The President's Identity Theft Task Force

COMBATING IDENTITY THEFT

VOLUME II: SUPPLEMENTAL INFORMATION

Exhibit K

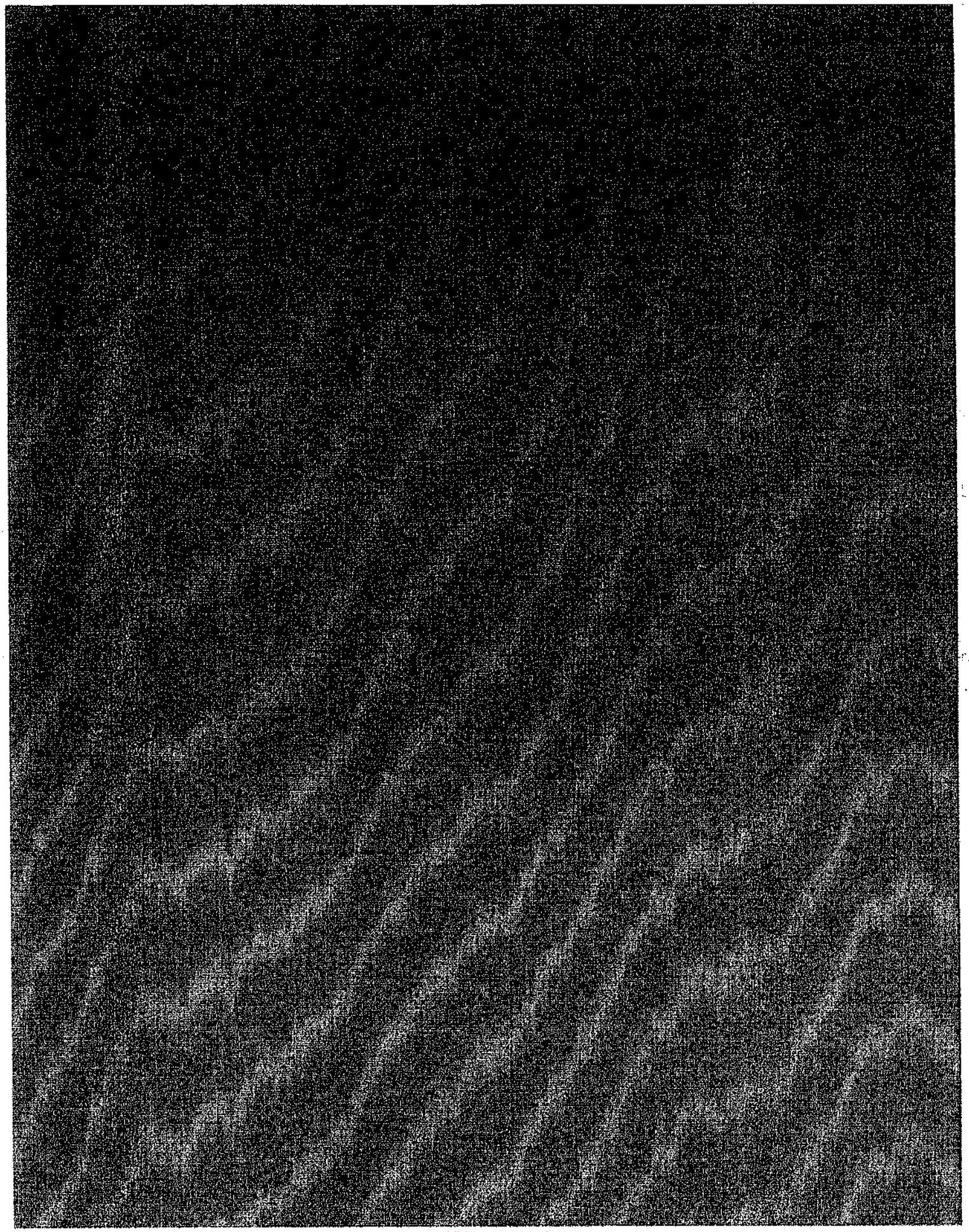

Exhibit K - Part 1 of 2

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/fighttheft/index.html***; the *Interagency Informational Brochure on Internet Phishing Scams*, available at ***www.fdic.gov/consumers/consumer/fighttheft/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/