

The FDIC's December 2004 Identity Theft Study recommended the development of an educational initiative targeted to online banking customers on how to avoid common scams. That initiative, entitled *Don't Be an On-Line Victim*, is comprised of three parts: how consumers can secure their computer; how consumers can protect themselves from electronic scams that can lead to identity theft; and what consumers should do if they become the victim of identity theft. The educational tool is being distributed through the FDIC website and via CD-ROM. Additionally, in 2005, the FDIC sponsored four identity theft symposia entitled *Fighting Back Against Phishing and Account-Hijacking*. Each symposium included presentations by panels of experts from federal and state government, the banking industry, consumer organizations, and law enforcement. Total attendance at the symposia exceeded 575. The FDIC's 2006 symposia series, *Building Consumer Confidence in an E-Commerce World*, was a continuation of the FDIC's efforts to facilitate dialogue on the risks and solutions for e-commerce and payment system fraud. The FDIC is also working on an educational campaign, scheduled for rollout in 2007, to educate consumers about online banking and the protections available to them that make it safe.

The FDIC's other publications on identity theft include the following:

Classic Cons... And How to Counter Them
www.fdic.gov/consumers/consumer/news/cnsprg98/cons.html

A Crook Has Drained Your Account. Who Pays?
www.fdic.gov/consumers/consumer/news/cnsprg98/crook.html

When a Criminal's Cover Is Your Identity
www.fdic.gov/consumers/privacy/criminalscover/index.html

Your Wallet: A Loser's Manual
www.fdic.gov/consumers/consumer/news/cnfall97/wallet.html

Identity Theft
www.fdic.gov/consumers/consumer/alerts/theft.html

NATIONAL CREDIT UNION ADMINISTRATION (NCUA)

www.ncua.gov

The NCUA's primary publication on identity theft, entitled *You Can Fight Identity Theft*, can be found at ***www.ncua.gov/publications/brochures/identitytheft/phishbrochure-web.pdf***.

FEDERAL RESERVE SYSTEM

www.federalreserve.gov

The Federal Reserve Bank of Boston has published a consumer brochure entitled *Identity Theft*, which can be found at ***www.bos.frb.org/consumer/identity/idtheft.htm***.

U.S. SOCIAL SECURITY ADMINISTRATION (SSA)

www.socialsecurity.gov

The SSA has a hotline for reporting fraud, which can be found at ***www.socialsecurity.gov/oig/guidelin.htm***. In addition, the SSA's website, ***www.socialsecurity.gov/pubs/idtheft.htm***, provides links to various resources to assist victims of identity theft. SSA has several printed publications (in English and Spanish) on safeguarding the use of SSNs and cards to help prevent identity theft. These include the following:

Identity Theft and Your Social Security Number
(SSA Publication No. 05-10064)
www.socialsecurity.gov/pubs/10064.html

Your Social Security Number and Card
(SSA Pub. No. 05-10002)
www.socialsecurity.gov/pubs/10002.html

New Rules for Getting a Social Security Number and Card
(SSA Publication No. 05-10120)
www.socialsecurity.gov/pubs/10120.html

Frequently Asked Questions on SSA's Internet website
www.socialsecurity.gov

SSA OIG (Office of Inspector General): When Someone Else Uses Your Social Security Number Fact Sheet
www.socialsecurity.gov/oig/hotline/when.htm

SSA OIG—Identity Theft Links
www.socialsecurity.gov/oig/investigations/links.htm

U.S. POSTAL INSPECTION SERVICE (USPIS)

www.usps.com

The USPIS has been active in engaging in outreach activities related to identity theft. For example, the USPIS, together with the FTC and the Better Business Bureau (BBB), developed the "Shred It & Forget It" campaign, which encourages consumers to shred discarded documents containing personal information. The USPIS also maintains an identity theft website and has conducted national campaigns about Internet fraud and identity theft, and produced two DVDs on these subjects–"Identity Crisis" and "Web of Deceit"–and Publication 248, "Safeguard Your Personal Information." Other publications include:

ID Theft Poster
www.usps.com/websites/depart/inspect/idposter.pdf

Identity Theft Is America's Fastest-Growing Crime
www.usps.com/websites/depart/inspect/idthft_ncpw.htm

Read These Tips to Protect Yourself from Identity Theft
www.usps.com/websites/depart/inspect/idtheftips.htm

Safeguard Your Personal Information
www.usps.com/cpim/ftp/pubs/pub280/welcome.htm

Identity Theft: Stealing Your Name and Your Money
www.usps.com/websites/depart/inspect/IDtheft2.htm

Identity Crisis—DVD
www.usps.com/websites/depart/inspect/idthft_ncpw.htm

LooksTooGoodToBeTrue.com
http://www.lookstoogoodtobetrue.com/fraud.aspx

U.S. DEPARTMENT OF EDUCATION

www.ed.gov

The Department of Education offers materials aimed at increasing students' and college administrators' awareness of identity theft and steps to reducing students' chances of falling victim. The Department also has included identity theft prevention tips in the billing statements that are sent to student borrowers. Its Federal Student Aid website, ***www.federalstudentaid.ed.gov***, contains information on safeguarding student aid information and reducing the risk of identity theft.[25] The Department's OIG's website, ***www.ed.gov/misused***, both offers and collects information on identity theft. The OIG also conducts presentations at conferences of financial aid professionals, and has developed a DVD, *FSA Identity Theft—We Need Your Help*, to alert the financial aid community to the problem.

DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS)
www.hhs.gov

Office of Disease Prevention and Health Promotion
HHS's Office of Disease Prevention and Health Promotion has circulated the following publication relating to identity theft: *Healthfinder—Protecting Your Identity*, which can be found at ***www.healthfinder.gov/docs/doc09195.htm***.

Centers for Medicare and Medicaid Services (*www.cms.gov*)
HHS's Centers for Medicare and Medicaid Services has released the following publications relating to identity theft:

Medicare and You 2006
www.medicare.gov/publications/pubs/pdf/10050.pdf

Holding Ourselves to a Higher Standard
www.cms.hhs.gov/InformationSecurity/

The National Women's Health Information Center
Protecting Yourself from Cybercrime
www.girlshealth.gov/safety/internet.cybercrime.htm

Food and Drug Administration (*www.fda.gov*)
The FDA's publications relating to identity theft include the FDA Consumer magazine (July-August 2005 Issue), and *Be Aware and Beware of Identity Theft*, which can be found at ***www.fda.gov/fdac/departs/2005/405_fda.html#theft.***

National Institutes of Health (NIH): National Institute on Aging
The NIH's National Institute on Aging provides guidance to the elderly on matters related to identity theft in a publication entitled *Age Page—Crime and Older People*, which can be found at ***www.niapublications.org/agepages/PDFs/Crime_and_Older_People.pdf***.

Administration on Aging
HHS's Administration on Aging has supported the development of the following materials related to identity theft:

Protect Yourself from Identity Theft
www.consumerlaw.org/action_agenda/seniors_initiative/identity_theft.shtml

What You Should Know About Your Credit Report
www.consumerlaw.org/action_agenda/seniors_initiative/content/CFactsCreditReport.pdf

Protecting Older Americans from Telemarketing Scams: A Quick Guide for Advocates
www.consumerlaw.org/initiatives/seniors_initiative/concerns_telemarket.shtml

What To Do If You've Become The Victim of Telemarketing Fraud
www.consumerlaw.org/initiatives/seniors_initiative/telemarketing_fraud.shtml

Neremberg, L. (June 2003). Daily Money Management Programs—A Protection Against Elder Abuse
www.elderabusecenter.org/pdf/publication/DailyMoneyManagement.pdf

In addition, the Administration on Aging's Senior Medicare Patrol (SMP) program utilizes the skills and expertise of volunteers that educate and empower beneficiaries to take an active role in the detection and prevention of health care fraud and abuse, with a focus on the Medicare and Medicaid programs. The National Consumer Protection Technical Resource Center (***www.smpresource.org***) provides further information on the SMP program and a variety of consumer protection materials.

SECURITIES AND EXCHANGE COMMISSION (SEC)

www.sec.gov

The SEC's guidance to consumers on identity theft includes a publication entitled *Online Brokerage Accounts: What You Can Do to Safeguard Your Money and Your Personal Information*, which can be found at ***www.sec.gov/investor/pubs/onlinebrokerage.htm***.

PART F

PRIVATE SECTOR CONSUMER EDUCATION EFFORTS

The private sector has produced, promoted, and distributed an extensive library of consumer education materials in print and electronic formats to help consumers learn about various aspects of identity theft. Listed below are titles and links to a sample of individual organizations' identity theft consumer education materials, presented by sector.

Information Technology (IT)

Material produced by the information technology industry, most often delivered through the Internet, focuses largely on secure and safe computing, urging consumers to install anti-spyware, anti-virus, and firewall software on their computers, and educating them about the harm that can result from phishing, malware, and spyware. The information generally warns consumers against responding to spam and divulging personal information in email or on unsecured websites, and provides tips on creating strong passwords. For example, the National Cyber Security Alliance maintains Stay Safe Online, a website with tips on safe computing for adults and children.[26] In addition, much of the material is directed to warning consumers about the existence of phishing attacks and assisting consumers in spotting suspect emails and websites. Microsoft and Best Buy, along with several other private and public partners, sponsor the Get Net Safe Tour, in which experts visit schools, hold assemblies, parents nights, local community and senior events, and Internet fairs to discuss general Internet safety, including topics related to identity theft. Similarly, Americans for Technology Leadership, a coalition of technology professionals, consumers, and organizations, conducts Take Back The Net cybersecurity workshops, which include discussions of phishing and other identity theft-related topics, for consumers throughout the country.

AOL
Money & Finance—Identity Theft
money.aol.com/creditdebt/identity/

Microsoft
Security at Home: Protect Yourself
www.microsoft.com/athome/security/privacy/default.mspx

Earthlink
Earthlink Identity Protection Center
www.earthlink.net/mysecurity/identity/

E-bay
Tutorial: Spoof (fake) E-mails
www.pages.ebay.com/education/spooftutorial/

The National Cyber Security Alliance
Don't Take the Bait! Avoid Getting Hooked By "Phishers" Trying to Steal Your Personal Information
www.staysafeonline.org/basics/pharming_tips.html

The Anti-Phishing Working Group
www.antiphishing.org/phishing_archive.html

Consumer Advice: What To Do If You've Given Out Your Personal Financial Information
www.antiphishing.org/consumer_recs2.html

GetNetWise
www.getnetwise.org

The Business Software Alliance / Cybersafety
Phishing: Do you know if someone is trying to steal your identity?
www.bsacybersafety.com/index.cfm

Financial Institutions and Credit Providers

The financial services sector provides a great deal of information about common frauds related to identity theft, such as phishing, pharming, spoofing, pretext calling, and dumpster diving. Many institutions and credit card service providers also offer their customers information about identity theft prevention and remediation through statement stuffers, mailers, and websites. The information often includes explanations of common terminology and definitions related to these frauds, as well as explanations about how they work. The Texas Bankers Association, for example, produces inserts, posters, and wallet cards about identity theft for distribution to customers by Texas banks.[27] The Securities Industry Association publishes a booklet that informs investors of how to avoid identity theft and what to do if they are the victim of identity theft.[28] Securities self-regulatory organizations (SROs), such as the NASD and the NYSE, also publish guidance relating to identity theft. For example, NASD has published "*Phishing and Other Online Identity Theft Scams: Don't Take the Bait.*"[29]

MasterCard
Identity Theft
www.mastercard.com/us/personal/en/securityandbasics/identitytheft/index.html

Visa USA
Protect Yourself
www.usa.visa.com/personal/security/protect_yourself/index.html

Bank of America
Identity Theft and Your Rights
www.bankofamerica.com/privacy/Control.do?body=privacy secur_idprotect

Capital One
Find Out How To Protect Yourself From Fraud And Identity Theft
www.capitalone.com/fraud/

Chase
Identity Theft
www.chase.com/ccp/index.jsp?pg_name=ccpmapp/shared/assets/page/Identity_Theft

Citi
Protect Yourself
www.citibank.com/us/cards/cm/theft01.htm

Columbia Credit Union
Security and Identity Theft
www.columbiacu.org/identity/identity_tips.html

Commerce Bank
Identity Theft and Fraud
www.commercebank.com/about/privacy/identity.asp

U.S. Bank
Online Security
www.usbank.com/cgi_w/cfm/about/online_security/index.cfm

Virginia Credit Union
Security and Identity Theft
www.vacu.org/education/security.asp

Wells Fargo
Identity Theft
www.wellsfargo.com/privacy_security/fraud/operate/idtheft

Health Care Industry

The health care industry also provides information specifically about "medical identity theft," which occurs when an unauthorized individual uses someone's personal information either to obtain medical treatment, prescription medications, or other medical goods or to make false claims for medical services. While this type of identity theft is detrimental to the victim's financial status, it also can result in the exhaustion of health insurance coverage and the addition of false entries to the victim's medical record, incorrect medical treatment, or even the loss of a job if employers require physical exams and medical history checks.[30] Minneapolis-based health system Allina Hospitals and Clinics, targeted by an identity theft ring, produced a booklet to alert physicians and their staff on how to prevent patient identity theft, and to provide tips for medical professionals to protect themselves from becoming identity theft victims.

"Medical Identity Theft: the information crime that can kill you," Dixon, Pam. World Privacy Forum, Spring 2006.
www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf

ECRI—Operating Room Risk Management, Healthcare Identity theft: Prevention and Response. Mar. 2006.
www.ecri.org/MarketingDocs/0306news.pdf

Educational Institutions

For a variety of reasons, college students are frequent targets of identity thieves. Colleges and universities store vast amounts of personal information about students. According to one report, one-half to one-third of all reported personal information breaches in 2006 occurred at colleges and universities.[31] The student lifestyle also may contribute to the high rate of identity theft in this age group. College students tend to keep personal information unguarded in shared dorm rooms. In recognition of the increased vulnerability of the college population, many universities are providing information to their students about the risks of identity theft through websites, orientation campaigns, and seminars. The University of Michigan undertook a wide-scale effort, launching Identity Web, a comprehensive site based on the recommendations of a graduate class in the fall of 2003.[32] 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 Ohio 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.

The higher education community, including associations and financial institutions, also has conducted outreach to financial aid counselors, students, parents, and borrowers. For instance, the National Council of Higher Education Loan Programs (NCHELP) reached out to its constituents and encouraged them to take advantage of identity theft resources produced by the FTC and share them with students. Many college bookstores now provide these educational materials to students purchasing textbooks. The following links provide examples of universities' educational information on identity theft.

Harvard
www.hupd.harvard.edu/id_theft.php

Northwestern University
www.it.northwestern.edu/security/protectingprivacy/index.html

Pennsylvania State University
consumerissues.cas.psu.edu/PDFs/CreditPrivacyIdentity.pdf

Tulane University
www.tuhscpd.tulane.edu/Safety/idtheft.htm

University of California—Los Angeles
www.ucpd.ucla.edu/ucpd/programs_persafe.html

University of Kansas
www.privacy.ku.edu/idtheft/

University of Michigan
identityweb.umich.edu/

University of Minnesota
safecomputing.umn.edu/safepractices/idtheft.html

University of Missouri—Kansas City
www.umkc.edu/adminfinance/police/tips/Identity.asp

University of Oklahoma
www.ou.edu/oupd/idtheft.htm

University of Utah
www.it.utah.edu/leadership/security/identity.html

Yale
www.yale.edu/security/goodmeasures/ProtectingYourIdentity.html

PART G

RECENT LAWS RELATING TO IDENTIFICATION DOCUMENTS

Since 2004, two major federal laws have imposed significant new requirements relating to identification documents. First, the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004[33] improves identification information security and requires a national strategy for combating international terrorist travel. As part of this plan, the law contains provisions for robust travel document screening and authentication and for improved training for a variety of federal officials who come into contact with fraudulent identification documents. The law also requires that part of the strategic plan will be to disrupt terrorists' production and use of false travel documents. It also requires that the President lead international efforts to provide for the detection of counterfeit or stolen foreign travel documents and to criminally punish those involved in such crimes.

One section of the law focuses on biometrics. The law requires that biometric identifier technology be studied, included in airport access controls, and incorporated into a new, uniform law enforcement officer credential. The law also requires that a plan be developed to accelerate the full implementation of an automated biometric entry and exit system.

The law also focuses on improving identification documents, from requiring that improved pilots' licenses be developed to providing for the creation of federal standards for birth certificates, drivers' licenses, and personal identification cards. The law included security enhancements for Social Security cards, such as restricting the issuance of multiple replacement cards and establishing minimum standards for verification of documents. Additionally, the law prohibits the use of SSNs on drivers' licenses.

In addition, the Real ID Act of 2005[34] supplements the requirements of state drivers' licenses and identification cards for use by federal agencies. The law requires a number of verification measures before such an identification is issued, including that the state verify the validity of supporting documents. The law also mandates that identification cards used for federal purposes expire every eight years and be produced in secure environments by personnel with appropriate clearances. It further requires that state identification cards that do not meet the federal security requirements state so on their face, and that all states provide electronic access to other states of their motor vehicle databases.

Numerous government initiatives relating to authentication methods are described at ***www.biometrics.gov***.

PART H

STATE CRIMINAL LAW ENFORCEMENT EFFORTS

All 50 states and the District of Columbia have some form of legislation that prohibits identity theft, and in all of those jurisdictions, except for Maine, identity theft can be a felony. In general, 11 states appear to use a narrower approach to criminalizing identity theft by focusing on the use of personal identifying information with intent to defraud. Other states use a broader approach to criminalization that often includes not only unauthorized use, but also possession, creation, recording, obtaining, selling, giving, or transmitting of personally identifiable information.

State law concerning identity theft is changing rapidly. As one indication, several states have amended their criminal identity theft provisions within the last year. One of the trends has been to make criminal law more specific, for example, making it a separate crime to traffic in stolen identities or to engage in phishing.

Data from the 2005 National Survey of State Court Prosecutors indicate that state and local prosecutors are actively engaged in prosecuting identity theft. According to the survey, 69 percent of all prosecutors surveyed, and 97 percent of prosecutors surveyed from areas with populations of 1 million or more, had litigated at least one computer-related identity theft case. In addition, 80 percent of all prosecutors surveyed, and 91 percent of prosecutors surveyed from areas with populations of 1 million or more, had litigated a computer-related credit-card fraud case.[35]

These are just a few examples of state and local identity theft prosecutions:

- The Arizona Attorney General announced the arrest of a Phoenix resident, on suspicion of using Green Bay Packers quarterback Brett Favre's credit card more than 40 times. The defendant was charged with four felony charges and two other men were charged with forgery. The unauthorized charges to the credit card totaled more than $10,000, and the use of Favre's card is suspected to be part of a large identity theft scheme run by the other two men.
- The Florida Attorney General announced that two defendants pleaded guilty to identity theft for manufacturing counterfeit Florida drivers' licenses and checks in names that belonged to real and fictitious individuals.
- The Michigan Attorney General filed charges against two former nursing home employees who allegedly obtained a resident's personal information and used the information to obtain a Comcast account.

- The Missouri Attorney General and the Jefferson County Prosecuting Attorney charged an individual with two counts of identity theft. The defendant allegedly stole the identities of Missourians online to purchase and obtain thousands of dollars worth of merchandise and gift cards.
- The New York Attorney General announced the indictment of an individual for his role in an identity theft scheme that defrauded financial institutions of more than $1.5 million. The defendant allegedly obtained the personal identifying information of two Staten Island residents and, using their home as collateral, applied for and obtained home equity loans and lines of credit.

PART I

SENTENCING IN FEDERAL IDENTITY THEFT PROSECUTIONS

The United States Sentencing Commission has treated the problem of identity theft seriously. Among other things, the Sentencing Commission implemented a two-part sentencing guideline amendment in response to the Identity Theft Penalty Enhancement Act of 2004.[36] First, the Sentencing Commission promulgated a new guideline at Guidelines Section 2B1.6 for aggravated identity theft, effective November 1, 2005. The guideline provides that offenders convicted under the aggravated identity theft statute are to be sentenced to the term required by statute. In Fiscal Years 2005 and 2006, the Sentencing Commission received 55 and 163 cases respectively, with at least one conviction under the aggravated identity theft statute.[37] The aggravated identity theft cases in Fiscal Years 2005 and 2006 had average sentences imposed of 33 and 44 months, respectively.[38]

Second, the Sentencing Commission expanded the applicability of a Sentencing Guidelines provision that is aimed at enhancing the sentences of those defendants who abuse a position of trust or use a special skill to commit the crime. Specifically, the Sentencing Commission expanded the enhancement to apply to any defendant who ". . . exceeds or abuses the authority of his or her position in order to obtain unlawfully, or use without authority, any means of identification."[39] In Fiscal Year 2006, 0.6 percent of 18 U.S.C. § 1028(a)(7) offenders received offense level increases under this provision.

The U.S. Sentencing Commission maintains a comprehensive, computerized data collection system that forms the basis for its clearinghouse of federal sentencing information. Sentencing Commission data show that more than 1,000 offenders have been sentenced for convictions under the identity theft statute, 18 U.S.C. § 1028(a)(7), since it was enacted in October 1998. There has been a substantial increase in the number of sentenced cases with at least one count of conviction under 18 U.S.C. § 1028(a)(7) each year, from 12 cases in Fiscal Year 1999 to 195 cases in Fiscal Year 2006. Average sentences for these identity theft cases have increased steadily from an average of 16 months of confinement in Fiscal Year 1999 to an average of 25 months of confinement in Fiscal Year 2006.[40]

The following are some examples of identity theft cases prosecuted by DOJ in which federal courts have imposed substantial terms of imprisonment:

- On May 12, 2006, the U.S. District Court for the Western District of Missouri sentenced a man to 10 years imprisonment and ordered him to pay $126,180 in restitution, for participating in an identity theft-related wire fraud conspiracy that involved more than 50 victims in 17 states. The conspiracy involved stealing the identities of victims and using their credit card information to receive money wired by Western Union. Both the defendant and a codefendant targeted Citibank credit card holders and Western Union agents. When targeting individual card holders, the defendant would call Western Union, posing as the credit card holder, and request a money transfer. Prior to making this call, he used his extensive knowledge of how the telecommunications network operated to have the victim's home telephone line forwarded to a location where he could pose as the victim card holder when Western Union called back to verify the wire transfer. When targeting businesses that served as Western Union agents, the defendant would call Western Union posing as an employee of a Western Union agent, to initiate a fraudulent and fictitious wire transfer that would be picked up by either of the defendants. To facilitate the scheme, the defendant sometimes posed as a "fraud early warning" employee of the Citibank credit card company in order to obtain information on true Citibank credit card holders.[41]
- In December 2004, three defendants were sentenced for installing a computer program on the nationwide computer system used by Lowe's in order to steal credit card account numbers. To carry out this scheme, the defendants secretly compromised the wireless network at a Lowe's retail store in Southfield, Michigan, and thereby gained unauthorized access to Lowe's Companies, Inc.'s central computer system in North Wilkesboro, North Carolina and, ultimately, to computer systems located in Lowe's retail stores around the United States. Having gained this unauthorized access, the defendants then installed a computer program on the computer system of several Lowe's retail stores, which was designed to capture the credit card information of customers conducting transactions with those stores. The lead defendant in the case received a sentence of 108 months imprisonment.
- On June 23, 2006, in the U.S. District Court for the Eastern District of Missouri, the leader and organizer of an identity theft ring and her two daughters were sentenced (respectively) to 70 months imprisonment; 2 years and 1 day imprisonment; and 4 years probation (with home confinement) on aggravated identity theft, identity theft, and related fraud charges, in a scheme to use stolen identities to open credit accounts and purchase merchandise. Some of the documents seized during the investigation came from patient records through one daughter's employment at a St. Louis area dental office. The entire

scheme resulted in losses exceeding $47,000 as a result of more than 252 fraudulent credit applications. More than 67 individuals had their identities compromised as a result of the fraud.

- In October 2004, the Secret Service arrested 21 individuals on charges relating to their involvement in "Shadowcrew." "Shadowcrew" was an international criminal organization with numerous members that promoted and facilitated various criminal activities including the electronic theft of personal identifying information, credit-card and debit-card fraud, and the production and sale of false identification documents. The organization operated a website with approximately 4,000 members that was dedicated to facilitating malicious computer hacking and disseminating stolen credit card, debit card, and bank account numbers, and counterfeit identification documents, such as driver's licenses, passports, and Social Security cards. In July 2006, one of the participants in Shadowcrew was sentenced to 90 months imprisonment.[42]

- In December 2005, a California man convicted of orchestrating a credit-card fraud scheme that involved skimming was sentenced to 87 months imprisonment and ordered to pay $140,000 in restitution to more than 50 identified victims of his scheme. In this case, which the Secret Service investigated, the defendant employed a waitress who worked at two restaurants to use a "skimmer" device and other means to obtain credit-card information. When federal agents searched the defendant's home, they found more than 1,500 stolen credit-card account numbers and software and hardware to download the account information on to blank credit card stock.[43]

- The IRS has pursued a number of identity theft prosecutions. For Fiscal Year 2005, in 25 identity theft cases where defendants were convicted and sentenced, the average prison sentence imposed was 41 months. For Fiscal Year 2006 (through June 30, 2006), 18 persons were convicted and sentenced in cases involving identity theft, and the average prison sentence received was 38 months.

PART J

INVESTIGATIVE APPROACHES TO IDENTITY THEFT: SPECIAL ENFORCEMENT AND PROSECUTION INITIATIVES

Each agency responsible for the investigation of identity theft tracks its identity theft cases independently. By any measure, however, it is clear that the federal investigative agencies have been aggressively pursuing identity theft. The FBI reports that as of September 30, 2006, it had 1,274 pending identity theft-related cases, and that it opened 493 identity theft-related cases in Fiscal Year 2006. The USPIS reports that it opened 1,269 identity theft cases and made 1,647 arrests in Fiscal Year 2006. The USSS reports that it made 3,402 identity theft arrests in Fiscal Year 2006. The Social Security Administration (SSA) Office of the Inspector General's (OIG) Office of Investigations reports that it opened 1,482 cases involving SSN misuse[44] in Fiscal Year 2006, and 412 cases involving SSN misuse from October 1, 2006 through January 31, 2007 in FY 2007.

SPECIAL ENFORCEMENT INITIATIVES

Many agencies involved in the investigation of identity theft have also undertaken special enforcement initiatives in recent years, including the following:

FBI

The FBI Cyber Division has conducted a number of investigative initiatives into various types of online crime that involve identity theft:

- **Operation "Retailers & Law Enforcement Against Fraud" (RELEAF):** RELEAF is an international investigative initiative directed at the related problems of "reshipping" (i.e., the use of one or more people to receive merchandise that criminals have fraudulently ordered from retailers, often using others' credit cards, and ship that merchandise to other participants in the fraud scheme to evade detection by retailers and law enforcement) and money laundering. This initiative involves more than 100 private sector participants and numerous law enforcement agencies and has produced more than 150 investigations.
- **Digital Phishnet:** Digital Phishnet is a phishing and identity theft initiative involving more than 60 organizations (banks, ISPs, and ecommerce companies) that assisted in the development of more than 100 investigations.
- **Operation Slam Spam:** Operation Slam Spam is a criminal spam and malicious code investigative initiative that is supported daily by more than 20 small and medium enterprises. An anti-spam email list provided intelligence on current cyber crimes, which involved over 95 industry members. In addition, 12 industries provided analysts who are co-

located with the Internet Crime Complaint Center (IC3) and Cyber Initiative and Resource Fusion Unit (CIRFU) to support this project, which resulted in more than 100 investigations.

In addition, as identity theft becomes more global in scope and impact, the FBI has provided some foreign law enforcement agencies with identity theft-related assistance and training in the execution of specific enforcement initiatives. Initial efforts in this context have already proved highly productive, and include the following:

- The FBI Legal Attaché in Bucharest contributed to the development and launching 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 Attaché 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 Attaché assisted the Romanian police and Ministry of Justice to prosecute Romanian subjects.
- Following up on the success of IC3's Operation RELEAF, IC3 and FBI Cyber Units developed and presented a "Cyber 101" course to law enforcement officials in Ghana and Nigeria. This course had immediate results, in the form of aggressive foreign law enforcement action to support FBI investigations, including the seizure of millions of dollars in stolen merchandise and fraudulent cashier's checks.

United States Secret Service

The USSS has approximately 15 online undercover investigations targeting suspects who are trafficking in government-issued documents (driver's licenses, Social Security cards, U.S. and foreign passports and visas). These suspects reside both within the United States and abroad. In the next year, the Secret Service intends to continue its undercover operations targeting these groups, increase its arrests of these suspects, and disrupt the online sale and distribution of stolen personal and financial information.

Internal Revenue Service—Criminal Investigation

IRS CI's Questionable Refund Program (QRP) and Return Preparer Program (RPP) are focused on identifying and stopping fraudulent tax refund claims schemes. These schemes often involve hundreds of returns, with refunds totaling hundreds of thousands or even millions of dollars of revenue at stake. These schemes can create significant problems for legitimate taxpayers by denying them refunds to which they would be entitled. Investigating and prosecuting those responsible for these ambitious schemes ranks among these programs' highest priorities. Although identity theft is not a component of all fraudulent refund schemes, the rise of identity theft has helped fuel an increase in fraudulent refund schemes and other tax frauds, specifically employment tax fraud. In Fiscal Year 2006, IRS-CI had 77 cases involving identity theft under active investigation. The IRS is also developing improved screening and detection processes to more effectively identify future fraudulent refund schemes.

Treasury Inspector General for Tax Administration

TIGTA's role in combating identity theft is protecting the privacy and security of confidential taxpayer data entrusted to the IRS. The integrity of IRS's information systems is fundamental to federal tax administration. A breach of IRS computer databases leading to identity theft would be devastating to the nation's voluntary tax system and the government's ability to collect taxes. TIGTA's Strategic Enforcement Division (SED) utilizes both proactive and reactive investigative methods to detect and deter unauthorized accesses (UNAX) to taxpayer information by IRS employees and by those who try to hack into IRS computer databases. SED administers a variety of audit trail and computer matching tools to proactively identify UNAX violations that could lead to identity theft. TIGTA's System Intrusion Network Attack Response Team (SINART) was formed to detect and investigate intrusions into IRS systems and information technology equipment. In fiscal year 2006, TIGTA initiated 488 investigations into suspected UNAX violations, and its investigations in fiscal year 2006 resulted in 385 referrals to DOJ for criminal prosecution and 409 administrative disciplinary actions.

Department of State—Bureau of Diplomatic Security

Since 2005, the State Department's Bureau of Diplomatic Security (DS) has been working on an initiative to address the use of identities of deceased people to obtain U.S. passports. As part of this initiative, some of the DS field offices have had several arrests and successful prosecutions, including some asset forfeiture cases. Some of these investigations resulted in the arrests of fugitives who had assumed the identities of others many years earlier to flee justice. DS plans to expand this initiative to all of its field offices.

One example of the value of this initiative involves the prosecution of Christopher J. Clarkson. On March 15, 2006, Clarkson pleaded guilty in Florida to bank fraud and was required to forfeit $500,000 in assets. Clarkson was a member of a widely known gang of bank robbers who reportedly robbed more than 100 banks and armored cars in the 1970s and 1980s in both Canada and the United States. For nearly 30 years, Clarkson used the identity of Stephen Duffy, a boy who lived in California and died there at age 4 in 1948. Using Duffy's identity, which he apparently had stolen in the late 1970s, Clarkson lived in Hollywood, Florida, and worked as a successful real estate broker. DS investigators found irregularities in "Duffy's" California driver's license because of the year of the true Duffy's death. Further investigation, including the discovery that Clarkson had applied for a passport in Duffy's name, led DS agents and Florida law enforcement to arrest Clarkson in October 2005.

SPECIAL PROSECUTION INITIATIVES

Since 2002, DOJ has conducted a number of enforcement initiatives targeting identity theft. The first of these initiatives, in May 2002, involved 73 criminal prosecutions by United States Attorney's Offices against 135 individuals in 24

districts. The cases in that initiative covered a broad range of fraud schemes such as mortgage fraud and securities fraud. 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 on 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. The cases in Cyber Sweep included phishing schemes and other efforts to use stolen credit cards to buy computer equipment online.[45]

In addition to these general enforcement initiatives, various United States Attorney's Offices have established their own identity theft initiatives:

- **"Fast Track" Program.** The District of Oregon has an identity theft fast track program that requires eligible defendants both to plead guilty to aggravated identity theft under 18 U.S.C. § 1028A(a)(1) and to agree, without litigation, to a 24 month minimum mandatory sentence. In exchange for their pleas of guilty, defendants are not charged with the predicate offense which would otherwise result in a consecutive sentence under the United States Sentencing Guidelines. The program is intended to capture cases that are smaller than the typical federal identity theft cases, but larger than typical state-level cases. Generally, in order for a defendant to be eligible for the program, the actual or intended loss, whichever is higher, must be more than $5,000 and less than $70,000. If the loss is less than $5,000, the defendant must be a manufacturer of fraudulent identification documents or the defendant's criminal activity must create a disproportionately adverse impact in the community. The offense must have 10 or more victims, but less than 50 victims, from multiple jurisdictions. Finally, there must be no applicable organizer, leader, manager, or supervisor adjustments under section 3B1.1 of the federal Sentencing Guidelines. The program relies upon a network of local investigators and prosecutors to identify eligible defendants, referring them to agents of the FBI, USSS, and the USPIS for follow-up work, and ultimately to designated Assistant U.S. Attorneys for federal prosecution.
- **"Operation Checkmate."** Two United States Attorney's Offices have collaborated on a special initiative to combat passport fraud, known as Operation Checkmate. Because approximately one-quarter of the 8.8 million passports issued by the State Department in 2004 were issued at the National Passport Center in Portsmouth, New Hampshire, the United States Attorney's Office for the District of New Hampshire initiated Operation Checkmate in collaboration with the State Department's Bureau of Diplomatic Security, ICE, and SSA OIG. Operation Checkmate aims to deter passport fraud by improving fraud detection efforts and dedicating resources to prosecuting these crimes.

Most evidence and witnesses are located where the fraudulent passport applications are detected by State Department passport adjudicators. Districts that are home to adjudication centers therefore are logical choices for prosecuting passport fraud cases, in addition to the districts where the perpetrators temporarily, and often illegally, reside. For these reasons, the United States Attorney's Offices in New Hampshire and South Carolina, where the largest passport centers are located, agreed to supply the additional prosecutorial resources necessary to support increased enforcement efforts.

PART K

HOW LAW ENFORCEMENT OBTAINS AND ANALYZES IDENTITY THEFT DATA

With the increased attention given to identity theft in recent years, federal law enforcement agencies have recognized the importance of the timely receipt, analysis, and referral of identity theft information, including complaints by identity theft victims. Currently, there are many different sources of identity theft data, and several different ways in which that data is being analyzed.

THE GENERAL PUBLIC AS A SOURCE OF INFORMATION

Identity Theft Data Clearinghouse (FTC)

The Identity Theft and Assumption Deterrence Act of 1998 directed the FTC to develop the federal government's centralized education and assistance program. Now, the FTC provides a federal "one-stop shop" for consumers and victims.

As a result, a wide variety of entities refer consumers to the FTC through its identity theft website and toll-free help line. The credit reporting agencies, credit card issuers, financial institutions, several federal agencies, several states' Attorneys General, and numerous local law enforcement agencies all refer consumers to the FTC. In 2006, the FTC recorded more than 4.2 million visits to its Identity Theft website (***www.ftc.gov/idtheft***) and more than 590,000 visits to the web version of its victim recovery guide, *Take Charge: Fighting Back Against Identity Theft*, as well as 113,000 visits to its Spanish-language website (***www.consumer.gov/idthet/espanol.htm***), and 55,000 visits to the Spanish-language version of its victim recovery guide.

The number of identity theft victims filing complaints with the FTC is similarly substantial. In 2006, the FTC logged in 246,035 new identity theft complaints. The complaints are promptly added to the Clearinghouse, which currently contains more than one million consumer complaints. Analysts from the FBI and the USPIS routinely work on site at the FTC to mine the Clearinghouse data to identify new leads or expand upon existing leads.

The FTC also provides remote access to the Clearinghouse data, and actively encourages law enforcement at all levels to use its complaints for their investigations and analysis. Local, state, and federal law enforcement officers can remotely access the Clearinghouse by a secure online connection. Officers and agents can query the data to identify significant clusters, leading to suspected perpetrators and targets, as well as to detect patterns and trends for further investigation. In addition, users can set the Clearinghouse's "Autoquery" program to notify them any time new data is entered that matches their specified parameters. The Clearinghouse also has a deconfliction tool: the officer can place an "Alert" on information relating to their investigations to notify other users that the officer is working with this information and would like to be contacted.

The FTC continues to work to simplify the victim's recovery process. One example is the Identity Theft Affidavit, which is posted on its website. The Identity Theft Affidavit was the result of the FTC working with industry and consumer advocates to create a standard form for victims to use in disputing identity theft accounts. Since its inception in 2001, more than 1.5 million hits to the English version and more than 62,000 hits to the Spanish version have been recorded.

Internet Crime Complaint Center (IC3) (FBI/National White Collar Crime Center) and Cyber Initiative and Resource Fusion Unit (CIRFU)

Another conduit for complaints about internet-related fraud and identity theft is the IC3. IC3 is a joint venture between the FBI and the National White Collar Crime Center (a nonprofit organization, funded by the DOJ's BJA, that, among other things, disseminates information on cybercrime and actionable cyber-related investigative leads to state and local law enforcement). The IC3 provides an important means of collecting, analyzing, and disseminating to law enforcement information about crimes committed over the Internet. The IC3 receives more than 20,000 complaints per month from Internet users. For Internet victims, the IC3 provides a convenient and easy means of alerting authorities to a suspected criminal violation, including online identity theft. For law enforcement and regulatory agencies, it offers a central repository for complaints related to Internet crimes and allows them to use the information to obtain timely statistical data and current crime trends.

A special component of the FBI that works closely with the IC3 is the CIRFU. The CIRFU, based in Pittsburgh, is housed within the National Cyber Forensic Training Alliance (NCFTA), a public/private alliance and fusion center. The CIRFU and NCFTA maximize intelligence development and analytical capabilities by combining resources from law enforcement with those of critical industry partners. Such resources are utilized to substantially enhance the development and support of joint initiatives aimed at new and/or high-profile cybercrime problems. It also fosters the development of public/private alliances and joint training in support of these investigative initiatives.

Other Government Agencies

Other federal law enforcement agencies also have processes to receive and analyze complaints from the public. For example, the USPIS uses the Financial Crimes Database (FCD), a web-based national database that is available to all inspectors for use in analyzing mail theft and identity theft complaints received from various sources, including, but not limited to, the financial industry (American Express, Discover, MasterCard, Visa); major mailers (Netflix, Blockbuster, GameFly); the Identity Theft Assistance Center (ITAC) complaints; on-line mail theft complaints, USPIS field offices, Corporate Customer Contact (1-800-ASK-USPS) telephone complaints; and U.S. Treasury Checks. The USPIS receives approximately 1,000 identity theft complaints per month that are entered into the FCD. Additionally, the SEC's

Enforcement Complaint Center receives approximately 5,000 to 7,000 complaints per day on all types of securities law violations, including those that involve account intrusion and identity theft.

When HHS receives complaints that involve allegations of telemarketing fraud and misuse of Part D beneficiaries' personal information for unauthorized bank transactions, it refers many of them to the FBI because the HHS OIG does not have primary jurisdiction over the identity theft offense (18 U.S.C. § 1028) or the wire fraud offense (18 U.S.C. § 1343). Even though beneficiaries may voluntarily disclose their personal information in connection with a transaction they believe they are authorizing, any unauthorized and fraudulent use by the telemarketers of the beneficiaries' information may constitute identity theft. HHS also refers to the Criminal Division of DOJ and to the FBI complaints that raise the possibility of identity theft from sources other than Medicare or its other payment programs. These complaints are received by HHS pursuant to its administrative enforcement of the HIPAA Privacy and Security Rules.

Public and Private Sector Collaborations

To improve information sharing and cooperation between law enforcement and private sector entities on online identity theft and fraud matters, IC3 and CIRFU representatives have been meeting with representatives from a number of industry coalitions combating online fraud, including: the Merchants Risk Council, the Business Software Alliance, as well as numerous financial services and other e-commerce stake holders, regarding co-location of analysts at both locations. Target Corporation (which in addition to being a merchant is also a bank and credit card issuer) and the USPIS have assigned full-time fraud investigators to work at both IC3 and/or CIRFU, with eBay and other organizations agreeing to rotate personnel through IC3 and/or CIRFU. Other law enforcement agencies have been invited to place personnel in both locations to further enhance cooperation among such agencies.

The Secret Service hosts a portal called the e-Information system for members of the law enforcement and banking communities. This system provides a forum for members to post the latest information on scams, counterfeit checks, frauds and swindles, and updated Bank Identification Numbers (BINs). It is widely used and receives a tremendous amount of positive comments from users.

In 2005, the USPIS created the Intelligence Sharing Initiative (ISI), a website that allows the Inspection Service and fraud investigators representing retail and financial institutions, as well as major mailers, to openly share information pertaining to mail theft, identity theft, financial crimes, investigations, and prevention methods. ISI interacts with the Financial Crimes Database and generates Alert Reports. These reports are posted to assist the industry in identifying "high risk" areas, closing suspect accounts, and saving thousands of dollars in potential fraud.

ISI also gives the users access to the "Hot Addresses List," i.e., a list of addresses located throughout the United States and Canada linked to a variety of fraud schemes, including fraudulent application schemes, account takeover schemes, mail order schemes, and reshipping schemes. The "Hot Addresses List" is published monthly and distributed by postal inspectors to the retail and financial industry, federal law enforcement, and government agencies and is also posted on the FTC's Identity Theft Data Clearinghouse for law enforcement use. This intelligence sharing has resulted in a reduction in fraud schemes and significant savings to the retail and financial industries.

PRIVATE SECTOR AS A SOURCE OF INFORMATION

Financial Services Industry

The financial services industry is an important source of identity theft data for law enforcement agencies. The financial services industry provides that information in a number of different ways, some of which are detailed below.

▶ Suspicious Activity Reports

A significant source of identity theft information is already available to federal law enforcement through Suspicious Activity Reports (SARs). In general, a federally regulated financial institution is required to file SARs with the Department of the Treasury's FinCEN for certain suspected violations of the law, including identity theft, and for suspicious transactions involving funds or assets of at least $5,000 (e.g., transactions that involve potential money laundering or Bank Secrecy Act violations).

To make more effective use of SAR data, the FBI has begun a SAR Exploitation Project. The Project is designed to identify financial patterns and criminal groups associated with identity theft, financial institution fraud, and other aberrant financial activities. Using SAR data from FinCEN, the Project analyzes financial information that is available but not readily exploitable for FBI investigators to generate leads for the field investigators. Analytical software enables analysts to visualize financial patterns, link discrete criminal activities, and display the activities on link charts. Leads developed from analysis of SAR activity may be instrumental in "connecting the dots" for cross-program investigations of criminal, terrorist and intelligence networks, all of which rely on financial transactions to operate. The Secret Service is also using SAR data to investigate identity theft crimes.

▶ Identity Theft Assistance Center (ITAC)

The ITAC is a nationwide cooperative initiative of the financial services industry that provides a free victim assistance service for customers of member companies. ITAC is run by the Identity Theft Assistance Corporation, a not-for-profit membership corporation sponsored by two other private-sector organizations, The Financial Services Roundtable and BITS. Currently, 48 financial services industry companies participate in ITAC. ITAC

helps victims of identity theft by facilitating the recovery process. First, the identity theft victim and the ITAC member company resolve any issues at that company. An ITAC counselor walks the consumer through his or her credit report to find suspicious activity, notifies the affected creditors, and places fraud alerts with the credit bureaus. In addition, ITAC shares information with law enforcement and the FTC to help catch and convict the criminals responsible for identity theft. Since opening its doors in August 2004, ITAC has helped approximately 13,000 consumers restore their financial identities.

ITAC has data sharing agreements with the USPIS and the FTC under which it provides those agencies, on a weekly basis, with information about victims and the circumstances of their identity theft incidents. The USPIS has loaded information into its Financial Crime Database, and the FTC adds the ITAC data to its Identity Theft Data Clearinghouse.[46]

▶ Credit Reporting Agencies

Section 621(f)(3) of the Fair Credit Reporting Act (FCRA) requires that the nationwide consumer reporting agencies (CRAs) submit an annual summary report to the FTC "on consumer complaints received by the agency on identity theft or fraud alerts." The three nationwide CRAs—Experian, Equifax, and TransUnion—have recently submitted their first set of annual reports to the Commission covering the 13-month period from December 1, 2004, the effective date of the FACT Act provision, through December 31, 2005. Review of the data by FTC staff is underway. Section 621(f)(3) of the FCRA does not require the FTC to report on the data submitted to it by the CRAs.

The first set of reports includes five categories of information: (1) the number of initial fraud alerts placed; (2) the number of extended fraud alerts placed; (3) the number of active duty alerts placed; (4) the number of inaccurate trade lines or items blocked from consumers' credit reports as a result of the consumer providing an "Identity Theft Report"; and (5) the number of accounts or items disputed as inaccurate as a result of identity theft or fraud.

Reports of Database Intrusions Mandated by Federal and State Law

Another potential source of reports on identity theft are reports that various state laws mandate for database intrusions. In addition, under federal securities and financial reporting laws, such as the Sarbanes-Oxley Act of 2002, publicly traded companies may be obligated to report any known instances of breaches, intrusions, or compromises of personal data that they control. As an example of how a similar regulatory regime may operate in other countries, in January 2006, the corporate owner of the Bahamian hotel resort Atlantis filed a document with the Bahamas SEC, reporting that data on approximately 55,000 customers of Atlantis were missing from Atlantis's computer database. The data, which included names, addresses, credit card and bank account information, SSNs, and driver's license numbers, were reportedly obtained by a hacker.[47]

PART L

FEDERAL LAW ENFORCEMENT OUTREACH EFFORTS

Federal law enforcement agencies have been supportive of the need to involve state and local law enforcement and the private sector in combating identity theft. The FBI, the USSS, the USPIS, and ICE, for example, all conduct outreach to and work with state and local law enforcement agencies on identity-theft matters, whether through interagency task forces or direct contacts from field offices. Additionally, several agencies have partnered with private sector entities to do outreach to consumers and others. Those efforts include the following:

- **"Operation: Identity Crisis."** In 2003, the USPIS partnered with the FTC and the USSS (with support from various other agencies) to educate American consumers about the ease with which identity theft occurs and how to prevent it. A multi-media effort included advertisements in 17 newspapers; a 3 million piece educational mailing; public service announcements; posters displayed in 38,000 Post Office lobbies as well as in lobbies of police departments, banks, and other financial institutions throughout the country; and release of a USPIS prevention DVD entitled "*Identity Crisis*."
- **"Operation Identity Shield."** In 2005, the FBI, the USPIS, IC3, the National White Collar Crime Center, the FTC, Merchants' Risk Council, Monster.com, and Target began an initiative to educate U.S. consumers about how to protect themselves and their personal information from the reach of online scam artists. A multi-media effort included the release of a free USPIS prevention DVD, "*Web of Deceit*," to update and inform consumers about new and evolving identity theft schemes that they may encounter; a posting of a joint law enforcement/industry website, ***www.LooksTooGoodToBeTrue.com***, to provide educational and prevention information; magazine ads with a combined circulation of over 22 million; newspaper and radio spots; banner ads on each magazine's website with links to the USPIS website; message inserts in stamp fulfillment orders; and a full-page ad placed in the October issue of the *Police Chief* magazine. This initiative also allows consumers to provide law enforcement authorities with valuable intelligence to assist in combating the problem.
- **Identity Theft Enterprise Strategy.** The IRS Identity Theft Program Office has adopted the Identity Theft Enterprise Strategy as a comprehensive approach to combating identity theft by focusing on outreach, prevention, and victim assistance. The outreach component seeks to alert and inform tax professionals, taxpayers, and other interested parties of the threat that identity theft poses to tax administration. The prevention component's objective is to proactively

address identity theft within the context of tax administration. An example of these activities is the IRS's efforts to identify and deter "phishing" schemes before taxpayers are victimized. The third component of the strategy is victim assistance, the important task of mitigating and correcting the harm suffered by taxpayers who are victims of identity theft.

- To address identity theft relating to health care, HHS Centers for Medicare and Medicaid Services (CMS) uses Consumer Alerts, press releases, speeches to beneficiary, provider, and health care industry associations, and cable television programs to educate the beneficiary and provider communities and alert them to emerging problems. CMS Alerts publicize the telephone number for victims to call to report Medicare scams (1-800-HHS-TIPS) and prescription drug fraud (1-877-7SAFERX or 1-877-772-3379), and contain specific tips for people with Medicare to protect themselves against scams. CMS also issues reminders to its contractors, providers, and beneficiaries, similar to internal departmental reminders to HHS employees, to inform them of their responsibility to protect private information and of actions they should take to keep data secure. CMS recently issued prescription drug compliance guidance similar to that previously issued by HHS OIG for other health care providers (e.g., hospitals, nursing homes, home health agencies, physicians in private practice, laboratories, and durable medical equipment suppliers) that includes safeguarding of beneficiary and provider information. Finally, CMS staff speak at national and local provider, beneficiary, and prescription drug plan associations and partner with the U.S. Administration on Aging, Area Agencies on Aging, and community outreach agencies to spread the word about scams and how to report complaints. CMS regularly participates in conferences sponsored by the National Health Care Anti-Fraud Association with federal, public, and private sector representatives involved in health care fraud and abuse.

In addition, federal law enforcement agencies have frequently established direct lines of communications on fraud and identity theft issues with various companies and financial institutions in various cities throughout the United States:

- The FBI, for example, has established Infragard, a national information sharing network between the FBI, an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States infrastructures. Infragard has more than 11,800 members in 79 chapters throughout the United States. Infragard's goals, at both the national and local levels, include increasing the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cybercrime, and other major crime programs,

and increasing interaction and information sharing among InfraGard members and the FBI regarding threats to the critical infrastructures, vulnerabilities, and interdependencies.

- U.S. Immigration and Customs Enforcement (ICE) conducts outreach programs to employers to provide them with training in identifying fraudulent documents.

One of the most productive approaches that the public and commercial sectors have been using to deal with identity theft and identity fraud issues is the creation of multi-sectoral working groups, organized by private companies, that provide a common forum for discussion of technological and other solutions to identity fraud with each other and with government agencies. The following descriptions of two multi-sectoral working groups interested in identity theft indicate the types of approaches that such groups can develop to address various aspects of identity fraud:

- **Anti-Phishing Working Group.** The APWG is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. The APWG has more than 2,300 members and more than 1,500 companies and government agencies participating in the APWG's activities. It provides a forum to discuss phishing issues, define the scope of the phishing problem in terms of hard and soft costs, and share information and best practices for eliminating the problem. Where appropriate, the APWG will also look to share this information with law enforcement. Membership is open to qualified financial institutions, online retailers, ISPs, the law enforcement community, and solutions providers. Certain members of the APWG have worked closely with federal law enforcement on other initiatives, such as Digital Phishnet.
- **Liberty Alliance.** Formed in September 2001, the Liberty Alliance is a global consortium of more than 150 leading merchants, service providers, technology vendors, and government organizations that work together to address the technical and business issues associated with developing an open standard for federated network identity. The Alliance is engaged in the ongoing release of open technical specifications as well as business and policy guidelines to help companies deploy federated identity services across a broad range of products, services, and devices.[48] Recently, the Alliance has held workshops on identity theft prevention in Chicago, Illinois, and Tysons Corner, Virginia. These workshops brought together law enforcement and private sector representatives to explore potential technological and procedural solutions to the problem of identity fraud.

Other groups and initiatives that facilitate productive discussions between law enforcement and the private sector include:

- **International Association of Financial Crimes Investigators.** The International Association of Financial Crimes Investigators (IAFCI) is a non-profit international organization that engages in training and information-sharing about financial fraud, fraud investigation, and fraud prevention methods. Its members are drawn from law enforcement, the banking and credit-card sectors, and other companies. IAFCI members have access to the IAFCI Network, a secure international electronic fraud information network that allows them to broadcast warnings to all participating members and request investigative assistance; a complete International Membership Directory listing invaluable investigative contacts worldwide; quarterly newsletters that alert IAFCI members to the latest schemes of fraud criminals; and the IAFCI International Annual Training Seminar, where members can learn a variety of fraud prevention techniques, as well as the latest technological advances and in-the-field instructions to stop fraud.

- **Financial Industry Mail Security Initiative.** In 1992, the USPIS started a Credit Card Mail Security Initiative (CCMSI) in an effort to work more effectively with the credit card industry. A coordinated crime prevention effort was needed to reduce fraud losses and allow law enforcement to concentrate investigative attention on organized criminals. Results were immediate; non-receipt fraud losses were reduced 35 percent in 1993 when compared with 1992. This reduction in loss trend has continued into 2006. In 2003, the USPIS broadened the scope of the meetings and included other significant trends that were taking place, such as counterfeit check schemes, internet fraud, and bank fraud schemes. Since the focus expanded, the name of the group was changed from the Credit Card Mail Security Initiative to the Financial Industry Mail Security Initiative (FIMSI). This group meets three times annually and provides a forum in which agency representatives can identify and share trend data. Representatives from the retail/financial industry, and federal, state, and local law enforcement agencies participate in these meetings. Timely presentations on current trends are given at these meetings by experts in their respective fields.

Working groups are created from these meetings to address specific problems and share best business practices. Examples of these working groups include Non-Receipt, Plant Security, Identity Theft, Convenience Checks, Nigerian Crimes, Skimming, Internet Fraud, and Address Validation. Through these working groups, the USPIS has been responsible for several preventive initiatives. Some of those initiatives are Card Activation where the consumer must call to activate a credit card that he receives through the mail; and the Inspection Service's full use of the National Change of Address service and Address Change Service to the Credit Card Industry, which prevents the fraudulent use of changes of address. It also identified addresses belonging to Commercial Mail Receiving Agencies and other mail drops. These services

reduced the risk of sending credit cards and other access devices to fraudulent addresses and vacant properties.

Working groups were also responsible for the development and publication of the Identity Theft Brochure, Publication 280, *Identity Theft: Safeguard Your Personal Information*, and the publication of the best practices guide, *Fighting Identity Theft, Best Practices for the Financial Industry, Law Enforcement Agencies, Prosecutors, and Consumer Awareness Groups*. In addition, the USPIS publishes a FIMSI newsletter three times annually for law enforcement and the financial services and retail industries. It contains information of relevance to financial crimes investigators, significant investigations, upcoming training, identity-theft articles, and a nationwide list of USPIS coordinators. These meetings have identified a number of new prevention strategies. Many of these strategies were implemented by the financial industry and have resulted in reduced fraud losses for them.

Finally, various agencies have had some success in sharing identity theft information with state and local law enforcement authorities through forums other than multiagency task forces. HHS OIG, for example, participates in an information sharing national teleconference that has produced a number of helpful tips to state Attorneys General by providing them with 800 numbers, names used and the names of organizations behind telemarketing fraud schemes directed at Part D beneficiaries, as well as processors of the electronic transfers through which those schemes were conducted.

PART M

INVESTIGATIVE APPROACHES TO IDENTITY THEFT: INTERAGENCY WORKING GROUPS AND TASK FORCES

A number of federal, state, and local law enforcement authorities have found multi-agency task forces or working groups especially valuable in investigating identity theft. Task forces typically share intelligence and investigative information about leading identity theft activities, groups, and offenders in their region, facilitate coordination among law enforcement agencies in the same area, and enable participating agencies to make the most efficient use of their respective resources to pursue significant identity theft cases. In addition, a few of these task forces have dedicated office space, where agents from different agencies can meet to exchange information and work together, and a prosecutor who is regularly assigned to handle task force cases.

Federal authorities lead or co-lead more than 90 task forces and working groups devoted (in whole or in part) to identity theft:

- **United States Attorney's Offices:** U.S. Attorneys lead approximately 17 identity theft task forces and working groups in cities such as Philadelphia, St. Louis, and Eugene, Oregon. Approximately 27 U.S. Attorney's Offices participate in identity theft task forces or working groups, one U.S. Attorney's Office participates on a task force that investigates identity theft, but also other white collar crime, and other U.S. Attorney's Offices are in the process of forming an identity theft task force or working group.
- **FBI:** The FBI leads four identity theft task forces, and participates in 21 identity theft/financial crimes task forces or working groups in most of the major metropolitan areas. In addition, the FBI's Cyber Division has more than 90 task forces and more than 80 working groups, consisting of federal, state, and local law enforcement personnel, that investigate all cybercrime violations, including identity theft and Internet fraud.
- **U.S. Secret Service:** The Secret Service has 29 Financial Crimes Task Forces and 24 Electronic Crimes Task Forces that focus, to varying degrees, on identity theft-related crimes. The Financial Crimes Task Forces are controlled through Secret Service offices in Atlanta, Austin, Baltimore, Charlotte, Chicago, Cleveland, Dallas, Ft. Myers, Houston, Jacksonville, Kansas City, Las Vegas, Little Rock, Memphis, Miami, New Orleans, Newark, Norfolk, Oklahoma City, Omaha, Orlando, Riverside, San Antonio, San Diego, St. Louis, Springfield, Tampa, Tulsa, and Washington, D.C. The Electronic Crimes Task Forces are located in Atlanta, Baltimore, Birmingham, Boston, Buffalo, Charlotte, Chicago, Cleveland, Columbia (South Carolina), Dallas, Houston, Las Vegas, Los Angeles, Louisville, Miami, Minneapolis, New York City,

Oklahoma City, Orlando, Philadelphia, Pittsburgh, San Francisco, Seattle, and Washington, D.C.[49]

- **U.S. Postal Inspection Service:** The Postal Inspection Service actively leads 14 Financial Crimes Task Forces/Working Groups in the following places: Atlanta, Birmingham, Boston, Hawaii, Los Angeles, Memphis, New York, Northern Kentucky, Philadelphia, Phoenix, Pittsburgh, Richmond, Springfield, and St. Louis. The Postal Inspection Service is also the co-leader of task forces in Chicago, Salt Lake City, St. Paul/Minneapolis, and Oklahoma City.
- **U.S. Immigration and Customs Enforcement (ICE):** ICE has established Document and Benefit Fraud Task Forces (DBFTFs) in 11 cities across the country to enhance interagency communications and improve each agency's effectiveness in fraud investigations. The DBFTFs consist of federal, state, and local agencies, and are co-located at ICE facilities. The DBFTFs combine the resources, authorities, and expertise of each of their partners to disrupt and dismantle organizations that commit various types of fraud and to deter the perpetration of fraud. The DBFTFs aggressively pursue many types of fraud that, by their nature, encompass identity theft. Additionally, ICE is aggressively focusing its anti-identity theft efforts in the area of worksite enforcement, and ICE is working with other departments and agencies to establish a comprehensive approach for employers to identify and employ authorized workers and reduce the use of counterfeit identification.

Other agencies do not lead, but actively participate in identity theft task forces. Examples include:

- **SSA OIG.** SSA OIG's Office of Investigations special agents participate in more than 100 various task forces, many devoted specifically to identity theft.
- **IRS Criminal Investigation Division (IRS CI).** Approximately one-quarter of IRS CI's 30 field offices have representatives on identity theft task forces. Some field offices have representatives in multiple judicial districts.
- **State Department Diplomatic Security.** The State Department's Bureau of Diplomatic Security is establishing an identity fraud task force with the Puerto Rican Police Department. The Bureau's 31 field and resident offices participate in multi-agency identity theft task forces in their regions.

The following are some examples of interagency working groups and task forces:

- In two areas of the country where the use of compromised identities are common, the HHS OIG has teamed with the FBI, the DOJ, the Medicaid Fraud Control Unit, the SSA OIG, and representatives of the CMS to target the perpetrators. This is an effective program to identify those who commit fraud against the government.
- The Regional Identity Theft Working Group (the RIT Group) in the Eastern District of Pennsylvania has the following purposes: (1) information sharing and deconfliction of investigations; (2) identification of new identity theft schemes and key identity theft targets; and (3) hosting of discussions about identity theft prevention. In order to increase federal prosecutions for identity theft, monetary thresholds are reduced for cases involving organizations, and for individuals who serve in certain leadership roles. In order to increase sanctions for such cases, Assistant United States Attorneys regularly seek upward departures in criminal defendants' sentences when the defendants disrupted victims' lives. The RIT Group is also developing an online database to foster better communication between law enforcement agencies about identity theft investigations.
- The Identity Theft Crimes Working Group in the District of New Hampshire is highly inclusive of both federal and state agencies, including a number of regulatory agencies for banking, insurance, and securities. It also monitors and uses information from the FTC Consumer Sentinel website to identify identity theft complaints over which it may have jurisdiction for the purpose of generating new cases.
- The Los Angeles Identity Theft and Economic Crimes Task Force, led by the USPIS, includes the USSS, the FBI, the Los Angeles Police Department, and the Los Angeles County Probation Department. This task force also has a working relationship with other federal law enforcement components, including ICE, IRS-CI, and the SSA OIG.

Numerous success stories reflect the impact of these task force efforts. For example, beginning in February 2005, the USPIS-led Identity Theft Economic Crimes Task Force (ITEC) in Los Angeles received information from Sears/Citibank regarding the fraudulent account takeovers of more than 300 linked Sears credit cards totaling more than $1 million in fraud losses. All of the account addresses were fraudulently changed through Sears/Citibank to various Commercial Mail Receiving Agencies (CMRAs) located throughout Southern California. Subsequent investigation by ITEC revealed that two Nigerian nationals obtained the credit cards from the various CMRAs. These individuals then used the credit cards and corresponding fraudulent identification to conduct fraudulent balance transfers and cash advances. They also used data search engines such as ChoicePoint and Merlin to obtain the necessary information on the victims to facilitate the account takeovers.

On July 19, 2005, members of ITEC executed federal search warrants at the suspects' residences, vehicles, and storage units. Fraudulent California identification cards and Nigerian passports bearing the individuals' photographs but issued in various names were recovered during the search of the residences. The names on the identification cards corresponded with the account holder information on more than 30 recovered credit cards. Also recovered during the search were a number of printouts bearing corresponding victim information issued from Merlin and Intelius. Recovered from the storage unit were several hundred credit cards and more than 3,000 ChoicePoint search printouts, many of which bore handwritten notations indicating credit cards issued in those identities that were shipped to CMRAs under their control. The suspects were taken into custody pursuant to federal arrest warrants for violations of conspiracy to commit access device fraud. Both defendants pleaded guilty in United States District Court to conspiracy and access device fraud, and one defendant pleaded guilty to an additional count of computer intrusion.

PART N

FEDERAL CRIMINAL STATUTES USED TO PROSECUTE IDENTITY THEFT

Federal law enforcement officers rely on a wide range of federal criminal statutes to investigate and prosecute identity theft. The two federal statutes that most directly prohibit identity theft are the identity theft (18 U.S.C. § 1028(a)(7)) and aggravated identity theft (18 U.S.C. § 1028A(a)) statutes. The identity theft statute generally prohibits knowingly transferring, possessing, or using a means of identification of another person in connection with any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.[50] Similarly, the aggravated identity theft statute (18 U.S.C. § 1028A(a)(1)) prohibits knowingly transferring, possessing, or using a means of identification of another person, during and in relation to any of numerous specified federal felonies listed in that section. Federal prosecutors have been making substantial use of the identity theft and aggravated identity theft statutes in pursuing identity theft cases.

In addition to using the identity theft and aggravated identity statutes, DOJ often charges other offenses that may be committed in the course of identity theft and fraud. Some of the most frequently used statutes in this regard are mail fraud (18 U.S.C. § 1341); wire fraud (18 U.S.C. § 1343); financial institution fraud (18 U.S.C. § 1344); access device fraud (18 U.S.C. § 1029); and SSN fraud (42 U.S.C. § 408(a)(7)(B)). In cases involving false documents, such as visas, passports, or other documents relating to identification, federal prosecutors also can charge a variety of identification document offenses. These include identification document fraud (18 U.S.C. § 1028(a)(1)-(6)); false statement in application and use of passport (18 U.S.C. § 1542); forgery or false use of passport (18 U.S.C. § 1543); misuse of passport (18 U.S.C. § 1544); and fraud and misuse of visas, permits, and other documents (18 U.S.C. § 1546). In some cases involving "pretexting" (i.e., fraudulent misrepresentations to obtain customer data) directed at or affecting financial institutions, the GLB Act[51] may apply.

Three other federal statutes may also apply to computer-related identity theft. First, the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(4), generally prohibits the unauthorized accessing of a computer with intent to defraud and thus furthering the fraud and obtaining anything of value. This statute has been used effectively to charge defendants engaging in identity theft by unlawful accessing of computers where the evidence shows that the data was taken as part of a fraud scheme. Second, 18 U.S.C. § 1030(a)(2) generally prohibits the theft of information from a computer, but limits a federal court's jurisdiction to instances in which the thief uses an interstate communication to access that computer (unless the computer belongs to the federal government or a financial institution). Third, 18 U.S.C. § 1030(a)(5) prohibits actions that cause "damage" to computers—that is, actions that impair the "integrity or availability" of data or computer systems.[52] Absent

special circumstances, however, the loss caused by the conduct must exceed $5,000 in order for it to constitute a federal crime.

Another federal criminal offense 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 subsection prohibits the transmission of a threat "to cause damage to a protected computer."[53] Subsection 1030(a)(7) is used, for example, to prosecute criminals who threaten to delete data, crash computers, or knock computers off of the Internet using a denial of service attack. This provision provides the electronic counterpart to traditional extortion statutes that generally require a threat to cause bodily harm or the destruction of physical property.

In addition, prosecutors often utilize statutes related to the programs and operations of the SSA, which are located in title 42 of the United States Code, to prosecute identity theft-related crimes. One of these statutes, 42 U.S.C. § 408, specifically addresses fraud relating to a SSN and Social Security card. It provides criminal penalties for an individual who fraudulently obtains, uses, or represents a SSN to be theirs. This statute also provides for criminal penalties for an individual who fraudulently buys, sells, or possesses a Social Security card with intent to sell or alter. It is also a violation of this statute to disclose, use, or compel the disclosure of the SSN of any person in violation of the laws of the United States.

Finally, HIPAA can be used to prosecute identity theft-related offenses. HIPAA provides for criminal sanctions against a health plan, health care clearing house, or health care provider subject to its provisions that wrongfully uses or causes to be used a unique health identifier, or that wrongfully obtains individually identifiable health information relating to an individual, or which wrongfully discloses such individually identifiable information to another party. 42 U.S.C. § 1320d-6(a). Violators may be fined not more than $50,000 and imprisoned not more than one year; or, if the offense is committed under false pretenses, be fined up to $100,000 and/or imprisoned not more than five years; or, if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000 and be imprisoned up to ten years.

PART O

TRAINING FOR AND BY INVESTIGATORS AND PROSECUTORS

At the National Advocacy Center (NAC) in Columbia, South Carolina, the DOJ offers training on identity fraud as part of other courses, including cybercrime and white-collar crime courses. The National District Attorneys Association (NDAA) also has a training program at the NAC, where it conducts courses on identity theft and cybercrime.

A number of other law enforcement entities also provide training, not only to their own investigators, but also to the private sector:

United States Attorney's Offices

- The U.S. Attorney's Office for the Eastern District of Pennsylvania organized a conference for hospitals, utilities, universities, banks, and corporations on data security. In addition to technical data management and employee screening sessions, the conference addressed the pitfalls of poor information security, such as civil liability.
- The U.S. Attorney's Office for the Southern District of West Virginia has implemented the Identity Theft/Document Fraud Initiative to train prosecutors, law enforcement officers, Department of Motor Vehicle employees, other state and federal agencies, and the banking industry about the prevention and detection of document fraud. The Initiative involves an extensive training plan for each member agency, and includes the IRS-CI, SSA's OIG, USSS, FBI-Joint Terrorism Task Force, ICE, West Virginia State Police, West Virginia Department of Motor Vehicles, Bureau of Prisons, West Virginia Bankers Association, and the Southern District of West Virginia's Anti-Terrorism Advisory Council.
- The U.S. Attorney's Office for the District of Oregon sponsors an annual financial crimes conference that serves law enforcement, financial fraud investigators for financial institutions, and internal auditors for public agencies. It provides investigators and prosecutors who handle financial crimes, and private-sector personnel who assist them, tools to assist in the prevention, detection, investigation, and prosecution of fraud and identity theft. It regularly includes sections on asset tracing, investigative techniques involving digital technology, basic data recovery, search and seizure laws, pertinent financial privacy and regulatory provisions, and trends associated with economic fraud.

FBI

- The FBI has provided in-service training on identity theft to its agents, and also includes identity theft information in other training sessions for FBI personnel. With respect to identity theft and health care, the FBI and the CMS are presenting Part D law enforcement training in several cities, which focuses on identity theft and scams that facilitate prescription drug fraud.

United States Secret Service

- The Secret Service provides a substantial amount of training to local and state law enforcement counterparts, as well as providing support in a variety of ways—such as forensic analysis and expert testimony in support of local cases. In connection with an interagency working group on identity theft, the Secret Service, the Postal Inspection Service, and the FTC, in conjunction with the International Association of Chiefs of Police, developed a roll-call video on identity theft for police departments to show to their officers. This video was provided to police departments throughout the country. In addition, the Secret Service's Electronic Crimes Section has trained over 150 state and local officers from across the United States to conduct computer investigations as well as computer forensic analysis. The Secret Service has also partnered with the National District Attorneys Association's National Center for the Prosecution of Identity Crime to provide training for local prosecutors focused primarily on identity crimes.

- The Secret Service provides six training seminars annually for U.S. Attorneys from across the United States. These seminars are hosted and coordinated by Secret Service personnel, and have included a block of instruction from the Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) in some of the seminars. The topics covered in this training included: Counterfeit Currency, Eurasian Hacking, Identity Theft, Electronic Crimes Task Forces and Private Sector Partnerships, Cyber Law, and Cyber Prosecutions. The seminars are intended to provide an education on the Secret Service's core violations and current trends observed in its daily investigations and investigations involving the Internet.

National White Collar Crime Center

- The National White Collar Crime Center (NW3C), a nonprofit organization that provides training programs and other assistance to state and local law enforcement in partnership with the Bureau of Justice Assistance, has completed the development of a three-day identity theft course. The curriculum includes topics such as investigative tools, techniques, and resources for investigating identity theft crimes; "criminal tools of the trade"; the basics of identity theft for financial gain or concealment (e.g., for terrorism or avoidance of prosecution); and proactive and reactive approaches to identity theft that provide students with practical investigative experience. NW3C has also included modules on identity theft in other courses it conducts, which include methods of following the financial trail of these types of crimes.

American Prosecutors Research Institute

- A nonprofit affiliate of the NDAA, the American Prosecutors Research Institute, has an established White Collar Crime Unit. With start-up funding from the BJA, the unit provides training to local prosecutors and law enforcement on a variety of issues including cybercrime, telemarketing fraud, and financial exploitation of the elderly. Trainings occur at specific sites across the country and as part of NDAA's training program at the NAC.

  NDAA recently established the National Center for the Prosecution of Identity Crimes to train local prosecutors, law enforcement, and members of the financial industry in the investigation and prosecution of identity crimes. The Center has conducted a Financial Identity Fraud training in Las Vegas and presented an Identity Theft Fall Conference at the NAC. The Center contemplates conducting several more conferences and providing clearinghouse services in the future.

Regional Information Sharing Systems (RISS)

- Through the RISS program, in partnership with BJA, several additional classes including identity theft have been taught for state and local law enforcement. For example, the Mid-States Organized Crime Information Center co-sponsored a Financial Records Examination and Analysis course (presented by NW3C) that included identity theft as one of the topics.

National Consortium for Justice Information and Statistics (SEARCH)

- Through a partnership with BJA, SEARCH trains state and local law enforcement on "Core Skills for the Investigation of Computer Crime," which covers the basics of investigating the misuse of identities online.

Other Multi-Agency Training

- Since 2002, several federal law enforcement agencies—the DOJ, the USPIS, the USSS, the FTC, and the FBI—and the American Association of Motor Vehicle Administrators (AAMVA) have jointly sponsored a series of more than 20 regional training seminars on identity fraud for state and local law enforcement agencies in numerous states across the United States. These one-day seminars, which are provided free of charge to state and local law enforcement, provide basic information tools and guidance with investigators' and prosecutors' perspectives on pursuing identity theft cases.

PART P

CURRENT REMEDIATION TOOLS AVAILABLE TO VICTIMS

Federal and state laws offer victims of identity theft an array of tools to avoid or mitigate the damage they incur. Numerous resources and websites advise consumers of the steps to take if they have become victims of identity theft, or if their personal information has been breached. Consumers should take specific actions as soon as they suspect that they have been or are about to become a victim of identity theft. The following options are available to identity theft victims:

▶ Place Fraud Alerts

Once a consumer suspects that he or she has been or may become a victim of identity theft, for instance, if their wallet was stolen or they are notified that their personal information was compromised by a data breach, they may place, at no cost, an "initial fraud alert" on their credit report by making a request to any one of the three national CRAs—Experian, Equifax, or TransUnion.[54] Fraud alerts can help prevent an identity thief from opening any accounts in the consumer's name. The presence of a fraud alert requires creditors to confirm the consumer's identity before opening new accounts or making changes to existing accounts.[55] An initial fraud alert remains in place for 90 days, but may be renewed.[56] If an identity theft occurs, the victim may place an extended seven-year alert.[57]

▶ File a Police Report

Victims of identity theft should file a report with law enforcement officials as soon as they learn of the crime. This is a necessary step in obtaining an extended fraud alert or blocking fraudulent trade lines on a credit report, and can help with creditors who may want proof of a crime. Because many police departments, as a matter of policy and/or practice, do not routinely take identity theft reports, consumers often must be persistent in their requests for police reports. Victims can print a copy of the online form and provide it to their local police department. The police can use the completed form as the foundation of a police report.

▶ Report the Theft to the FTC's Identity Theft Data Clearinghouse

Consumers who experience identity theft should report the event to the FTC either through the online complaint form (***www.ftc.gov/idtheft***) or the toll free hotline (877 ID THEFT). The FTC maintains the federal clearinghouse for complaints by victims of identity theft. Identity theft reports are available through the FTC's Consumer Sentinel Network to law enforcement officials across the country for use in their investigations.

As noted above, victims of identity theft should file a report with law enforcement officials as soon as they learn of the crime.

Obtain Document Related to Fraudulent Transactions

Under section 609(e) of the FCRA,[58] victims, or law enforcement officers acting on their behalf, can obtain records and application information from financial institutions that have handled transactions that identity thieves conducted in the victims' names. (Some law enforcement officials, however, report that their agents have had difficulty in doing so because certain financial institution personnel are not familiar with the relevant provisions of the FCRA.)

Close Fraudulently Opened or Compromised Accounts

Consumers should close any accounts, such as bank accounts and/or credit cards that were established fraudulently or appear to have been compromised. A consumer may be required to provide evidence, including a police report and other supporting documents, before a creditor closes the account or forgives the fraudulent debt.

Order a Credit Report

All consumers are entitled to receive a free copy of their consumer report from each of the three national CRAs (Experian, Equifax, and TransUnion), as well as from various other nationwide specialty CRAs, every twelve months.[59] Additionally, placing a fraud alert entitles consumers to immediately request free copies of their credit reports regardless of the timing of their previous requests.[60] Consumers who have had an extended fraud alert placed on their credit reports are entitled to request two free copies of their credit report from each of the CRAs in the twelve months following the date the extended alert was placed.[61]

Blocking Fraudulent Information on Credit Reports

When a credit report contains fraudulent information as a result of identity theft, the consumer can ask that the information be blocked from the credit report. CRAs block fraudulent information from a credit report when the consumer provides certain information including a copy of a police report and a statement that the information does not relate to any transaction made or authorized by the consumer.[62]

Seek Assistance from Information Furnishers

An "information furnisher" is any entity that provides information to the CRAs. For example, a department store that opens a store account for a consumer would furnish information about that credit account to

the three CRAs. When a CRA notifies an information furnisher that it has blocked fraudulent information about a credit transaction by that furnisher, the information furnisher may not continue to report that information to the CRAs, and may not hire someone to collect the debt that relates to the fraudulent account, or sell the debt to someone else who would try to collect it.[63]

Receive an Accounting of Disclosures Made By Health Care Providers and Health Plans

All consumers can protect themselves against a form of identity theft, medical identity theft, by requesting from their health care providers or health plans accountings of any disclosure made of their protected health information during the preceding six years, other than those that relate, among other exceptions, to treatment, payment, and health care operations. 45 C.F.R. § 164.528. The HIPAA Privacy Rule requires health plans, health care clearinghouses, and covered health care providers to provide one free accounting per year upon the request of the consumer.

Seek Assistance from IRS

In some cases of identity theft, the suspect either obtains a refund or incurs tax liability in the victim's name. In such cases, the victim may need to obtain assistance from the IRS. The IRS is updating procedures to provide notices and assistance to taxpayers whose name and SSN were used by an identity thief for employment purposes. The Identity Theft Program Office can provide further information regarding this comprehensive effort.

Dispute Fraudulent Debts with Debt Collectors

Consumers also have rights if they are contacted by debt collectors about debts incurred in their name by identity thieves. The consumer can stop contacts by a debt collector by sending a letter within 30 days of being contacted, informing the collector that the debt is not theirs. The debt collector may not contact the consumer again until it sends proof of the debt to the consumer. After a debt collector is notified that a debt is the result of identity theft, it is required to inform the creditor for whom it is collecting that the consumer disputes the debt.

Pursue State Remedies

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.

Contact Identity Theft Victim File Programs

Identity thieves have sometimes committed crimes using another's name. Victims who experience this form of identity theft often must establish that they are not the person who, in their name, committed the crime. Several states and the FTC have programs that address this serious situation. For example, California maintains a registry of individuals whose identities have been used in the commission of a crime. The registry is used to help consumers establish that they were not responsible for crimes committed in their name.[64] Similarly, Ohio's PASSPORT system for identity theft victims issues a card to identity theft victims that can be used to verify their identities to law enforcement officers and creditors. Several other states, too, have begun to use "passport" programs like these. The FBI has a similar program, which is managed through the Criminal Justice Information Service.

Consider Private Sector Assistance

The private sector and not-for-profit entities also provide tools for victims to repair the damage caused by identity theft. For example, both the ITRC and the Privacy Rights Clearinghouse (PRC) provide direct consumer assistance under certain circumstances. Other organizations offer recovery programs for a fee that promise to repair the damage caused by the identity thief.[65] CRAs and other companies offer credit monitoring services that claim to provide early warning of identity theft.[66]

In addition, a consortium of dozens of large financial institutions created the not-for-profit ITAC in 2004, to provide free, one-on-one assistance to consumers who experience identity theft through one of the member entities. Identity theft victims who contact an ITAC member company first try to resolve their dispute with that company, and then can choose to refer their identity theft case to the ITAC.

Consider Whether to Seek a New Social Security Number

In limited circumstances, the SSA may assign a new SSN to a victim who provides evidence of SSN misuse and, despite efforts to resolve the problem, continues to be disadvantaged by the misuse. A major drawback to getting a new SSN is that an individual may have a difficult time re-establishing an identity under the new SSN, including a credit, educational, and medical history. (SSA will cross-refer the old and new SSNs in SSA records to ensure proper crediting of earnings.)

ENDNOTES

1. Gramm-Leach-Bliley Act § 501(b), 15 U.S.C. § 6801; Fair Credit Reporting Act § 628, 15 U.S.C. § 1681w.

2. The FACT Act also includes restrictions on the circumstances under which consumer reporting agencies may furnish consumer reports that contain medical information about consumers. In particular, a consumer reporting agency may not furnish a consumer report that contains medical information about a consumer except under certain delineated circumstances involving consumer consent to the furnishing of the report, or if the information is limited to account status and is reported in a manner that does not reveal the nature of the medical treatment.

3. *See also* Identity Theft and Pretext Calling, Board SR Letter 01-11 (Supp) (Apr. 26, 2001), OCC AL 2001-4 (April 30, 2001), OTS CEO Memorandum #139 (May 4, 2001), FDIC FIL-39-2001; Threats from Fraudulent Bank Web Sites: Risk Mitigation and Response Guidance for Web Site Spoofing Incidents, OCC Bulletin 2005-24 (July 1, 2005); Phishing and E-mail Scams, OTS CEO Memorandum #193 (Mar. 8, 2004); Phishing, OTS CEO Memorandum #205 (Sep. 8, 2004); Phishing, FDIC FIL-103-2004; Bank Use of Foreign-Based Third-Party Service Providers, OCC Bulletin 2002-16 (May 15, 2002); Third Party Arrangements, OTS Thrift Bulletin 82a (September 2, 2004); Infrastructure Threats—Intrusion Risks, OCC Bulletin 2000-14 (May 15, 2000); Voice Over Internet Protocol- FDIC FIL-69-2005; Spyware- FDIC FIL-66-2005; FDIC Identity Theft Study Supplement- FDIC FIL-59-2005; FDIC Identity Theft Study- FDIC FIL-132-2004; Software Due Diligence- FDIC FIL-121-2004; Instant Messaging- FDIC FIL-84-2004; Virus Protection- FDIC FIL-62-2004; Internet Fraud- FDIC FIL-27-2004; Patch Management- FDIC FIL-43-2003; Wireless- FDIC FIL-8-2002. The financial institution regulators also issue alerts from time to time, such as Customer Identity Theft: E-Mail Related Fraud Threats, OCC Alert 2003-11 (September 12, 2003), and Network Security Vulnerabilities, OCC Alert 2001-4 (April 24, 2001).

4. *See*, *e.g.*, The Financial Services Roundtable, *Voluntary Guidelines for Consumer Confidence in Online Financial Services*, ***www.bitsinfo.org/downloads/Publications%20Page/bitsconscon.pdf***; *BITS Voluntary Guidelines for Aggregation Services*, ***www.bitsinfo.org/downloads/Publications%20Page/bitsaggguide2004.pdf***.

5. *See* "BITS," the Technology Group of the Financial Services Roundtable, ***www.bitsinfo.org/downloads/Publications%20Page/bitsidtheftwhitepaper.pdf***, Financial Identity Theft: Prevention and Consumer Assistance, June 2003.

6. *See* ***http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html***.

7. *See* the data security guidelines of Truste.org, at ***www.truste.org/pdf/SecurityGuidelines.pdf***.

8. *See id*.

9. *See id*.

10. *See id*.

11. *See* Peter Mell et al., *Guide to Malware Incident Prevention and Handling: Recommendations of the National Institute of Standards and Technology at ES-1* (Nov. 2005), ***http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf***.

12. *Id*.

13. *Id*.

14. *Id*.

15. *See, e.g.,* Visa USA Cardholder Information Security Program, What To Do If Compromised (Nov. 14, 2005), ***http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf***, American Express, *Data Compromise Workbook* (2006).

16. American Express, *Data Compromise Workbook* (2006), at 6-8.

17. Visa USA Cardholder Information Security Program, *What To Do If Compromised* (Nov. 14, 2005), at 3.

18. *Id*.

19. American Express, *Data Compromise Workbook* (2006), at 10.

20. For instance, Educause, a nonprofit that emphasizes technology and information security for institutions of higher education, has created a Data Incident Notification Toolkit, which provides users with information about legal obligations, policies and procedures, thresholds for notification, and notification templates. *See* Educause, *Data Incident Notification Toolkit*, available at ***http://www.educause.edu/DataIncidentNotificationToolkit/9320***.

21. The IT Compliance Institute (ITCI) has provided some key recommendations for companies to consider in the event of a security incident. *See* ***http://www.itcinstitute.com/display.aspx?id=1731***. First, ITCI recommends that companies develop a good communications strategy and ensure that only pre-approved public relations personnel speak about any incident. Also, regardless of state laws, it advises that companies should provide nationwide notice to consumers of a potential data breach using multiple consumer notification techniques, such as a combination of telephone and letter. Any notification provided by a business should quickly, clearly, and thoroughly communicate to its customers what happened, the potential harm for the customer, what the company is doing to help, and how it plans to prevent future breaches. Finally, ITCI recommends providing essential information and steps that customers should take to protect themselves. IT Compliance Institute, *Data Breach Damage Control* (May 16, 2006), available at ***www.itcinstitute.com/display.aspx?id=1731***.

22. Some companies have provided technical advice, such as the use of specific backup and encryption technologies, in the event of lost or stolen media, as well as specific types of data collection and analysis software that companies should use for forensic investigations. Others assist members and others in developing and implementing information security as well as breach response programs.

23. Available at ***www.ncpc.org/cms/cms-upload/prevent/files/idtheftrev.pdf***.

24. *See* ***http://www.ojp.gov/ovc/help/it.htm***.

25. Available at ***http://studentaid.ed.gov/PORTALSWebApp/students/english/idtheft.jsp***.

26. *See* ***http://www.staysafeonline.org/basics/consumers.html***.

27. *See* ***http://www.texasbankers.com/pdfs/StopIDtheft.pdf***.

28. *See* "Identity Theft: How To Avoid Theft And What To Do If It Happens To You," available at ***www.sia.com/publications/pdf/Identity_Theft.pdf***.

29. Available at ***www.nasd.com/InvestorInformation/InvestorAlerts/FraudsandScams/PhishingandOtherOnlineIdentityTheftScamsDontTaketheBait/index.htm***.

30. "Medical Identity Theft: The Information Crime That Can Kill You," Dixon, Pam. World Privacy Forum, Spring 2006, ***www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf***, at 6.

31. "Colleges are textbook cases of cybersecurity breaches", USA TODAY, August 1, 2006, available at ***www.usatoday.com/tech/news/computersecurity/hacking/2006-08-01-college-hack_x.htm?POE=TECISVA***.

32. *See* ***http://identityweb.umich.edu/***.

33. Pub. L. 108-458.

34. Pub. L. 109-13.

35. *See* Bureau of Justice Statistics Bulletin, Prosecutors in State Courts, 2005 (July 2006), available at ***http://www.ojp.usdoj.gov/bjs/pub/pdf/psc05.pdf***.

36. Pub.L. 108-275, July 15, 2004, 188 Stat. 831.

37. No cases with a conviction under 18 U.S.C. § 1028A were received by the Commission in Fiscal Year 2004. Cases with incomplete information on statutory subsection and/or applicable statutory minimum were excluded.

38. Average sentences include prison and alternative confinement as defined in USSG § 5C1.1. Cases with sentences of 470 months (or more, including life) or probation were included in the average sentence calculations as 470 months and zero months, respectively.

39. *See Guidelines Manual* USSG § 3B1.3 App. Note 2(B) for full text including examples.

40. Average sentences include prison and alternative confinement as defined in USSG § 5C1.1. Cases with sentences of 470 months (or more, including life) or probation were included in the average sentence calculations as 470 months and zero months, respectively.

41. *See* ***kansascity.fbi.gov/dojpressrel/pressrel06/identitytheft051006.htm***.

42. *See* U.S. Department of Justice, Press Release (July 11, 2006), available at ***www.usdoj.gov/opa/pr/2006/July/06_crm_424.html***.

43. *See* United States Attorney's Office, Central District of California, Press Release (December 15, 2005), available at ***http://www.usdoj.gov/usao/cac/pr2005/170.html***.

44. SSN misuse includes both identity theft and identity fraud not involving another real person's identity, e.g., when an individual fraudulently obtains a second SSN.

45. *See* Department of Justice, Press Release (November 20, 2003), available at ***http://www.fbi.gov/dojpressrel/pressrel03/cyber112003.htm***.

46. *See* Prepared Statement of Anne Wallace, Executive Director, Identity Theft Assistance Corporation, Before the Subcommittee on Crime, Terrorism and Homeland Security of the House of Representatives Committee on the Judiciary, June 11, 2006, available at ***http://www.identitytheftassistance.org/resources/Wallace.ITAC.pdf***.

47. *See* Reuters, *IDs of 50,000 Bahamas resort guests stolen*, New Zealand Herald, January 9, 2006, available at ***http://www.nzherald.co.nz/location/story.cfm?l_id=520&ObjectID=10362953***.

48. *See* Liberty Alliance, ***http://www.projectliberty.org/***.

49. *See* U.S. Secret Service, Press Release (May 23, 2006), available at ***http://www.secretservice.gov/press/gpa0613.pdf***.

50. 18 U.S.C. § 1028(d)(7).

51. 15 U.S.C. §§ 6821 and 6823.

52. *See* 18 U.S.C. § 1030(e)(8).

53. 18 U.S.C. § 1030(a)(7).

54. Fair Credit Reporting Act § 605A, 15 U.S.C. § 1681c-1.

55. FCRA § 605A(h)(1)(B), 15 U.S.C. § 1681c-1(h)(1)(B).

56. FCRA § 605A(a)(1)(A), 15 U.S.C. § 1681c-1(a)(1)(A).

57. FCRA § 605A(h)(1)(B), 15 U.S.C. § 1681c-1(h)(2)(B).

58. FCRA § 609(e), 15 U.S.C. § 1681g(e).

59. FCRA § 612(a), 15 U.S.C. § 1681j(1).

60. FCRA § 605A(a)(2), 15 U.S.C. § 1681c-1(a)(2).

61. FCRA § 605A(b)(2)(A), 15 U.S.C. § 1681c-1(b)(2)(A).

62. FCRA § 605B(a); 15 U.S.C. § 1681c-1(a).

63. FCRA § 623(a)(6)(A), 15 U.S.C. § 1681s-2(a)(6)(A).

64. *See* ***http://ag.ca.gov/idtheft/general.htm***.

65. *See*, *e.g.*, ***http://inova.org./inovapublic.srt/eap/idtheft.jsp?tStatus=5 www.identitytheft911.com/home.htm***.

66. *See* ***http://www.fightidentitytheft.com/credit-monitoring.html***.