Testimony of

Joanne McNabb

March 21, 2007

United States Senate Committee on the Judiciary
Subcommittee on Terrorism, Technology & Homeland Security
Identity Theft: Innovative Solutions for an Evolving Problem
March 21, 2007
Testimony of Joanne McNabb, Chief California Office of Privacy Protection

Chairman Feinstein, distinguished members of the Subcommittee, thank you for the opportunity to share with you California's experience over the past several years in tackling identity theft. My name is Joanne McNabb and I am Chief of the California Office of Privacy Protection. The Office of Privacy Protection, in existence since 2001, is an education and advocacy office, with a mission of identifying consumer problems in the privacy area and facilitating the development of fair information practices. The Office's functions include assisting consumers with privacy concerns; providing information and education to consumers and to organizations; coordinating with law enforcement on identity theft and other privacy crimes; and recommending privacy practices to organizations.

From the beginning, identity theft has been the focus of many of our efforts. Historically over 60% of the calls and email we get are about identity theft. Several of the consumer information sheets available on our Web site cover aspects of identity theft and most of our Recommended Practices documents for businesses and other organizations address the responsible handling of the personal information that is the target of identity thieves. Last year we conducted or participated in 50 consumer workshops and seminars on identity theft, including 19 last June for veterans and military personnel in collaboration with the California Department of Veterans Affairs, and also 41 seminars on privacy practices for business or government.

California has been acknowledged as a national leader in privacy protection and in responding to identity theft. Since 1999, the California Legislature has enacted more than 80 privacy laws, 31 of them on identity theft. The Schwarzenegger Administration has made identity theft a priority, increasing the budget of the Office of Privacy Protection to enable us to undertake a program that has included developing a law enforcement manual on identity theft investigation and prosecution, working with universities on privacy and security awareness, training community-based organizations in identity theft victim assistance and prevention strategies, and developing privacy training materials for all State employees. This April we will hold our third annual California Identity Theft Summit. The first Summit, in 2005, focused on identifying the barriers to the investigation and prosecution of identity theft crimes. The 2006 Summit responded to some of the findings of the previous year by providing targeted training for all those who must play a role in stemming this crime - consumers, business, law enforcement officers, prosecutors, and government. This year's Summit, "Protecting Privacy Online," will include more training

sessions and also policy discussions of two issues critical to preventing identity theft: privacy and public records, and verifying identity in the online world.

California laws intended to prevent or respond to identity theft have served as models for other states and for the federal government. The 2003 FACT Act amendments to the Fair Credit Reporting Act contained several provisions based on California laws, including the truncation of credit card numbers on customer receipts, the requirement to securely destroy certain customer records, and the rights of identity theft victims to block fraudrelated items in credit files and to get copies of documents on fraudulent accounts. California laws such as those on notice of security breach, freezing credit files, and the confidentiality of Social Security numbers have inspired many states to enact similar laws and are, as we know, being considered in Congress. Because California has had these laws in effect for a few years now, I would like to share with the Subcommittee some of the observations of the California Office of Privacy Protection on the impact they seem to be having. I base these comments on what we learn in advising consumers of their rights and recommending strategies to pursue them, and in discussing information management practices with businesses and other organizations.

Social Security Number Confidentiality

I want to highlight the measures that seem to be having an impact on protecting consumers and protecting personal information. The first is a law that took effect starting in 2003, prohibiting the public posting or display of Social Security numbers. We all know that Social Security numbers have become the key to the vault for identity thieves, giving them the ability to open new credit accounts, get medical care, gain employment, even create criminal records in victims' names. The California law does not prevent organizations from using Social Security numbers for internal administrative purposes, but instead focuses on making the numbers less publicly available. It is thanks to this law, for example, that my Blue Shield card no longer has my Social Security number on it. It's also why colleges and universities in California no longer use Social Security numbers on student ill cards, thereby removing the number from many other uses as well: every professor no longer has to have every student's Social Security number on class lists. The presence of Social Security numbers on public records that end up on the Internet remains a challenging problem, involving the potentially competing values of open government and individual privacy.

Security Breach Notification

Certainly the best known California privacy law is the one requiring businesses and state agencies to notify individuals of a security breach involving their personal information. Taking effect in mid-2003, the law defines personal information narrowly, as the kind that identity thieves are after: name plus Social Security number, driver's license or state ID number, or financial account number. When the law was being considered by the California Legislature it was discussed as a way to give individuals early warning that a breach may have put them at risk of identity theft, thereby allowing them to take steps to protect themselves. Much of the debate on such laws has focused on how to defme a notification trigger based on an appropriate level of risk. The California law was conceived as risk-triggered, based on the assumption that acquisition of the information by an unauthorized person - or the reasonable belief in such acquisition - constitutes a risk.

The California Office of Privacy Protection does not enforce the breach notice law, or any other privacy law. Our role in dealing with breaches has been to assist both notice recipients and organizations that experience breaches. We are part of our state government's breach response procedure, and we also have regular conversations with other organizations experiencing breaches. We first issued our "Recommended Practices on Notice of Security Breach" when the law took effect. It contains best practice recommendations on prevention, preparation for notification, and notification. The recommendations are based on fair information practice principles and input from an advisory group of stakeholders, updated with what we've learned from breach notification incidents over the past four years.

While the original intent of the law may have been to warn individuals of potential identity theft, and the law has had that result, I think the larger impact has been on improving the information management practices of organizations. Whereas information security has generally been viewed by organizations as a cost only, the requirement to notify has revealed the cost of insecurity. A 2006 benchmark study by the Ponemon Institute found that the cost per individual notified was $187. For many organizations, that cost, which includes lost business, justifies spending on security measures to protect information.

I would like to summarize some of the lessons that have been learned - or in same cases are still being learned - from breaches.

The Office of Privacy Protection learns of breaches in several ways. Individuals whohave received notices call or e-mail us. State agencies consult with us as part of their incident response procedure. Occasionally companies call us, sometimes anonymously, when considering a possible notification. And, like everyone else, we learn about incidents through the news media. We have reviewed available information on 530 breach notifications since 2003. Our set does not contain every breach notification that has occurred, but it probably contains nearly all of those that affected enough people to attract media attention.

When we learn of a breach from a notice recipient, we generally contact the organization's privacy or compliance office. We may ask for more information or a copy of the notice, to help us in responding to consumer callers. We let the organization know of the assistance we can provide. Our Recommended Practices document contains sample notice letters, covering the different types of personal information that may be involved. We have a one-page flyer, in English and Spanish, which explains simply what steps an individual should take in response to a breach involving Social Security numbers only.

We also have Frequently Asked Questions for call centers, which cover the typical questions people ask, mostly about dealing with credit bureaus. All of these are available on our Web site.

What Types of Organizations Are Notifying of Breaches?

In our sample of 530 breach notifications, universities and government agencies account for most of the incidents, about 28% universities and 25% government. The prominence of universities may be explained by a couple of factors that create special challenges for information security on campus. The culture encourages the free flow of information as part of academic freedom and the scientific method. Campuses usually have very decentralized information technology structures,

with individual departments, schools, centers and programs operating their own systems, making system-wide policies and procedures difficult to enforce. I also think that universities might be particularly responsible about reporting and notifying of breaches.

Financial services companies experienced 14% of the breaches in our set, medical facilities 11%, retailers 5%, and schools 3%. The remaining 15% are manufacturers, data brokers, and other businesses.

What Types of Breaches Are Triggering Notification?

Nearly half (46%) of the notifications in our sample are the result oflost or stolen laptops and other devices. Hacking, which was the nature of the breach that led to the passage of the California law, accounts for 21%. Web site exposures make up 11%, insider theft 5%, improper disposal 5%, mis-sent mail 3%, mis-sent email 2%, lost shipments or mail 1%, outsider fraud 1%, and other 3%. (It is worth noting that breaches resulting from mailing errors involved paper records, arguably not "computerized data," but some companies have taken a best practices approach and notified even when the law's application is not clear.)

Social Security numbers, the most problematic type of personal information, were involved in 69% ofthe breaches. Financial account numbers, including credit card numbers, were at risk in 17%, and driver's license numbers in 4%. In 18%, either other types of personal information, such as passport numbers, were involved or we don't know what information was involved. (The numbers add to more than 100% because some incidents involved more than one type of information.)

What Have We Learned from Breaches?

One lesson - made clear by the significant share of breaches resulting from lost or stolen devices - is that organizations need to pay more attention to how they protect personal information when it's on a portable computer or other device. Some organizations are doing this by using encryption on laptops and other portable devices. California state government policy requires agencies to encrypt personal or confidential information on laptops and other portable devices. Some organizations have adopted new procedures to safeguard the information, such as cabling PCs to desks or not allowing the downloading of Social Security numbers from mainframes onto PCs or laptops. Some have tightly restricted the number of people who are permitted to carry sensitive personal information on portable devices.

Another lesson, which should not come as a surprise, is the ubiquity of Social Security numbers in databases and other records. Fully 69% of the breaches in our sample involved Social Security numbers. Individuals face the greatest risk of serious identity theft problems when their Social Security numbers fall into the wrong hands. With a name and a Social Security number, an identity thief can open new credit accounts, take out a car or mortgage loan, gain employment, claim government benefits or even create a criminal record. Recovering from these types of identity theft can take hundreds of hours and thousands of dollars, making early discovery critical.

Some organizations that have experienced breaches of Social Security numbers have revised their data retention policies. After a breach that exposed 15-year-old data, a university decided not to retain certain information, including Social Security numbers, on applicants who were not admitted.

Others have reconsidered their collection of the sensitive personal information in the first place. One blood bank which, like several others with mobile operations, had a laptop stolen, changed its policy of collecting Social Security numbers and decided to rely instead on the unique donor numbers that they were already using.

Another key lesson is the need for training on privacy and security practices. It is not just information technology or human relations staff who handle personal information. On the contrary, nearly everyone in an organization - from the janitor, to themailroomclerk.to the CEO - is likely to touch personal information on the job. The best technology and procedures can be ineffective if people do not use them properly. Training in proper information handling is a continuous process, part of building a culture that respects privacy and protects people by protecting personal information.

Security Freeze

Another California law created what is probably the strongest protection available to consumers to protect them from new-account identity theft, one of the more difficult kinds to recover from. The law giving California consumers the right to "freeze" their credit files took effect in mid-2002. It allows identity theft victims in possession of a police report to freeze their files for free and allows any individual to place a freeze for a charge of up to $10 per credit reporting agency. When a consumer has frozen her files, a credit issuer checking her credit history will receive a message saying "file frozen." This essentially prevents the issuance of new credit, because the credit issuer cannot get a credit score. The consumer receives a PIN that allows her to temporarily "lift" the freeze when she wants to apply for new credit. A freeze does not interfere with existing accounts, as existing creditors are still permitted to access a frozen credit file to perform periodic account reviews. Nor would a freeze allow someone to hide debts, since debt collectors have access to frozen files.

Since the law took effect in 2002, the California Office of Privacy Protection has received a few complaints from consumers or businesses about the functioning of a freeze. The most common complaint has been from consumers who were attempting to place a freeze and were not able to complete the process with one of the credit bureaus. In all such cases, we were able to contact the credit bureau and facilitate the process for the consumer. We have also received complaints from consumers who felt that the freeze should be available for free to all, that consumers should automatically have control of access to their credit histories.

We do not know how many Californians have frozen their credit files in the past five years. Only the credit bureaus know that. About six months after the law took effect, I understand that there were only about 150 people who had placed freezes on their files. By early 2005, soon after the ChoicePoint and other high-profile security breaches began to raise awareness of the security freeze as a protective measure, I heard that there were 4,000 California freezes. More recently, I have heard the figure quoted as 50,000. While that is a very small percentage of Californians, I

think the increase demonstrates that when people learn about the option of freezing their files, many choose to do so. It is not easy for individuals to find out about the freeze, as it is not advertised in mass media and only in recent months have the credit bureaus made information about the freeze easier to find on their Web sites and automated phone systems. The number of calls the Office of Privacy Protection received from people asking how to place a freeze increased 10-fold between July 2004 and July 2005, a growth I would attribute to the mention of the freeze in news stories on breaches.

Even with much greater awareness, I would not expect the security freeze to be used by a large percentage of consumers. Unlike the Do Not Call Registry, the freeze is not free. The $10 charge per credit bureau, which comes to a total of $60 for a married couple in our community property state, is a definite barrier. It is also more difficult to place a freeze than to sign up for the Do Not Call Registry. The freeze must be requested in writing to each of the bureaus, along with a lot of personal information. Also, people who are very active in the credit market would likely find the freeze an inconvenience. It effectively moves you from the world of instant credit at the check stand to credit in three business days. For some people, waiting three days is well worth the protection afforded by a freeze.

A definition of information privacy is the ability to control one's personal information, and a security freeze allows individuals who want it to have significant control over access to the personal information in their credit files.

Criminal Identity Theft Registry

Perhaps the most difficult form of identity theft to deal with, and fortunately one of the least common kinds, is criminal identity theft. While all identity theft is a crime in California law, the term "criminal identity theft" is used to refer to an imposter's use of someone's personal information when arrested or charged with a crime, thereby creating a false criminal record for the victim. The victim of this kind of crime may lose his driver's license, be arrested repeatedly, or be unable to get work, sometimes for years.

California's approach to helping criminal identity theft victims was the creation, in 2001, of a Criminal Identity Theft Registry maintained by the California Department of Justice. Victims listed in the Registry are given a PIN and a toll-free number, which allows the victim to exonerate himself in future situations. For example, if a victim in the Registry is stopped on the highway for a broken taillight, he can tell the officer that he is a criminal identity theft victim and that a record of that status is kept in the Registry. The victim can give the officer the phone number and his PIN, allowing the officer to verify his status - a "get-out-of-jail faster" procedure. For employment situations, the Registry staffwill send a letter to a prospective employer.

In order to become listed in the Registry, someone who has learned that he is a victim of criminal identity theft must obtain verification by a court, usually via a Judicial Finding of Factual Innocence. With that court order, the victim files an application to the Registry, along with LiveScan fingerprinting.

One challenge for victims has been in getting the court order. For the first four years of the Registry's existence, there were fewer than five registrants. Victims who contacted us found that

they needed the help of an attorney to get the court order. In 2003, the Office of Privacy Protection developed a guide to help victims of criminal identity theft get a Judicial Finding of Factual Innocence in order to get into the Registry, making it easier for them to represent themselves. Since that time, the number of victims taking advantage of the Registry has increased to 70. With continuing education of court clerks, judges, prosecutors, and law enforcement on the procedures, we believe that the Registry represents a reasonable approach to helping victims resolve the recurring problems created by this form of identity theft.

Thank you for this opportunity to testify and to share some of California's experiences in dealing with identity theft.