Testimony and Statement for the Record of

Professor Deirdre K. Mulligan
Clinical Professor of Law;
Director, Samuelson Law, Technology & Public Policy Clinic
Faculty Director, Berkeley Center for Law and Technology
Director, Clinical Program

&

Chris Jay Hoofnagle
Senior Staff Attorney, Samuelson Law, Technology & Public Policy Clinic
Senior Fellow, Berkeley Center for Law and Technology

Boalt Hall School of Law
UC-Berkeley
396 Simon Hall
Berkeley, CA 94720

Hearing on
Identity Theft: Innovative Solutions for an Evolving Problem

Before the Senate Judiciary Committee
Subcommittee on Terrorism, Technology and Homeland Security
Chairwoman Feinstein Presiding

March 21, 2007
2:30 PM
Dirksen-226

Introduction

Chairwoman Feinstein, Ranking Member Kyl, and Members of the Subcommittee, thank you for providing the opportunity to participate in this timely and important hearing. I am senior staff attorney to the Samuelson Law, Technology & Public Policy Clinic, based at Boalt Hall School of Law (University of California-Berkeley). Joining me in this testimony is Professor Deirdre K. Mulligan, who directs both the Samuelson Clinic and the Center for Clinical Education at Boalt Hall. Professor Mulligan played a key role in the conception and drafting of California Assembly Bill 700 when then Assemblyman Joseph Simitian, which was enacted by the State's legislature as SB 1386.

The Samuelson Clinic gives students hands-on training while providing a new voice for the public interest. Through the clinic, students file friend-of-the-court briefs, comment on proposed legislation and regulations, and provide legal assistance in matters that raise important issues relating to law and technology. The clinic represents consumer interests in intellectual property, communications regulation and privacy issues.

Professor Mulligan is a member of the Team for Research in Ubiquitous Secure Technology (TRUST), a multi-disciplinary, multi-institutional research project funded by the National Science Foundation. TRUST is devoted to the development of new science and technology that will transform the ability of organizations to design, build, and operate trustworthy information systems. As part of its research, TRUST is developing improved technology to combat phishing, spyware, botnets, and related threats, and studying the policy and legal context and implications of related activities such as ID theft. TRUST researchers have developed anti-phishing technologies, explored enhanced

web authentication methods, studied human factors in the installation of spyware, and researched the growing problem of botnet attacks on the internet. The full scope of TRUST's research is available online at http://www.truststc.org/. Students and staff of the Clinic and PhD and post-docs working with Professor Mulligan participate in research and policy development related to TRUST's agenda.

In our testimony today, we make recommendations on how to address the evolving problem of identity theft, including a proposal to require banks to report on identity theft incidents, and credit freezes; explain the often overlooked policy goals and benefits of security breach notification laws; provide feedback on S. 239, the Notification of Risk to Personal Data Act of 2007 and S. 495, the Personal Data Privacy and Security Act of 2007.

Overview

Congress should consider the broad policy goals of security breach notification laws. These laws are "light-weight regulatory mechanisms," modeled upon groundbreaking environmental statutes that require public reporting of releases of toxic chemicals. Like their environmental analogues, security breach notification laws create strong incentives for investment in best practices. They create incentives to reduce reliance upon sensitive personal information, particularly the Social Security number. And, they have identified areas where more security investment is needed, most immediately in the securing of laptop computers.

Research should inform policy on security breach notification. We are performing several empirical studies into aspects of security breaches. These include

research into how entities are giving notices under the current state laws, and a study into how security breach notification laws have affected security investment.

Central, standardized reporting of breaches, similar to the form of reporting required by toxic chemical release statutes would improve the effect of security breach notification efforts, by creating a centralized base of knowledge about security risks and failures that will facilitate the identification of areas ripe for best practices (whether industry driven or regulatory), identify long-hanging fruit for immediate resolution through the deployment of existing technology, practices and policies, facilitate risk assessment critical to the development of internal policies as well as external risk mitigation systems such as insurance markets, and support research to further enhance our capacity to develop secure trustworthy information systems. That is, security breaches should be registered with a federal agency and statistical information about these incidents should be made available to the public by default. Access to basic information about who has experienced breaches and how the breaches occurred will provide important guidance about how to improve the information security landscape.

The security breach notification laws around the country are laying the groundwork for a data-driven analysis of possible improvements in information and network security. Advances in the policy and technological solutions to identity theft, similarly, depend upon the availability of valid data. This data is lacking, and the policy discussion is weakened by its absence. Currently, identity theft is measured through survey polls of victims that cannot fully capture the scope of the problem. If lending institutions themselves were to report on the prevalence and severity of identity theft, a more complete picture of the problem could emerge, and adequate resources and policies

could be allocated to fighting the crime. Reporting could also create a market for identity theft safety, where banks compete to provide the products most impervious to the crime.

Credit freezes, also known as security freezes, represent an important state innovation in fighting identity theft. Because lending institutions ignore fraud alerts too frequently, credit freezes are the only remedy individuals can effectively use to prevent identity theft in certain situations. Individuals should be able to enjoy the benefits of security freezes as no cost, and be able to "thaw" their credit file quickly in order to take advantage of opportunities.

Security Breach Notification

Regulatory interventions, such as the requirement to notify individuals of security breaches, play an important role in shaping institutions' policies. The duty to give individuals notice of security breaches is similar to public reporting duties embodied in the Emergency Planning and Community Right-to-Know Act of 1986 ("EPCRA").[1] That law requires companies to make inventories of certain toxic chemicals, and to report to the public when such chemicals are released. EPCRA is reported to have a dramatic effect in reducing the prevalence of toxic releases. We make several observations on how EPCRA created a "race to the top" and how security breach notification laws have created similar incentives to improve practices:

First, just as EPCRA created strong incentives to secure toxic chemicals, security breach laws create incentives for information security investment. Prior to enactment of these laws on the state level, businesses were free to keep security incidences secret, and in effect, pass the costs to individuals who would be subject to identity theft and other

[1] 42 USC § 11023 (2007).

misuse of their data. The 2002 Computer Science and Telecommunications Board (CSTB) report on cyber security[2] noted several barriers to adequate investment in security:

- Security is expensive and is not productive,[3] which creates an incentive to invest as little as possible in security.
- Security is hard to measure, breaches are difficult to notice, and, as a result, might go unreported.
- Security has an "arms race" quality of action and reaction.
- It is easier to attack a system than it is to defend; a system might have many vulnerabilities, any one of which might be a single point of failure.
- Policymakers and researchers face a particularly acute problem of having insufficient data about information system security vulnerabilities.
- Security is an externality.[4]

The research literature on security identifies the need for a scheme to encourage investments in trustworthiness, because there is a gap between the self-interests of businesses (namely, not to invest in trustworthiness) and what's best for society (namely, trustworthy systems). Traditionally, such gaps are bridged by law and government

[2] National Research Council (CSTB), *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*.

[3] By this I mean that security investments do not directly contribute to individual or business productivity. I cannot use anti-virus software to write law review articles, though virus protection lowers the risk that I'll have to spend time and money recovering from a computer virus.

[4] According to Camp and Wolfram, "[e]conomists define externalities as instances where an individual or firm's actions have economic consequences for others for which there is no compensation." Compensation, of course could flow to or from the actor, leading to the distinction between *positive* (uncompensated benefits to others) and *negative* (uncompensated costs imposed on others) externalities. Economists also define a third externality, the *network externality*, which describes "products for which the utility that a user consumption of the good increases with the number of other agents consuming the good." Michael Katz and Carl Shapiro, *Technology Adoption in the Presence of Network Externalities*, 94 J. Pol. Econ. 822 (1986).

regulation. Thus, the question is what legal rules might be effective in altering investments. Security breach notification laws have caused entities to internalize more of the costs of the use and misuse of personal information, by responding to some of the failings noted by the CSTB.

Second, information disclosure and reporting mechanisms can encourage companies to reduce the risk to the public of a harm, without directing the business to take specific actions. Whereas typically, regulation places government in the midst of business practices to specify standards and procedures, these light-weight mechanisms leave businesses with more leeway for finding solutions. The mechanism ensures compliance through transparency, using "sunlight as a disinfectant." They also mitigate a key objection to regulation, in that they do not reify a given set of best practices but rather encourage those in the best position to evaluate new threats and risks to invest wisely in technologies, practices and policies to secure assets and information.

In the context of security breach notification laws, as part of the internalization of costs, entities have much stronger incentives to reduce the collection of sensitive personally identifiable information, particularly the Social Security number. Because the Social Security number plays a key role in identification and authentication in the credit markets, it is important that information policy discourage its collection and use.

Third, in the EPCRA context, disclosure of toxic releases provided benchmarks and information that could inform where additional investment was needed. The same is true in the security breach notification context. These laws have identified areas where more security investment is needed. For instance, based on news reports and statements issued by entities that have experienced breaches, we know that laptop theft is a major

vector for data loss. Investments can now be tailored to that specific vector, and we believe we will see new products developed to ensure that data on laptops are more secure from theft. We know that the economic calculus around investment in encrypting data on portable devices has been altered due to security breaches that have been disclosed.

Accordingly, like the EPCRA before it, security breach laws perform more functions than simply warning individuals of risk. As such, focusing only on identity theft is a narrow view of the benefits of security breach notification laws. These laws have contributed to security investment, changes in the collection of personal information, and a better understanding of security risks.

In our research, we are interviewing Chief Security Officers to understand the effect of the security breach disclosure laws on their role in the institution and the institutions behavior and investments around information and network security. We have also collected 206 security breach notification letters. We are coding the letters for over thirty variables to learn more about breaches and how companies choose to give notice. For instance, we are trying to determine how long entities take to provide notice after experiencing a breach, what vulnerabilities cause breaches, whether entities typically offer credit monitoring or other remedial efforts, and whether basic letter writing forms are followed (i.e. whether a date appears on the letter, whether contact information for the entity experiencing the breach is provided, and so on). When we have completed coding the information, we will share our report and raw statistics with the Committee and the public.

Security Breach Notification: State Law Innovations

As part of our research, we have surveyed the various state laws that require notification of security breaches. Several states have created new innovative approaches to the problem. These innovations should be considered in any federal legislation; some should be adopted.

First, several states, including New York, New Jersey, and North Carolina, require some form of centralized reporting after a breach. This is an important innovation that should be adopted at the federal level. There are cases where a breach affects a single individual. These breaches may be a result of exceptionally poor practices, but are unlikely to come to public light if small numbers of individuals are told of them. Centralized reporting will allow consumer protection authorities to track trends in security breaches, large and small, and to determine whether entities are providing adequate protections for information.

Second, both New York and North Carolina officials have developed standard forms for reporting breaches. These forms are attached as Appendix A. A version of them should be adopted at the federal level. Having a standard form encourages entities to disclose basic information about breaches, such as the date that the breach occurred, how it occurred, and how many people were affected. In our coding of security breach letters, we have already found that this basic information is omitted in some cases. Reporting also allows for the statistical study of breaches, which in turn, can inform information security policy and investment.

Similar form reporting under the EPCRA has enabled citizens to use toxic release data for civic engagement and research. Benchmarking and information analysis will be possible if form reporting is mandated for security breaches.

Finally, states have created new personal information triggers for security breaches. Some protect medical information, and the account numbers of savings and checking accounts, account passwords, and biometric identifiers.

S. 239, The Notification of Risk to Personal Data Act of 2007

Senate Bill 239, the Notification of Risk to Personal Data Act of 2007, is an ambitious proposal that will require both businesses and federal government agencies to give notice of some information security breaches. The legislation is broader than many state mandates, in that it covers a wider array of companies that possess but do not own personal information. For instance, a company that processes data for others that experiences a breach may not have to give notice under state laws, as it neither owns nor licenses the data. S. 239 would fix this loophole.

It defines security breaches broadly, but only requires notice of breaches involving "sensitive personally identifiable information." Nevertheless, many identifiers can serve as a trigger for issuing a breach notice. For instance, biometric data, account numbers, and combinations of home address, date of birth, and mother's maiden name can constitute "sensitive personally identifiable information."

The Safe Harbor

A significant safe harbor in the legislation allows covered entities to avoid giving notice if a risk assessment is performed that concludes that, "no significant risk that the security breach has resulted in, or will result in, harm to the individuals whose…"

information was breached. The risk assessment must be disclosed to the United States Secret Service, but the bill does not specify whether the risk assessment or basic statistical data about the breach will be made publicly available.

California law has no safe harbor for risk of harm to individuals. California Civil Code 1798.82(a) specifies that notice is required whenever, "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

While the legislation broadens the types of identifiers subject to security breach notification, the "significant risk" safe harbor creates a loophole that could allow entities to "look the other way" in order to avoid giving notice. This is a significant tradeoff.

Furthermore, it introduces the concept of "harm" into privacy law. Privacy law generally does not require individuals to demonstrate injury in order to recover for an invasion of privacy. Most privacy statutes provide money damages by default if a violation is proven.

Harm is also inappropriate because it is a subjective standard, and it is often equated with physical injury, which is rare in privacy violations. A more appropriate standard would be "misuse" of personal information. "Use" of personal information is well understood in privacy law; many privacy statutes set forth acceptable and unacceptable uses of data.

Misuse is more intuitive, more flexible, and more applicable to a situation where data is stolen but the wrongdoer intends some other type of action than identity theft. Individuals may have particularized sensitivity to having personal information released. For instance, the release of basic contact information of a victim of domestic violence

could cause harm completely unrelated to identity theft or fraud, although the institution experiencing the breach would not perceive this problem, and conclude that there is no significant risk of harm to the individual. Similarly, victims of stalking live with the same risks. Information may be accessed and disclosed simply to embarrass another, or in the case of the Hewlett-Packard pretexting controversy, to investigate another person in an invasive way. All of these risks could be covered by the concept of misuse of information.

We believe that security breach notification laws should favor disclosure over non-disclosure. Allowing the entity that experienced the breach, rather than the individual who may be affected by it, to decide whether to give notice favors non-disclosure. A better standard would be to place the onus on the entity to certify that there is no reasonable risk of misuse of information.

The risks of non-disclosure could be addressed by requiring public, statistical reporting on the breach to a federal agency. Appendix A has two examples of forms required for centralized reporting in New York and North Carolina. These forms contain basic but critical information that individuals can use after a breach occurs, including the date on which the breach occurred, the date when notice was issued, the number of people affected, contact information for the entity, and a simple explanation of what happened. Such reporting could provide a check upon entities that seek to avoid giving notice inappropriately.

The Financial Fraud Prevention Exemption

The financial fraud prevention exemption allows any business entity to be exempt from the notice requirement if it uses or participates in a security program that blocks

unauthorized financial transactions. This exemption is intended to limit the duty to give notice of security breaches where credit card numbers alone are lost or stolen.

This exemption should be considered carefully. It essentially is a sector-specific exemption from a broad information security law. It is not clear why credit card companies, a sector whose products have been identified with the largest data breaches, should be given special, preferential treatment here. Many of the largest information security breaches, ones that led to an understanding that there were weaknesses in compliance with the Payment Card Industry Data Security Standard, would never have come to light if this exemption were in place.

Additionally, in effect, the exemption mandates the use of a specific technological approach to preventing fraud.

Requiring notice in situations where the security program fails and fraud or unauthorized transactions have occurred is insufficiently narrow. Entities often cannot determine basic information about a breach. It is likely that an investigation into a breach could not determine whether that specific breach led to fraud or authorized transactions.

Contents of Notice

The bill specifies that notices sent to individuals include a description of the information stolen, a toll-free number of the entity that experienced the breach, and contact information for the major consumer reporting agencies.

It is important that other information be included as well. We have found that some entities' breach notification letters lack basic information. In some cases, the letters are undated. In others, the timeframe of the breach is not disclosed.

There is also a risk that disclosure may be obscured by promotional text. For instance, in Appendix B, we attach a breach notification letter from H&R Block. Unlike other breach notification letters, the H&R Block one does not advise the reader of the security incident until the second paragraph. The first paragraph only discusses a company promotion and notes how useful its product is.

Notices can be written so as to discourage readership. For instance, in *Ting v. AT&T*, a district court found that AT&T conducted research to develop a notice regarding new contract terms that consumers would be likely ignore.[5] Legislation should anticipate and discourage such efforts.

S. 495, the Personal Data Privacy and Security Act of 2007

Senator Leahy's S. 495, the Personal Data Privacy and Security Act of 2007, incorporates much of the same language of S. 239. In differs in several important ways, and these differences make S. 239 a superior bill. Three provisions of S. 495 are problematic and will limit the policy objectives of security breach notification laws.

First, S. 495 exempts a broader scope of public record information from notification duties than S. 239. S. 495 would create a notice loophole in cases where an entity had a database of sensitive personal information stolen, so long as the data derived from a public record.

---

[5] "Another part of AT&T's research, the Qualitative Study, concluded that after reading the bolded text in the cover letter which states 'please be assured that your AT&T service or billing will not change under the AT&T Consumer Services Agreement; there's nothing you need to do,' 'at this point most would stop reading and discard the letter.' (J. Ex. 9-9.) One of the authors of the study did not find this conclusion to be a cause of concern, and no one on the detariffing team ever expressed concern to her about this conclusion." *Ting v. AT&T*, 182 F. Supp. 2d 902 (N.D. Cal. 2002).

This loophole is problematic, because sensitive information contained within public records often exist in "practical obscurity." That is, they are public records, but they are stored in media generally inaccessible to the public. Once aggregated, these records create a powerful new vector for misuse of personal information.

Just imagine the impact to untold numbers of Americans who have purchased a home, and in the process, had their Social Security numbers filed on the deed. Those Social Security numbers are essentially locked in paper public records across the country. If a company collects that information and digitizes it, thereby making it more accessible to wrongdoers, why should it be exempt from security breach notification?

The Supreme Court has recognized that aggregations of otherwise public information create new risks to privacy. In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the Court held that disclosure of FBI-aggregated rap sheets, detailing criminal histories, violated the privacy exemption of the Freedom of Information Act. Although the data contained in the compilation of the rap sheets were technically public, they were distributed across the country in documents that were difficult to access. The Court observed that in "an organized society, there are few facts that are not at one time or another divulged to another." It logically flows that an aggregation of these facts could end individuals' right to privacy. The Court appropriately recognized that there is a "distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole."[6]

[6] 489 U.S. at 763 (1989).

In aggregating information from obscure public records, entities make it more likely that this information can be misused. If such an entity suffers a breach, it is just as serious as one where the information was collected by other means. Such an exemption undermines the public policy objectives of security breach notification laws, and may create incentives for entities to inject sensitive personal information into the public record so that privacy laws do not cover it. The broader language from S. 495 should not be included in S. 239.

Second, S.495 provides immunity to the proposed crime of intentionally and willfully concealing a security breach. Individuals qualify for this immunity if they inform the Secret Service of the security breach risk assessment and the agency does not direct the entity to give notice within ten days. We think it extremely unlikely that the Secret Service will have the capacity to routinely review and act upon risk assessments with ten days of their receipt. It will thus make this protection against wrongful concealment illusory and impossible to enforce. This immunity provision should not be included in S. 239.

Finally, S. 239 requires the Secret Service to issue a report to Congress on security breaches. S. 495 limits this important report by prohibiting it from containing any information from a risk assessment. The Secret Service's report should not be limited in this way. For instance, the agency may want to report examples of risk assessments that, in its opinion, were inadequate or demonstrated poor security procedures. This provision should not be included in S. 239.

Identity Theft Reporting

Another aspect in which research could be used to aid policy development on identity theft is to require lending institutions to report basic data about the crime. While there is widespread agreement that identity theft causes financial damage to consumers, creditors, retail establishments, and the economy as a whole,[7] not enough is known about the contours of the crime. We do not have reliable statistics to measure how much of it there is, the relative rates of credit card fraud or "new account" thefts, or how much the crime impacts the economy.

The lack of data on identity theft causes serious problems. As a result, we cannot determine the scope of the crime and the resources that should be allocated to it. We cannot determine whether various consumer protection interventions have been effective. We cannot tell whether consumers, regulators, and businesses are over or under reacting to the crime. We cannot determine whether identity theft is more or less prevalent, or more or less severe than a year ago. We cannot determine how the costs of the crime are being distributed back upon society.

The inability to fully understand the crime stems from the methods used to measure it--what we do know has been learned through telephone and internet surveys. While well-intentioned, and valuable for some purposes in the identity theft policy debate, these surveys cannot completely document the contours of the crime.

More fundamentally, surveys ask the wrong people about the crime. The surveys performed seek to obtain information about the crime from victims, individuals who have

[7] GOVERNMENT ACCOUNTABILITY OFFICE, IDENTITY THEFT, AVAILABLE DATA INDICATE GROWTH IN PREVALENCE AND COST GAO-02-424T (Feb. 14, 2002), available at http://www.gao.gov/new.items/d02424t.pdf.

the most limited view of the problem. Victims often cannot tell how the crime occurred, how their information was stolen, or who stole it. Emerging forms of the crime, such as "synthetic identity theft" (also known as fictitious identity theft), occur in such a way that the individual whose data was used never becomes aware of the crime, and thus cannot report being a victim in a survey poll.

A solution can be found in gathering information from the entity that knows the most about the crime—the lending institution. If "lending institutions," companies that actually extend credit (such as banks and credit card companies) and those that control access to accounts (including payment companies such as Paypal and Western Union), were required to provide statistical data about the crime, a more complete and focused picture would emerge. Lending institutions have not provided this information because it could cause embarrassment and because it could attract unwanted regulatory attention.

In a new paper, Chris Hoofnagle proposes that lending institutions should be required to disclose 1) how many identity theft incidences they suffered or avoided, 2) the form of identity theft attempted (i.e. new account fraud, credit card fraud, etc.) and the product targeted (mortgage loan, credit card, etc), and 3) the amount of loss suffered or avoided.[8]

This proposed intervention is relatively simple and does not require extensive regulatory mandates. While there are many challenges, practically and politically, to implementing it, it would result in great benefit to the public. It will enable benchmarking and the identification of additional consumer protections that work and those that do not. It will help regulators and law enforcement allocate the proper

[8] Chris Jay Hoofnagle, *Identity Theft: Making the Known Unknowns Known* (March 2007), available at http://ssrn.com/abstract=969441

resources to fight the crime. It will help clear the air of suspicious polling mischief, the release of surveys that have used questionable assumptions to pin the blame of identity theft to the victims of the crime.

Credit Freeze

Finally, we wish to briefly address the merits of and need for the ability for individuals to have credit freeze rights. Credit freeze gives individuals the option to have more control over their credit reports, while allowing the information to flow for legitimate business purposes, such as to maintain existing accounts.

Credit freeze is necessary because of lax credit granting practices that have made it impossible for consumers to avoid identity theft. This is because the credit reporting system law treats credit issuers, such as retailers and credit card issuers, as trusted insiders. As trusted insiders, credit issuers can easily gain access to reports with or without legal justification.

Furthermore, these trusted credit issuers have not adopted sound measures for determining the actual identity of credit applicants. Such protocols allow identity thieves to open new accounts in others' names. And the harm of identity theft is heightened by the alacrity with which credit grantors issue credit. Competition in the credit markets motivates companies to issue first, and the ask questions later. This allows identity thieves to quickly obtain multiple credit lines.

There is no better illustration of this problem than the rise of "synthetic identity theft" cases. In synthetic identity theft cases, the impostor creates a new identity using some information from a victim that is enhanced with fabricated personal information.[9]

[9] FDIC, PUTTING AN END TO ACCOUNT-HIJACKING IDENTITY THEFT (Dec. 14, Mulligan & Hoofnagle, IDENTITY THEFT:

For instance, the impostor may use a real Social Security number, but a falsified name and address. Since this synthetic identity is based on some real information, and sometimes supplemented with artfully created credit histories, it can be used to apply for new credit accounts.

Examples of mistakes in credit granting abound in the media, and bring into question whether consumers can do anything to avoid identity theft, short of freezing their credit report:

- One consumer took an unsolicited credit card offer, ripped it up, reassembled it with tape, and then submitted it to a bank with a change of address. The bank issued the card, and even sent it to the different address, thus demonstrating that a thief could easily use even a torn-up offer for fraud.[10]
- Chase Manhattan bank issued a platinum visa card to "Clifford J. Dawg." In this instance, the owner of the dog had signed up for a free e-mail account in his pet's name and later received a pre-approved offer of credit for "Clifford J. Dawg." The owner found this humorous and responded to the pre-approved offer, listing nine zeros for the dog's Social Security number, the "Pupperoni Factory" as employer, and "Pugsy Malone" as the mother's maiden name. The

---

2004), available at http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html; Fred H. Cate, *Information Security Breaches and the Threat to Consumers* (Sept. 2005), available at http://www.hunton.com/files/tbl_s47Details/FileUpload265/1280/Information_Security_Breaches.pdf.

[10] Bob Sullivan, *Even torn-up credit card applications aren't safe*, MSNBC, Mar. 14, 2006, available at http://redtape.msnbc.com/2006/03/what_if_a_despe.html.

owner also wrote on the approval: "You are sending an application to a dog! Ha ha ha." The card arrived three weeks later.[11]

- Credit has been offered and issued to other dogs, including Monty, a Shih-Tzu who was extended a $24,600 credit line.[12] It also has been granted to children and babies.[13]
- In *Vazquez-Garcia v. Trans Union de Puerto Rico*, Sears issued a credit card to an impostor who used the victim's Social Security number but wrong address and date of birth. The victim was a resident of Puerto Rico, but several cards were issued to an impostor using a Nevada address.[14]

---

[11] *Dog Gets Carded*, Wash. Times (Jan. 30, 2004), available at http://washingtontimes.com/upi-breaking/20040129-031535-6234r.htm; *Dog Issued Credit Card, Owner Sends In Pre-Approved Application As Joke*, NBC San Diego (Jan. 28, 2004), available at http://www.nbcsandiego.com/money/2800173/detail.html.

[12] *Identity thieves feed on credit firms' lax practices*, USA TODAY, Sept. 12, 2003, p. 11A; Kevin Hoffman, *Lerner's Legacy: MBNA's customers wouldn't write such flattering obituaries*, CLEVELAND SCENE, Dec. 18, 2002; Scott Barancik, *A Week in Bankruptcy Court*, ST. PETERSBURG TIMES, Mar. 18, 2002, p 8E.

[13] IDENTITY THEFT RESOURCE CENTER, FACT SHEET 120: IDENTITY THEFT AND CHILDREN, available at http://www.idtheftcenter.org/vg120.shtml.

[14] 222 F. Supp. 2d 150 (D.P.R. 2002). Many other cases demonstrate that credit can be obtained by imposters, even when they use incorrect personal information. In *Nelski v. Pelland*, 2004 U.S. App. LEXIS 663 (6th Cir. 2004), Ameritech opened an account for an impostor who used the victim's name, but a different address and slightly different Social Security number. In *Dimezza v. First USA Bank, Inc.*, 103 F. Supp. 2d 1296 (D.N.M. 2000), First USA Bank issued a credit card to an impostor who used the victim's Social Security number but a different first name and address. In *Alward v. Fleet Bank*, 22 F.3d 616 (8th Cir. 1997), Fleet Bank issued two credit cards in the name of the victim to a New York address. The victim had never lived in that state. In *Fritzhand v. Discover Financial Services*, 800 N.Y.S.2d 316 (New York Supreme Court, Nassau County 2005), Discover accepted a $14,000 balance transfer from a fraudulently-obtained American Express account. Both accounts were opened with the victim's name but with a fictitious address. In *Farley v. Williams & U.C. Lending*, 2005 U.S. Dist. LEXIS 38924 (W.D.N.Y. 2005), a store line of credit and a Citibank platinum card were issued to an impostor using the victim's name and Social Security number but the impostor's home address.

These anecdotal examples from news reports and litigation demonstrate that in some cases, credit is issued to people who obviously are impostors. Simple tools long available to lending institutions, such as address verification databases, could have prevented the frauds. But the individual has no ability to ensure that lending institutions are using these tools, nor can they avoid these unsophisticated cases of identity theft.

Credit freeze could put consumers back in control of their credit reports, and thus, act as a shield against even the most irresponsible granting practices.

Conclusion

Madame Chairwoman, thank you again for inviting us to participate in this hearing. As our research into security breach notification and investments in privacy and security progresses we will update the Committee about our findings. We would be honored to speak with the Committee in depth about the issues raised above and other proposals to reduce the risks of identity theft and improve information and network security more broadly.

Reporting Form
For Business, Individual or NY State Entity reporting a "Breach of the Security of the System" Pursuant to the Information Security Breach and Notification Act (General Business Law §889-aa; State Technology Law §208)

Name of Business, Individual or State Entity: H&R Block
Date of Discovery of Breach: December 19, 2005
Estimated Number of Affected Individuals: 28,750
Date of Notification to Affected Individuals: December 22, 2005
Manner of Notification: [X] written notice
[ ] electronic notice (email)
[ ] telephone notice

Are you requesting substitute notice? [ ] Yes [X] No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice.

As part of a promotional campaign, H&R Block recently mailed free copies of our TaxCut® tax preparation software to a select group of individuals. For a small percentage of recipients of this mailing, we inadvertently included some personal information in the mailing label. Embedded within the more than 40-character source code were the nine digits of the recipient's Social Security Number (SSN). These digits were not formatted in a way that identified them as an SSN, and to an unknowing observer they would appear to be random digits within a very long character string. However, the recipient may have recognized his or her own SSN. H&R Block quickly recognized the error and is voluntarily notifying all affected recipients to advise them of the situation and offer helpful information. The actual notice provided to affected New York residents is included as Attachment A.

Name of Business or Individual Contact Person: Murray Walton
Title: Vice President and Chief Compliance Officer
Telephone number: 816-932-8414
Email: mwalton@hrblock.com
Dated: December 29, 2005
Submitted by: Murray Walton
Title: Vice President and Chief Compliance Officer
Address: 4400 Main Street
Kansas City, MO 64111
Email: mwalton@hrblock.com
Telephone: 816-932-8414 Fax: 816-932 -8462

North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005

Name of Business Owning or Licensing Information Affected by the Breach: _____
Address: _____
_____
Telephone: _____
Fax: _____
Email: _____

PLEASE SUBMIT FORM TO:
Consumer Protection Division
NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6000
Toll Free in NC: (877) 566-7226
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: _____

Date the Security Breach was discovered: _____

Estimated number of affected individuals: _____

Estimated number of NC residents affected: _____

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b): _____
_____

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: _____
_____

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. _____ If so, please describe the security measures protecting the information: _____
_____

Describe any measures taken to prevent a similar Security Breach from occurring in the future: _____
_____

Date affected NC residents were/will be notified: _____

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c)): _____
_____

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified?
(pursuant to N.C.G.S. § 75-65(e))
Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

- ☐ written notice
- ☐ electronic notice (email)
- ☐ telephone notice
- ☐ substitute notice

Signature: _____ Date: _____
Contact Person, Title: _____
Address: _____
(if different from above) _____
Telephone: _____ Fax: _____ Email: _____

Attachment A
Notice to New York Residents

December 22, 2005

[FirstName] [LastName]
[Address]
[City], [State] [ZIP]

Dear [FirstName] [LastName]:

Recently we mailed you a free copy of our TaxCut® software. We believe that this complimentary software will meet your 2006 tax preparation needs, based on our prior experience with you as an H&R Block client. We hope that you will try TaxCut and find it to be a great solution for filing your next tax return.

However, since we originally sent you this CD, we have become aware of a mail production situation that has affected a small percentage of recipients, including you. Due to human error in developing the mailing list, the digits of your social security number (SSN) were used as part of your mailing label's source code, a string of more than 40 numbers and characters. Fortunately, these digits were embedded in the middle of the string, and they were not formatted in any manner that would identify them as an SSN.

Nevertheless, we sincerely apologize for this inadvertent error, which is completely inconsistent with our strict policies to protect our clients' privacy. Our internal policies limit the use of client SSNs for purposes other than tax preparation. Furthermore, our internal procedures require that mailing source codes are formulated in a manner that excludes use of any sensitive or confidential information. Please know that we have conducted a thorough internal review of this matter, and are taking actions to ensure this does not re-occur.

Again, please understand that the digits of your SSN were embedded in the middle of a lengthy source code, and they were not formatted in a manner that identifies them as an SSN. As a result, we believe the exposure of your SSN digits was limited to you alone, since you are the only person who would recognize their significance. Nonetheless, we suggest that you destroy the wrapper and mailing label of the free TaxCut CD we sent you. If you would like more information about this incident, please visit www.taxcut.com/answers, a special Website that contains additional details and an e-mail link for contacting us with your questions.

On behalf of the more than 100,000 associates of H&R Block, allow me to apologize for this unfortunate situation. Through 50 tax seasons, H&R Block has earned a reputation as a valued, trustworthy ally to our clients, and we sincerely hope that you will find the free TaxCut CD and our information-packed taxcut.com Website to be helpful tools for the 2006 tax filing season.

Sincerely,

Tom Allanson

Tom Allanson
Senior Vice President & General Manager
H&R Block Digital Tax Solutions