PRIVACY TIMES
EDITOR: EVAN HENDRICKS

Testimony of

Evan Hendricks, Editor/Publisher
Privacy Times
www.privacytimes.com

Before The House Committee On Financial Services
Subcommittee On Oversight & Investigations
Subcommittee on Consumer Credit
April 3, 2003

Madame Chairwoman, Mr. Chairman, thank you for the opportunity to testify before the Subcommittees. My name is Evan Hendricks, Editor & Publisher of Privacy Times, a Washington newsletter since 1981. For the past 23 years, I have studied, reported on and published on a wide range of privacy issues, including credit, medical, employment, Internet, communications and government records. I have authored books about privacy and the Freedom of Information Act. I have served as an expert witness in litigation, and as an expert consultant for government agencies and corporations.

The three cases you have chosen serve as excellent illustrations of several privacy and security problems that are inherent when data on millions of individuals are maintained electronically in vast databases or data networks.

In summarizing some of the problems that enabled these data leakages, you will see why it is very likely there will be more leakages, and that the overall problem of the misuse of personal data will get worse before it gets better.

- While thousands of organizations have instant access to consumers' sensitive personal data, consumers do not have the same instant access to their own data. Therefore, they generally are unable to monitor when their data are accessed, by whom, and for what purpose.

- Except in California after July 1, 2003, organizations to my knowledge are not obligated by statute to inform record subjects that their personal information has been compromised.
- The over-reliance on the Social Security number as a personal identifier can increase the vulnerability of stored personal information, and, more importantly, increase its value once it is compromised.
- There is not a strong organizational culture of data security throughout many organizations, even though they maintain or have access to the personal data of millions of Americans. This is due in part to the relative "newness" of the electronic data age, but in my opinion, more attributable to the absence of law and policy that would require organizations to take seriously the issues of data security and privacy. In the Eli Lilly case, the Federal Trade Commission has taken an important first step on this front. But the three cases we discuss today demonstrate that much, much more needs to be done.
- Unlike most other Western countries, the United States lacks an independent enforcement office for privacy. In other countries, Privacy Commissioners (sometimes called Data Protection Commissioners) can investigate and/or audit organizational practices, and provide assistance to victims of data leakages.

Clearly, a central issue is the lack of transparency to consumers of what is happening to their personal data. This is one reason why the access issue is vital.

Teledata Communications Inc (TCI)

The facts of the TCI case have already been described by previous witnesses. More details are available at www.msnbc.com/news/839678.asp. In fact, to see how the problem of credit fraud and data leakages consistently has worsened over the past five years, one only needs to do a search at msnbc.com under the name of Bob Sullivan, to see his excellent reporting on numerous cases.

TCI is a classic case of some of the problems I described above, including incredibly lax security in a credit bureau environment in which the data of 200 million Americans are at risk, and, 30,000 consumers that did not have a clue their data was misused until they received nasty calls from debt collectors or were rejected for a loan based on an inaccurate, polluted credit report.

What's stunning about TCI is that it continued for three years, allegedly perpetrated by a ring led by a 10-month employee, Philip Cummings. Security for

passwords was so lax that Cummings was able to electronically masquerade as Ford Motor Co. and other major companies, pull credit reports in their names, and sell the data to a Nigerian fraud ring. Even after Cummings left TCI and move out-of-state, he was able to continue using passwords that allowed him, from February to May 2002, to pull 6,000 reports, 100 at a time, in the name of Washington Mutual Bank. And as recently as September 2002, long after the Ford Motor incident had been well-publicized, the Cummings ring ordered 4,500 credit reports through Central Texas Energy Supply.

When a company did change its password, temporarily stumping the laptop on which Cummings had downloaded passwords and given to another ring member, the ring member, who is now cooperating with prosecutors, claimed he just called Cummings, who had an ample list of additional passwords that still worked.

The result was some 30,000 individuals having their good names used for fraud, with initial losses pegged at $2.7 million and rising fast. Those individuals all must endure the nightmare of being blindsided by identity theft, which includes the time-consuming, emotional distressful process of cleaning up a polluted credit report and restoring their good names.

This is where the issue of access is important. If individuals were "plugged into" their credit reports, they could receive alerts via e-mail of activity on their credit report. Upon seeing that, say, Texas Energy Supply, pulled their report, they would immediately know that something was wrong and take action. In fact, the three major credit bureaus (CRAs) are selling electronic access and alert services to consumers. But they generally charge in the $60-80 range, meaning it would cost a consumer around $200 to get the service from all three bureaus. In my opinion, this is an excessive charge, considering that consumers are seeking information about themselves. The Fair Credit Reporting Act caps the price CRAs can charge for credit reports, but does not address excessive charges for the relatively new monitoring services. The more we can encourage American to be plugged into their credit reports and other personal data, the better we will be able to combat the kinds of problems that we are discussing here today. Meanwhile, CRAs look at their credit monitoring and alert services as a potentially major revenue stream.

The TCI case also illustrates a shocking lack of security and vigilance on the part of the credit bureaus. For three years, the Cummings gang ran what appeared to be a readily discernible pattern of wholesale ripoffs of thousands of confidential

credit reports. Yet throughout that period it appears that none of the CRAs had a monitoring or audit system to spot this suspicious pattern of activity. It's widely known and accepted that credit card companies use software to monitor suspicious buying patterns as a means of flagging stolen credit card use. This protects both the consumer and the credit card company. But the TCI case, and my own experience, suggests that CRAs have not used similar systems to flag suspicious activities.

Finally, because this was a criminal case prosecuted by the U.S. Attorney, the U.S. Attorney attempted to notify the 30,000 victims. In my opinion, because their lax security was the cause of this problem, TCI and the CRAs, not the American taxpayer, should have borne the cost of notifying victims. Conversely, if this had not become a criminal case, would individuals have been notified? Did the CRAs notify victims after their credit reports were pulled in the highly publicized Ford Motor incident?

TriWest Break-In

The TriWest break-in remains a mystery. Although promising frequent updates on the case when it first became public, TriWest has not posted an update since February 2, 2003. Federal authorities reportedly are investigating. TriWest said computer containing incredibly sensitive medical claims history was stolen from a "secure room." To its credit, TriWest said it attempted to notify beneficiaries by sending them letters and by posting notices on the Web site. Moreover, the TriWest Web site now creates a pop-up ad that easily allows beneficiaries to place a "fraud alert" on their credit report.

TriWest illustrates how an organization that had every reason to take reasonable steps to safeguard data security, didn't. A major part of this is the organization's decision to use the SSN as a personal identifier, which increases the value of the stolen data and the risk to individuals.

As a DOD contractor, TriWest presumably must comply with the Privacy Act. One of the Act's requirements:

> "Agencies must establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm,

> embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

Moreover, TriWest was handling very sensitive medical information deserving a high level of protection. To leave it in database without encrypting it or other protective measures is, in my opinion, inexplicable, particularly in light of the Privacy Act's reference to "anticipated threats."

Also highly questionable is the reliance on the SSN as an identifier. Like many health care providers, TriWest is neither required nor prohibited from using the SSN, but insists on using it. This raises the risk level, because the SSN is one of the first pieces of information coveted by an identity thief. Meanwhile, America's fighting troops are at great risk because nearly all of their military records are tied to the SSN.

Hopefully, pending litigation will shed important light on the details of the TriWest case.

DPI Merchant Services

Another case shrouded in mystery is the theft of more than 10 million Visa, MasterCard and American Express Card numbers via DPI Merchant Services, a credit card processor. When the story first was reported, Visa and Mastercard initially declined to disclose which credit card processor had been hit. Then when DPI's role was revealed, no one would reveal which banks were affected. As you'll see from the following story from the March 3 edition of *Privacy Times*, Visa fined someone, something, but wouldn't say who or what. There was also a conscious policy by many of the entities involved not to inform cardholders that their credit card numbers had been compromised.

> The firm, also known as DPI Merchant Services, said that there still was no sign of fraudulent use of the stolen credit card numbers. According to news reports, Citizens Financial Bank of Providence, R.I., closed 8,800 accounts and sent customers new cards. PNC Bank said 16,000 debit cards were exposed. However, the vast majority of cardholders apparently have not been informed, and there has not been a complete disclosure of which issuing banks were affected. DPI's parent company, TransFirst Corp., said in one press release that it services 450 community banks.

> DPI told the *Detroit News* that consumers who are concerned should contact the issuing banks. However, N. Scott Jones, a DPI spokesman, declined to identify which banks had been hit. "That's not our call – it's the Associations'," he said referring to Visa and MasterCard. Both organizations already had notified the affected banks, he added.
>
> At 11:00 pm (EST), Friday, Feb. 28, Visa posted a statement at www.businesswire.com that, "In relation to the unauthorized intrusion that occurred in early February, Visa USA has levied substantial fines in this matter. We will take whatever further action is necessary to safeguard Visa cardholders. Visa continues to monitor the potentially compromised accounts, however, to date there has been no fraudulent activity. While we must respect the sensitive nature of this ongoing investigation, it is important for Visa cardholders to know they are fully protected by Visa's $0 liability policy, which means they pay nothing in the event of unauthorized purchases." Visa declined to release more details, stating that it never names banks whose security has been compromised or entities that it has fined.
>
> Jones downplayed the importance of further disclosure, stating that it would be difficult to misuse stolen credit card numbers and expiration dates without the cardholder's name and address, and without the three-digit security number on the back of the card. He said no other personal information about cardholders was compromised.

It's my firm belief that when there are security breaches of personal data, national policy and organizational practice should generally require that individuals be notified. In most other contexts, if authorities known that someone is a victim of a crime, the victim is notified. As with nearly all privacy issues, reasonableness standard must be applied case-by-case as to when notice is required, as well as to the means of delivering notice. But there should be no escaping the fundamental premise that people have a right to know when organizational negligence has exposed their personal data to serious risk. Unfortunately, the DPI case shows this is clearly not the standard adhered to by some leading financial institutions.

A California law that takes effect July 1, 2003 is the first to require such notification. Below is a description of the new law.

> A new law in California requires state agencies and businesses that own databases to disclose security breaches involving certain personal information. The bill comes in response to an April 2002 incident in which the records of over 200,000 state employees were accessed by a computer cracker. The California legislation exceeds federal protections, as there is no national requirement for notice to individuals when personal information is accessed without authorization.

> Senate Bill 1386, sponsored by Senator Steve Peace (D-El Cajon), creates a notice requirement where there has been an unauthorized acquisition of an individual's name along with a Social Security Number, a driver's license number, or an account number and corresponding access code. The notice requirement is also triggered when there is a reasonable belief that a security breach occurred. Notice must be given "in the most expedient time," but may be delayed where it would impede a criminal investigation.
>
> The law requires notice to be given to individuals in writing or electronically, in accordance with federal e-signature law. If the cost of notice were to exceed $250,000, or where over 500,000 people were affected by the security breach, notice could be delivered through a combination of e-mail, a conspicuous posting on the agency or company Web site, and notification of statewide media outlets. Agencies and companies could also create information security policies in advance of security breaches to address the notice requirement.
>
> The law does not apply to non-computerized files, such as personal data stored on paper. Also, only California residents enjoy the law's protections. Californians can bring civil actions for damages and injunctive relief against entities that fail to comply with the law. The law takes effect on July 1, 2003.

This also illustrates why Congress should be very, very cautious about preempting State law in the area of privacy or data security. In the past few years, at a time when these issues are increasing in importance, Congress generally has not demonstrated that it is capable of enacting adequate privacy and security protections for consumers. However, the States continue to respond more quickly with innovative legislative approaches that have helped improve organizational practice nationwide.

Finally, a sidebar issue is that the technology exists so that credit cards, instead of relying on a constant payment number that is vulnerable whenever stored, could issue one-time or "disposable" numbers that would be good for only one transaction. However, the credit industry has declined to invest in this technology.

Identity Theft Will Worsen As Well

A new report by the Tower Group confirms losses from identity theft are growing, but effectively predicts the problem will worsen. Although pegging identity theft losses at $1 billion a year and rising, a financial analyst does not foresee any major near-term changes in the practices of financial institutions.

Christine Pratt, the author of the report and a senior analyst in TowerGroup's consumer credit practice, said losses still only constitute a fraction of overall revenues, and financial institutions benefit more by offering easy and quick credit than they are hurt by losses stemming from identity theft.

"Nobody has taken a huge hit yet. And there are not a lot of easy ways to tighten up controls without putting yourself at a competitive disadvantage. Almost no one thinks the consumer is willing to give up much of anything to prevent ID theft," Pratt said.

Conclusions & Recommendations

These are complex and serious issues. Unfortunately they promise to worsen for many of the reasons I've described above.

Here are some of my preliminary recommendations:

- **Expand & Improve Consumer Access to Their Own Financial Data**. The FCRA already gives consumers the right to see their credit report and caps how much CRAs can charge. This approach needs to be upgraded to the electronic age and expanded to the entire realm of financial data, especially since large financial institutions are maintaining their profiles on customers, perhaps beyond the reach of the FCRA. In the meantime, Congress could pass a Resolution or Sense of the Congress that as a matter of principle and fundamental fairness, Americans should have a right to see and correct information about themselves.

- **Extend to financial institutions the following security standard** that federal agencies must abide by under the Privacy Act: "Agencies must establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." Again, this goal could be advanced in the interim through a resolution or Sense of the Congress.

- **Impose A General Duty To Notify Consumers After Data Leakages.** The new California law provides a model starting point.

- **Curtail The Use of SSNs as a personal identifier**. Rep. Clay Shaw and others have introduced legislative proposals to this effect.

- **Create An Independent Privacy Office** Most people don't realize that Sen. Sam Ervin originally proposed such an office along with the Privacy Act. Now, every advanced nation has one except the United States.

- **Create A Private Right Action So People Can Enforce Their Own Rights**. Privacy affects virtually all 200 million adult Americans. In this electronic age, they must have rights, and those rights must be enforceable. You will never be able to build a bureaucracy big enough to adequately enforce Americans' right to privacy, nor should you want to. Thus, the private right of action is essential.

I'd be happy to answer any questions.