

**PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON
IDENTITY THEFT**

**Before the
HOUSE FINANCIAL SERVICES COMMITTEE**

Washington, D.C.

April 3, 2003

I. INTRODUCTION

Mr. Chairman, and members of the Committee, I am Howard Beales, Director of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").¹ I appreciate the opportunity to present the Commission's views on the impact of identity theft on consumers and the importance of information security in preventing identity theft.

The Federal Trade Commission has a broad mandate to protect consumers, and controlling identity theft is an important issue of concern to all consumers. The FTC's primary role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act").² The Act directed the Federal Trade Commission to establish the federal government's central repository for identity theft complaints and to provide victim assistance and consumer education. The Commission also works extensively with private industry on ways to improve victim assistance, including providing direct advice and assistance in cases when information has been compromised. The Commission can take enforcement action when companies fail to take adequate security precautions to protect consumers' personal information.

¹The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any Commissioner.

²Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

II. THE FEDERAL TRADE COMMISSION'S ROLE IN COMBATING IDENTITY THEFT

The Identity Theft Act strengthened the criminal laws governing identity theft³ and focused on consumers as victims.⁴ Congress also recognized that coordinated efforts are essential to best serve the needs of identity theft victims because these fraud victims often need assistance both from government agencies at the national and state or local level and from private businesses. Accordingly, the FTC's role under the Act is primarily one of facilitating information sharing among public and private entities.⁵ Specifically, Congress directed the Commission to establish procedures to: (1) log the receipt of complaints by victims of identity theft; (2) provide identity theft victims with informational materials; and

³18 U.S.C. § 1028(a)(7). The statute broadened "means of identification" to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.*, credit cards), electronic identification number or routing code, and telecommunication identifying information.

⁴Because individual consumers' financial liability is often limited, prior to the passage of the Act, financial institutions, rather than individuals, tended to be viewed as the primary victims of identity theft. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals: to recognize the individual victims of identity theft. *See* S. Rep. No. 105-274, at 4 (1998).

⁵Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. *See, e.g.*, *FTC v. Assail, Inc.*, W03 CA 007 (W.D.Tex Feb. 4, 2003) (order granting preliminary injunction) (defendants alleged to have debited consumers' bank accounts without authorization for "upsells" related to bogus credit card package) and *FTC v. Corporate Marketing Solutions, Inc.*, CIV - 02 1256 PHX RCB (D. Ariz Feb.3, 2003) (final order) (defendants "pretexted" personal information from consumers and engaged in unauthorized billing of consumers' credit cards). In addition, the FTC brought six complaints against marketers for purporting to sell international driver's permits that could be used to facilitate identity theft. Press Release, Federal Trade Commission, *FTC Targets Sellers Who Deceptively Marketed International Driver's Permits over the Internet and via Spam* (January 16, 2003) (*at* <http://www.ftc.gov/opa/2003/01/idpfinal.htm>).

(3) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.⁶ To fulfill the purposes of the Act, the Commission has implemented a plan that centers on three principal components: (1) A toll-free telephone hotline, (2) the Identity Theft Data Clearinghouse (the “Clearinghouse”), a centralized database used to aid law enforcement, and (3) outreach and education to consumers, law enforcement, and private industry.

A. Toll-free Telephone Hotline

On November 1, 1999, the Commission established a toll-free telephone number, 1-877-ID THEFT (438-4338), for consumers to report identity theft and to receive information about identity theft.

In 2002, hotline counselors added almost 219,000 consumer reports to the Clearinghouse, up from more than 117,000 in 2001. Of the 219,000 reports, almost 162,000 (74%) were complaints from actual victims of identity theft, and almost 57,000 (26%) were inquiries about identity theft generally.

Despite this dramatic growth in reports, the FTC is cautious in attributing it entirely to a commensurate growth in the prevalence of identity theft. The FTC believes that the increase is, at least in part, an indication of successful outreach in informing the public of its program and the availability of assistance.

Callers to the hotline receive telephone counseling from specially trained personnel to provide them with general information about identity theft or to help them through the steps they need to take to resolve the problems resulting from the misuse of their identities. Victims are advised to: (1) Contact each of the three national consumer reporting agencies to obtain copies of their credit reports and

⁶Pub. L. No. 105-318, § 5, 112 Stat. 3010 (1998).

request that a fraud alert be placed on their credit reports;⁷ (2) contact each of the creditors or service providers where the identity thief has established or accessed an account, to request that the account be closed and to dispute any associated debts; and (3) report the identity theft to the police and get a police report, which is very helpful in demonstrating to would-be creditors and debt collectors that the consumers are genuine victims of identity theft.

Counselors also are trained to advise victims having particular problems about their rights under relevant consumer credit laws including the Fair Credit Reporting Act,⁸ the Fair Credit Billing Act,⁹ the Truth in Lending Act,¹⁰ and the Fair Debt Collection Practices Act.¹¹ If the investigation and resolution of the identity theft falls under the jurisdiction of another regulatory agency that has a program in place to assist consumers, callers also are referred to those agencies.

⁷ These fraud alerts indicate that the consumer is to be contacted before new credit is issued in that consumer's name. See Section II.C.(3) *infra* for a discussion of the credit reporting agencies new "joint fraud alert" initiative.

⁸ 15 U.S.C. § 1681 *et seq.*

⁹ *Id.* § 1666. The Fair Credit Billing Act generally applies to "open end" credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts, such as loans or extensions of credit that are repaid on a fixed schedule.

¹⁰ *Id.* § 1601 *et seq.*

¹¹ *Id.* § 1692 *et seq.*

B. Identity Theft Data Clearinghouse

The Identity Theft Act directed the FTC to log the complaints from victims of identity theft and refer those complaints to appropriate entities such as law enforcement agencies. Before launching this complaint system, the Commission took a number of steps to ensure that it would meet the needs of criminal law enforcement, including meeting with a host of law enforcement and regulatory agencies to obtain feedback on what the database should contain. Access to the Clearinghouse via the FTC's secure Web site became available in July of 2000. To ensure that the database operates as a national clearinghouse for complaints, the FTC has solicited complaints from other sources. For example, in February 2001, the Social Security Administration Office of Inspector General (SSA-OIG) began providing the FTC with complaints from its fraud hotline, significantly enriching the FTC's database.

The Clearinghouse provides a much fuller picture of the nature, prevalence, and trends of identity theft than was previously available.¹² FTC data analysts aggregate the data to develop statistics about the nature and frequency of identity theft. For instance, the Commission publishes charts showing the prevalence of identity theft by states and by cities. Law enforcement and policy makers at all levels of government use these reports to better understand the challenges identity theft presents.

Since the inception of the Clearinghouse, 75 federal agencies and 549 state and local agencies have signed up for access to the database. Within those agencies, over 4500 individual investigators have the ability to access the system from their desktop computers twenty-four hours a day, seven days a week. The Commission actively encourages even greater participation.

¹² Charts that summarize 2002 data from the Clearinghouse can be found at www.consumer.gov/idtheft and www.consumer.gov/sentinel.

One of the goals of the Clearinghouse and the FTC's identity theft program is to provide support for identity theft prosecutions nationwide.¹³ To further expand the use of the Clearinghouse among law enforcement, the FTC, in cooperation with the Department of Justice and the United States Secret Service, initiated a full day identity theft training seminar for state and local law enforcement officers. Last year, the FTC held sessions in Washington, D.C., Des Moines, Chicago, San Francisco, Las Vegas, and Dallas. More than 600 officers have attended these seminars, representing more than 130 different agencies. This year, the FTC tentatively plans to hold similar training seminars in Phoenix, Seattle, New York, and Houston -- cities the FTC has identified as having high rates of identity theft.

The FTC staff also helps develop case leads. Now in its second year, the Commission runs an identity theft case referral program in coordination with the United States Secret Service, which assigned a special agent on a full-time basis to the Commission to assist with identity theft issues and has provided the services of its Criminal Research Specialists.¹⁴ Together, the FTC and Secret Service staff develop preliminary investigative reports by examining significant patterns of identity theft activity in the database and refining the data through the use of additional investigative resources. Thereupon, the staff refer the investigative reports to appropriate Financial Crimes Task Forces located throughout the country for further investigation and potential prosecution.

¹³The Commission testified last year in support of S. 2541, the Identity Theft Penalty Enhancement Act of 2002, which would increase penalties and streamline proof requirements for prosecution of many of the most harmful forms of identity theft. *See* Testimony of Bureau Director J. Howard Beales, Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Government Information (July 11, 2002).

¹⁴The referral program complements the regular use of the database by all law enforcers from their desk top computers.

C. Outreach and Education

The final mandate for the FTC under the Identity Theft Act was to provide information to consumers about identity theft. Recognizing that the roles of law enforcement and private industry play an important part in the ability of consumers to both minimize their risk and to recover from identity theft, the FTC expanded its mission of outreach and education to include these sectors.

(1) *Consumers*: The FTC has taken the lead in coordinating with other government agencies and organizations in the development and dissemination of comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime. The FTC's extensive, multi-media campaign includes print materials, media mailings, and interviews, as well as the identity theft website, located at www.consumer.gov/idtheft, which includes the publications, descriptions of common identity theft scams, and links to testimony, reports, press releases, identity theft-related state laws, and other resources.¹⁵ The site also has a link to a web-based complaint form, allowing consumers to send complaints directly to the Clearinghouse.

The FTC's comprehensive consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name*, has been a tremendous success. The 26-page booklet, now in its fourth edition, covers a wide range of topics, including how identity theft occurs, how consumers can protect their personal information and minimize their risk, what steps to take immediately upon finding out they are a victim, and how to correct credit-related and other problems that may result from identity theft. It also describes federal and state resources that are available to consumers who have particular problems

¹⁵www.consumer.gov is a multi-agency "one-stop" website for consumer information. The FTC hosts the server and provides all technical maintenance for the site. It contains a wide array of consumer information and currently has links to information from more than 170 federal agencies.

as a result of identity theft. The FTC alone has distributed more than 1.2 million copies of the booklet since its release in February 2000.¹⁶ Last year, the FTC released a Spanish language version of the Identity Theft booklet *Robo de Identidad: Algo malo puede pasarle a su buen nombre*.

(2) *Law Enforcement*: Because law enforcement at the state and local level can provide significant practical assistance to victims, the FTC places a premium on outreach to such agencies. In addition to the training described above, the staff recently joined with North Carolina's Attorney General Roy Cooper to send letters to every other Attorney General letting him or her know about the FTC's identity theft program and how each Attorney General could use the resources of the program to better assist residents of his or her state. The letter encourages the Attorney General to link to the consumer information and complaint form on the FTC's website and to let residents know about the hotline, stresses the importance of the Clearinghouse as a central database, and describes all of the educational materials that the Attorney General can distribute to residents. North Carolina took the lead in availing itself of the Commission's resources in putting together for its resident victims a package of assistance that includes the ID Theft Affidavit (*see* Section II.C.(3)), links to the FTC website, and its own booklet containing information from *Identity Theft: When Bad Things Happen to Your Good Name*. Through this initiative, the FTC hopes to make the most efficient use of federal resources by allowing states to take advantage of the work the FTC has already accomplished and at the same time continuing to expand the centralized database of victim complaints and increase its use by law enforcement nationwide. Other outreach initiatives include: (1) Participation in a "Roll Call" video

¹⁶Other government agencies, including the Social Security Administration, the SEC, and the FDIC also have printed and distributed copies of *Identity Theft: When Bad Things Happen to Your Good Name*.

produced by the Secret Service, which will be sent to thousands of law enforcement departments across the country to instruct officers on identity theft, investigative resources, and assisting victims; and (2) the redesign of the FTC's website to include a section for law enforcement with tips on how to help victims as well as resources for investigations. The FTC will launch the new web site shortly.

(3) *Private Industry:*

(a) Victim Assistance: Because identity theft victims spend significant time and effort restoring their good name and financial records, the FTC devotes significant resources to conducting outreach with the private sector on ways in which victim assistance procedures can be improved. One such initiative arose from the burdensome requirement for victims to complete a different fraud affidavit for each different creditor when the identity thief opened or used an account in the victim's name.¹⁷ To reduce that burden, the FTC worked with private industry and consumer advocates to create a standard form for victims to use in absolving identity theft debts with each of the creditors with whom identity thieves had opened accounts. From its release in August 2001 through February 2003, the FTC has distributed more than 264,000 print copies of the ID Theft Affidavit. There have also been more than 351,000 hits to the Web version. The affidavit is available in both English and Spanish.

Another initiative is the development of a "joint fraud alert" among the three major credit reporting agencies ("CRAs"). This initiative will allow the CRAs to share among themselves requests from identity theft victims that fraud alerts be placed on their consumer reports and copies of their reports

¹⁷See *ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Judiciary Comm.* 106th Cong. (2000) (statement of Mrs. Maureen Mitchell, Identity Theft Victim).

be sent to them, thereby eliminating the victim's need to contact each of the three major CRAs separately. A pilot program is expected to begin this month.

(b) Information Security Breaches: Additionally, the FTC is working with institutions that maintain personal information to identify ways to help keep that information safe from identity theft. Last April, the FTC invited representatives from financial institutions, credit issuers, universities and retailers to a one day informal roundtable discussion of ways to prevent access to personal information in employee and customer records. The FTC will soon publish a self-audit guide to make businesses and organizations of all sizes more aware of how they are managing personal information and to aid them in assessing their security protocols.

As awareness of the FTC's role in identity theft has grown, businesses and organizations who have suffered compromises of personal information have begun to contact the FTC for assistance. For example, in the cases of TriWest¹⁸ and Ford/Experian,¹⁹ in which massive numbers of individuals' personal information was taken, the Commission provided advice on notifying those individuals and what steps they should take to protect themselves. From these experiences, the FTC developed a business record theft response kit that will be posted shortly on the identity theft web site. The kit includes the steps to take in responding to an information compromise and a form letter for notifying the individuals whose information was taken. The kit provides advice on the type of law enforcement agency to contact, depending on the type of compromise, business contact information for the three major credit

¹⁸Adam Clymer, *Officials Say Troops Risk Identity Theft After Burglary*, N.Y. TIMES, Jan. 12, 2003, § 1 (Late Edition), at 12.

¹⁹Kathy M. Kristof and John J. Goldman, *3 Charged in Identity Theft Case*, LA TIMES, Nov. 6, 2002, Main News, Part 1 (Home Edition), at 1.

reporting agencies, suggestions for setting up an internal communication protocol, information about contacting the FTC for assistance, and a detailed explanation of what information individuals need to know. Organizations are encouraged to print and include copies of *Identity Theft: When Bad Things Happen to Your Good Name* with the letter to individuals.

The FTC particularly stresses the importance of notifying as soon as possible individuals whose information has been taken so that they can begin to take steps to limit the potential damage to themselves. Individuals who place a fraud alert promptly have a good chance of preventing, or at least reducing, the likelihood that the theft of their information will turn into the actual misuse of their information. Prompt notification also alerts them to review their credit reports and to keep watch for the signs of identity theft. In the event that they should become victims, they can quickly take action to clear their records before any long-term damage is done. In addition to providing the business record theft response kit, FTC staff can provide individual assistance and advice, including review of consumer information materials for the organization and coordination of searches of the Clearinghouse for complaints with the law enforcement officer working the case.

III. THE FEDERAL TRADE COMMISSION'S ROLE IN INFORMATION SECURITY

In addition to providing assistance to victims of identity theft, the Commission also examines security precautions involving consumers' personal information to determine whether law enforcement may be appropriate. If so, the Commission has two valuable legal tools to work with: Section 5 of the FTC Act,²⁰ which prohibits unfair and deceptive acts or practices, and, starting in May of this year, the Commission's Gramm-Leach-Bliley Safeguards Rule (the "Safeguards Rule" or the "Rule").²¹

A. Law Enforcement Under Section 5

One of the mainstays of the Commission's privacy program is the enforcement of promises that companies make to consumers about privacy, and in particular, the precautions they take to ensure the security of consumers' personal information. The Commission currently enforces such promises both online and offline. The Commission is particularly concerned about breaches involving sensitive information because they put consumers at the greatest risk of identity theft and other harms.

Last August, the Commission announced a settlement with Microsoft regarding misleading claims made by the company about the information collected from consumers through its Passport services – Passport, Passport Wallet, and KidsPassport.²² Passport is a service that collects information from consumers and then allows them to sign in at any participating site using a single name and password. Passport Wallet collects and stores consumers' credit card numbers, and billing and

²⁰ 15 U.S.C. § 45.

²¹ 16 C.F.R. Part 314, available online at <http://www.ftc.gov/os/2002/05/67fr36585.pdf>.

²² The Commission's final decision and order in the Microsoft case is available at <http://www.ftc.gov/os/2002/12/microsoftdecision.pdf>. The Commission's complaint is available at <http://www.ftc.gov/os/2002/12/microsoftcomplaint.pdf>.

shipping addresses, so that consumers do not have to input this information every time they make a purchase from a site. Kids Passport was promoted as a way for parents to create accounts for their children that limited the information that could be collected from them.

The Commission's complaint alleged that Microsoft misrepresented the privacy afforded by these services, including the extent to which Microsoft kept the information secure. For example, in various online statements, Microsoft said that the Passport service "achieves a high level of Web Security by using technologies and systems designed to prevent unauthorized access to your personal information." In fact, the Commission alleged that Microsoft failed to employ reasonable and appropriate measures to protect the personal information collected in connection with these services because it failed to: (1) implement procedures needed to prevent or detect unauthorized access; (2) monitor the system for potential vulnerabilities; and (3) perform appropriate security audits or investigations.

The Commission's order against Microsoft contains strong relief that will provide significant protections for consumer information. First, it prohibits any misrepresentations about the use of and protection for personal information. Second, it requires Microsoft to implement a comprehensive information security program similar to the program required under the FTC's Gramm-Leach-Bliley Safeguards Rule, which is discussed below. Finally, to provide additional assurances that the information security program complies with the consent order, Microsoft must have its program certified as meeting or exceeding the standards in the order by an independent professional every two years. The provisions of the order will expire after 20 years.

Microsoft is an important case because the settlement required that the company adhere to its security promises even in the absence of a known breach of the system. The Commission found even the potential for injury actionable when sensitive information and security promises were involved, and when the potential for injury was significant. This determination is an extremely important principle. It is not enough to make promises about protecting personal information, and then just hope that nothing bad happens or, if it does, that nobody finds out. Fulfilling privacy and security promises requires affirmative steps to ensure that personal information is appropriately protected from identity theft and other risks to consumers' personal information.

The Microsoft case followed on a similar case the Commission settled earlier last year against Eli Lilly.²³ The Lilly case also involved alleged misrepresentations regarding the security provided for sensitive consumer information – in that case, consumers' health information. Like Microsoft, Lilly made claims that it had security measures in place to protect the information collected from consumers on its website. As in Microsoft, the Commission charged Lilly with failing to have reasonable measures in place to protect the information.

Specifically, in sending an e-mail to Prozac users who subscribed to a service on the site, Lilly put all of the consumers' email addresses in the "To" line of the e-mail, essentially disclosing to all users the identities of all of the other Prozac users. The Commission's complaint alleged that this happened because Lilly failed, among other things, to provide appropriate training and oversight for the employee who sent the email and to implement appropriate checks on the process of using sensitive customer data.

²³ The Commission's final decision and order against Eli Lilly is available at <http://www.ftc.gov/os/2002/05/elilillydo.htm>. The complaint is available at <http://www.ftc.gov/os/2002/05/elilillycmp.htm>.

The order in the Lilly case prohibits the misrepresentations and, as in Microsoft, requires Lilly to implement a comprehensive information security program.

It is important to note that the Commission is not simply saying “gotcha” for security breaches. While a breach may indicate a problem with a company’s security, breaches can happen even when a company takes all reasonable precautions. In such instances, the breach does not violate the laws that the FTC enforces. Instead, the Commission recognizes that security is an ongoing process of using reasonable and appropriate measures in light of the circumstances. That is the approach the Commission took in these cases and in its Gramm-Leach-Bliley Safeguards Rule, and the approach it will continue to take.

B. GLB Safeguards Rule

Last May, the Commission finalized its Gramm-Leach-Bliley Safeguards Rule, which requires financial institutions under the FTC’s jurisdiction to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information. On May 23, 2003, the Rule becomes effective and the Commission expects that it will quickly become an important tool to ensure greater security for consumers’ sensitive financial information. Whereas Section 5 authority derives from misstatements particular companies make about security, the Rule requires a wide variety of financial institutions to implement comprehensive protections for customer information – many of them for the first time. The Rule could go far towards reducing risks to this information, including identity theft.

The Safeguards Rule requires financial institutions to develop a written information security plan that describes their program to protect customer information. Due to the wide variety of different entities covered, the Rule requires a plan that takes into account each entity’s particular circumstances –

its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

As part of its plan, each financial institution must: (1) designate one or more employees to coordinate the safeguards; (2) identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks; (3) design and implement a safeguards program, and regularly monitor and test it; (4) hire appropriate service providers and contract with them to implement safeguards; and (5) evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards. The Safeguards Rule requires businesses to consider all areas of their operation, but identifies three areas that are particularly important to information security: employee management and training; information systems; and managing system failures.

The Commission has already issued guidance to businesses covered by the Safeguards Rule to help them understand the Rule's requirements.²⁴ Commission staff are currently meeting with trade associations and companies to find out how industry is progressing in coming into compliance with the Rule, to discuss areas in which additional FTC guidance might be appropriate, and to gain a better understanding of how the Rule will affect particular industry segments. When the Rule becomes effective, the Commission plans to conduct sweeps to assess compliance within various covered industry segments.

²⁴ *Financial Institutions and Customer Data: Complying with the Safeguards Rule*, available at <http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm>.

C. Education and Workshops

The FTC also plays a role in improving security and reducing the risks to personal information by fostering dialogue and educating the public on security issues. For example, the Commission held a workshop last May to examine the security of consumer information – both as maintained by consumers on their own computers and by businesses in their systems.²⁵

The main messages from the workshop are: (1) That consumers need greater education about steps they can take to protect their information; (2) that manufacturers, ISPs, and other businesses need to make it easier for consumers to protect themselves; and (3) that the government and private sector should work together to create a “culture of security” for consumers and businesses. Since then, the Commission has launched a major initiative to educate consumers and businesses about security. The Commission created a new mascot for this effort, Dewie the Turtle, who has his own web site at www.ft.gov/infosecurity that offers practical tips for staying secure online; complying with the Commission’s Safeguards Rule; staying secure when using dial up or broadband access; and other resources available to consumers.

Finally, in May and June of this year, the Commission will host two workshops focusing on the role technology plays for both consumers and businesses in protecting personal information.²⁶ A number of products promise to help consumers control their sensitive information and guard against internal and external threats. Similarly, there are an increasing number of products designed to help businesses

²⁵ Additional information about the workshop is available at <http://www.ftc.gov/bcp/workshops/security/index.html>.

²⁶ Additional information about the workshop is available at <http://www.ftc.gov/bcp/workshops/technology/index.html>.

manage the consumer information they maintain and ensure that it is secure. Despite the widespread availability of these products, however, it is unclear just how much consumers and businesses are using them and whether they are meeting consumer and business needs in this area. The Commission's workshops will foster a wide-ranging discussion on these issues, with the goal of gaining a better understanding of whether technology is being used effectively to protect personal information.

IV. CONCLUSION

Large scale security breaches place substantial costs on individuals and businesses. The Commission, through its education and enforcement capabilities, is committed to reducing these breaches as much as possible. The Commission will continue its efforts to assist criminal law enforcement with their investigations. Prosecuting perpetrators sends the message that identity theft is not cost-free. Finally, the Commission knows that as with any crime, identity theft can never be completely eradicated. Thus, the Commission's program to assist victims and work with the private sector on ways to facilitate the process for regaining victims' good names will always remain a priority.