STATEMENT OF

STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION
WASHINGTON, D.C.

BEFORE THE

House Financial Services Subcommittees
on
Oversight and Investigations
and
Financial Institutions and Consumer Credit

ON

Fighting Fraud: Improving Information Security

April 3, 2003

Chairwoman Kelly, Chairman Bachus, and members of the committees, thank you for this opportunity to appear at this joint hearing of your committees. For the record, I am Stuart Pratt, President and CEO of the Consumer Data Industry Association.

CDIA, as we are commonly known, is an international trade association representing approximately 500 consumer information companies that provide credit and mortgage reporting services, fraud prevention and risk management technologies, tenant and employment screening services, check fraud prevention and verification products, and collection services, as well.

We commend you for holding this hearing on the implications of breaches in information security at TCI Communications, DPI Merchants Services and TRIWest Healthcare Alliance. Specifically, your committees have asked us to comment on each of these breaches of security from the perspective of our members who operate as nationwide consumer credit reporting agencies.[1] In each case where we can comment, we have provided some background on the incident for purposes of context.

TCI Communications:

Background: On November 25, 2002, federal authorities announced they had arrested a man, 33-year-old Phillip Cummings, who had stolen passwords and codes, which gave him access to credit reporting systems. Cummings was a help-desk employee at Teledata Communications, Inc. (TCI), a Long Island, N.Y.-based company providing lenders with software, terminals and

support related to accessing consumer reports for permissible purposes under the FCRA. Cummings appeared in the U.S. District Court in Manhattan on charges that he and another man downloaded the personal information of 30,000 individuals over a period of time and accessed reports from consumer reporting agencies using access codes assigned to several lenders including Ford Motor Credit, Co.

Nationwide Consumer Credit Reporting Agencies: Our members have no direct relationship, contractual or otherwise, with TCI, since it provides its services directly to lenders. Our members learned of the possibility that access codes for their systems had been compromised via contact with their customer, Ford Motor Credit and also through subsequent law enforcement contacts. Those of our members with a compromised access code recognized the potential seriousness of the situation and worked collaboratively with Ford Motor Credit, law enforcement and with affected consumers as the investigation unfolded.

Upon learning of the problem our members quickly assessed what steps were necessary to mitigate the possible risks for consumers whose files may have been accessed for fraudulent purposes. In polling our members with regard to the types of actions taken on behalf of consumers we identified the following steps were commonly taken:

- The consumers' files were, in some cases, temporarily blocked to prevent additional use pending a notification being sent. Note that proactively blocking access to a file is very draconian and would, for example, stop a consumer who was in the middle of a home mortgage approval process from successfully purchasing a new home.

[1] CDIA's members include all of the nationwide consumer credit reporting agencies: Equifax, Experian and TransUnion.

- Notification letters were sent to consumers, in some cases by Ford and in some cases by CDIA members, notifying them of the incident. Dedicated toll-free numbers were brought online by our members and these were included in the notifications sent to affected consumers and they were shared with Ford.
- Once consumers contacted CDIA members, they were offered a range of services not require by law: 1. free file disclosures; 2. they were opted out of prescreened offers of credit; 3 a fraud alert was added to the file; 4. free access to additional file disclosures during the next 90 days following contact; 5. they were also offered free access to file monitoring services which can notify a consumer of changes in addresses, the inclusion of new accounts or negative information in their files, and also notification of who is accessing their files.

Beyond the priority of assisting consumers whose files may have been compromised, our members also took proactive steps to ensure that the scope of the fraud was contained. They conducted analyses of other passwords and sub-codes related to customers of TCI and other similar third-party vendors. They deployed pattern-recognition tools and initiated reviews to ensure that they could identify other anomalies related to access code usage.

The degree of law enforcement contact varied depending on the CDIA member. Our members did, however, cooperate with law enforcement in setting up sting operations and conducting other internal audits, which helped in these investigations.

DPI Merchant Services:

Our members reported to us that to date they have not been contacted with regard to this incident and therefore we do not have any information to add to the record.

TriWest Healthcare Alliance:

Background: The situation with TriWest was very different from that of TCI. News accounts report that individuals were able to steal hard drives from TriWest's data center. These hard drives contained information on approximately 500,000 military families.

Nationwide Consumer Credit Reporting Agencies: Since TriWest is not a customer of any of our members, there was understandably less immediate coordination. TriWest, as we understand it, did take quick action to notify all of the families and apparently this notice did recommend that affected families should take a number of steps to mitigate risks, including contacting nationwide consumer credit reporting agencies.

Many families followed the instructions in the TriWest letter and did contact our members. Consumers who contacted our members indicated that they were concerned that they were victims of fraud and thus they received free file disclosures.[2] TriWest did remain proactive beyond the letter they sent and contacted CDIA's members to request their coordination of some additional steps for the affected families and our members did voluntarily work with TriWest to

[2] Since CDIA's announcement in March of 2000, our members have executed a three-step process for any consumer who indicates that he/she is a victim of identity theft. These steps include the automatic inclusion of a fraud alert in the file, opting the file out of any non-initiated offers of credit and ensuring that the file disclosure is in the mail within three-business days. Included at the end of this testimony is a complete summary of all of the CDIA's efforts to assist victims.

provide them with the means to forward additional families to CDIA's members where the family contacted TriWest directly.

Summary:

As we can see by the three examples above, security breaches can occur in a variety of ways including hacking, but also through the common criminal behavior of an employee. We believe there are some important points to consider stemming from our members' experiences with these incidents and with others that were not the subject of this hearing.

- Where the criminal behavior of an employee involves accessing information from a consumer reporting agency, through the illegitimate use of legitimate access codes or otherwise, the Fair Credit Reporting Act (15 U.S.C. Sec. 1681q) stipulates that this is an offense which can result in fines and imprisonment under Title 18 of the U.S. Code. These actions are also a violation of the "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984" (18 U.S. C. Sec. 1030).[3] We applaud the fact that law enforcement aggressively investigated the TCI case and caught the perpetrator. Increased resources are necessary for law enforcement to continue to build on this effort and we should evaluate the value of increasing the penalties relative to these crimes.
- We must begin to learn to measure the risks relative to various breaches of information. Not all security breaches necessarily result in large-scale identity theft. In 2002, the state of California reported that they believed that more than 200,000 names of state employees had been stolen. Like the TriWest situation, state employees were instructed, unbeknownst to our members, to contact them. Our members voluntarily cooperated with the state in coordinating efforts, and one of our members reports that not a single

dispute has been submitted relative to any of the file disclosures sent to CA state employees.

- Our members voluntary efforts to assist other companies which have experienced a security breach is taking a toll on our members' ability to service other consumers, including other victims of identity theft. One member reports that the costs of servicing the families of TriWest reached $1.5 million. We are not questioning the necessity of ensuring that military families received every level of support necessary during this time in our nation's history. But in the long run, our members cannot be placed in the ongoing position of having to bear a significant financial burden for every breach of information where the cause of the breach was not related to our members' data security practices[4] and where it did not involve our members' data.
- Coordinating assistance for consumers is important and as you can see in the attached summary of our efforts to assist verified victims of identity theft, we have taken and will continue to take action to ensure that victims of crimes are effectively served.

We appreciate this opportunity to testify and share our views.

[3] This amendment was enacted via PL 98-473 – October 12, 1984

[4] Note that the CDIA's members which operate as nationwide consumer credit reporting agencies are now governed by new security protocols which are established via the enactment of the Gramm-Leach-Bliley Act and the subsequent GLB Safeguards Rules. Included with this testimony is a summary of those rules.