Before the United States House of Representatives

Committee on Financial Services

Subcommittee on Financial Institutions and Consumer Credit

Testimony of Lee Lundy
Vice President, Consumer Services
Experian

www.experian.com

Lee Lundy
Experian
701 Experian Parkway
Allen, TX 75013

INTRODUCTION 3

WHAT WORKS IN THE FIGHT AGAINST FRAUD 5

HELPING BUSINESSES STOP FRAUD 5
THE CONSUMER'S ROLE 7
THE IMPORTANCE OF LAW ENFORCEMENT 9

CONSUMER VICTIM ASSISTANCE 10

WHAT DOES NOT WORK IN THE FIGHT AGAINST FRAUD 12

RESTRICTING DATA FLOWS 12
FREE CREDIT REPORTS 14

CONCLUSION 16

APPENDIX A: EXPERIAN'S BUSINESS FRAUD SERVICES 18

APPENDIX B: EXPERIAN CASE STUDIES 21

LEADING CREDIT CARD ISSUER REDUCES FRAUD LOSSES THROUGH IMPLEMENTATION OF EXPERIAN'S AUTHENTICATION SERVICES 21
NATIONAL TELECOMMUNICATIONS PROVIDER BENEFITS FROM EXPERIAN FRAUD SOLUTIONS 21

APPENDIX C: CDIA CONSUMER FRAUD VICTIM ASSISTANCE INITIATIVES 23

APPENDIX D: EXPERIAN'S CONSUMER FRAUD VICTIM ASSISTANCE PROCESS 25

STEP 1: CONSUMER CONTACTS EXPERIAN'S CONSUMER ASSISTANCE CENTER 25
STEP 2: CONSUMER RECEIVES REPORT 25
STEP 3: INVESTIGATION BEGINS 26
STEP 4: FRAUDULENT DATA IS REMOVED 27

Introduction

For more than 50 years Experian has been a leader in the information industry. In fact, the company's roots date back more than 100 years to the pioneers of credit reporting. Its success is based on sound information values that guide the development of practices and policies that protect consumer privacy, ensure security and provide benefit to consumers and our business clients alike.

Responsible information use today affords consumers greater choice, convenience, and lower prices than ever before. In past decades, our economy was local. Businesses were located where consumers lived. Product and service choices were limited to what was available in a consumer's neighborhood, the local main street, or perhaps a nearby city. Consumers learned about businesses by walking down the street, or reading ads in the local newspaper.

Today we have a national credit reporting system. Businesses in Los Angeles and New York compete daily to sell financial products and services to consumers in Kansas. Where once there was only a single provider of a product or service, or maybe two or three to choose from, there now are hundreds. Because of responsible information sharing, those businesses can reach consumers who are most likely to need their products and services. That greatly increases consumer choice and promotes competition, which drives down prices.[1]

Today, consumers expect instant access to credit, affordable, high quality goods and convenient customer service 24-hours a day, seven days a week. Businesses in our "always-open" economy struggle to meet their customers' expectations of value,

affordability and convenience while at the same time protecting consumers and themselves from fraud and identity theft.

Every day Experian is on the front lines of the war against fraud because of its role as a leading information solutions provider, and because of its role as a consumer reporting agency. We are driven to provide the best fraud tools available so businesses can prevent victimization from occurring, and we strive to help consumers recover from fraud and identity theft as quickly as possible.

Economic crime cost U.S. businesses more than $1 trillion dollars in the year 2000.[2] According to a study by Meridien (July 2002), institutions absorb approximately $18,000 per identity theft including loss of goods, revenue and costs associated with customer service and victim assistance.

More than 1 million consumers contact Experian's National Consumer Assistance Center each month to request a credit report, get help with questions about their reports, or for fraud assistance. Every interaction is important, but none more so than helping consumers victimized by fraud or identity theft.

Experian worked with the U.S. General Accounting Office during 2001-2002 in researching fraud and identity theft. We found that approximately 30,000 consumers add fraud victim statements to their credit histories each year.[3] The number includes individuals who are not victims, but who are concerned about fraud and identity theft,

---

[1] Fair Credit Reporting Act: Access, Efficiency & Opportunity; the Economic Importance of Fair Credit Reauthorization. Information Policy Institute; June 2003
[2] From studies by the American Bankers Association (ABA), BAI, Cellular Telephone and Internet Association (CTIA), Coalition Against Insurance Fraud (CAIF) and UN.
[3] Identity Theft: Prevalence and Cost Appear to be Growing, GAO-02-363, March 2002

and not all victims add a statement to their credit history. Therefore, this figure does not represent a precise number of victims.

Clearly, fraud and identity theft are serious crimes that affect consumers and businesses across all industries, among them financial services, health care, insurance, cellular services, utilities, retail, technology and online commerce.

Our experience in business fraud prevention has shown us what works and what does not work in the battle against fraud and identity theft. When fraud does occur, we are in the forefront of consumer fraud victim assistance.

What works in the fight against fraud

The most effective strategy in the war against fraud is responsibly using the free flow of information to enable cooperation among the national credit reporting agencies, businesses, law enforcement agencies and consumers to effectively prevent and fight the crime. Fraud and identity theft can be curtailed only if we all work together effectively and efficiently.

Helping businesses stop fraud

Businesses must work together, as well as with Experian and other information service providers, to identify fraudulent activity and prevent proliferation of the crime at the point of application.

Today, there are highly effective tools to fight fraud and identity theft. Information services providers are in a position to help develop and implement those tools because of the data they collect, maintain and manage. Experian has invested heavily in developing the industry's leading fraud prevention and detection tools. Our

expertise with traditional data sources and ability to develop new tools based on responsible information sharing have enabled us to create some of the industry's most effective fraud detection and prevention systems. Our goal is to help businesses prevent fraud at its origin. Targeting prevention reduces business' fraud losses, protects consumers from fraud and eliminates the challenges of victim assistance.

Among the most effective ways to fight fraud and identity theft is by sharing information about known fraudulent activity as part of a cooperative database, such as Experian's National Fraud Database. The National Fraud Database is comprised of known, verified fraudulent activity provided by businesses from across industries. The database alerts users to information associated with verified fraudulent activity enabling them to stop fraud before it starts.

Experian's Detect service, another cooperative database, takes fraud prevention to the next level by comparing application information for anomalies that may indicate fraud.

The online environment poses its own unique set of challenges to fraud prevention. The most difficult issue is authenticating the identity of a customer whom a business will never meet face-to-face. Our Authentication Solutions are designed to prevent online fraud by requiring customers to pass an "identity quiz" which includes questions from a number of sources. Customers are asked questions to which only they are likely to have the answers. The questions are drawn from credit history information and other sources. The various data sources are essential because they enable businesses to ask questions that have answers that would not be found in a stolen wallet, which

commonly includes identification elements such as name, address or even Social Security number.

With the National Fraud Database, Detect and Experian's Authentication Solutions, lenders are equipped with some of the most effective fraud and identity theft prevention tools available today. *(Appendix A: Experian's Business Fraud Services, p. 18)*

For example, one national credit card issuer realized a 13 percent decrease in application fraud losses and annual savings of $18 million by implementing only one of Experian's most basic identity authentication tools. Businesses utilizing Experian's fraud prevention tools often report decreases in fraud losses of 50 percent or more within the first year of implementation. Similarly, a national telecommunications provider experienced a 55 percent decrease in fraud losses per handset and decreased the time it took to confirm fraud records by more than two-thirds. *(Appendix B: Experian cases studies, p. 21)*

The consumer's role

Consumers, too, play an important part in protecting themselves from identity theft. Much of what they can do is simple. Experian, through its consumer education materials, consumer advocates and government agencies recommend that consumers:

- Sign their credit cards as soon as they receive them.
- Store credit cards and other identification documents in a safe place.
- Do not carry identifying information in a purse or wallet that the consumer does not need, such as a Social Security card.

- Do not carry in a purse or wallet more credit cards than necessary. For instance, carry only the one or two cards the consumer uses most.
- Do not provide sensitive information over the telephone unless the consumer initiated the call, trusts the business or individual with which they are speaking and understands why the information is needed.
- Do not write driver's license or Social Security numbers on postcards or the outside of envelopes.
- Do not leave receipts at the sales counter, ATM machine or fuel pump.
- Shred all documents containing sensitive identifying or financial information before discarding them.

Online shopping offers great convenience and opportunity, but similar common sense actions apply:

- Do not provide sensitive identifying or financial information in response to an e-mail message unless the consumer initiated the communication.
- Conduct transactions only through secure connections.
- Only shop online with reputable, known businesses with posted privacy policies and clear merchandise satisfaction and return policies.
- Subscribe to a monitoring service that alerts the consumers when their credit history has been accessed.

The importance of law enforcement

While sophisticated fraud prevention tools and effective victim assistance are critical, strict enforcement of anti-fraud laws is equally important. Experian and our credit reporting counterparts worked with the Federal Trade Commission to establish a uniform fraud affidavit to make reporting fraud easier. We block any account reported as fraudulent when a valid police report is provided by the consumer, effectively suppressing the fraudulent information immediately from the credit history. Yet, it remains difficult for consumers in many instances to obtain a police report because of jurisdictional issues.

Conversely, credit repair clinics and others who hope to alter or delete accurate, negative information from consumer reports have falsified police reports provided to Experian and the other consumer reporting agencies.

Improved multi-jurisdictional law enforcement efforts are essential to solving the fraud problem. Consumers often find themselves being sent from precinct to precinct and agency to agency. Some agencies are unwilling or unable to issue a report, and all of them lack sufficient resources to conduct a thorough investigation. Resolving jurisdictional conflicts and sufficiently funding enforcement are essential actions for winning the battle against fraud.

Until recently, law enforcement kept few meaningful statistics on fraud and identity theft. Such statistics are important to better understanding the extent of identity fraud in its various forms. There are many types of fraud including account takeover, "friendly" fraud in which the victim knows or has a relationship with the perpetrator, and

true name fraud. Some statistics suggest that up to 40 percent of all identity fraud is perpetrated by a family member or by someone the victim knows.

Better defining the prevalence of the various fraud types and the ways in which they are perpetrated will enable more effective law enforcement and development of meaningful protective measures by the private sector.

Improved relationships between victims and law enforcement agencies are also important. Too often, consumers are not seen as victims by law enforcement. Rather, businesses are viewed as the victim because they usually suffer greater monetary loss. Maintaining a closer relationship with consumers, assuring them that an investigation is taking place, notifying them of progress, and updating them on prosecution are important steps in victim assistance.

Stronger penalties against those who perpetrate financial fraud are needed. Current penalties are inconsistent and range from probation to imprisonment. Penalties must have teeth to be effective, and they need to be consistent from jurisdiction to jurisdiction.

Consumer victim assistance

Unfortunately, identity theft has already occurred by the time a fraudulent account becomes part of a credit report. In some cases, a full understanding of the breadth of the crime may not be known for some time. Identity theft, unlike other crimes of theft, often occurs over a period of weeks or perhaps months. It is frequently a longitudinal crime – different than a burglary. Therefore, when you hear reports in the media that it took a consumer months to unravel financial records affected by identity theft, it is often the case that elements of the criminal activity did not reveal themselves until weeks or

months later. When a victim identifies a fraudulent entry on a consumer report, we work promptly with the provider of the information and the consumer to resolve the issue. At that point, our role as a consumer reporting agency becomes one of victim assistance.

Experian and our counterparts work together continuously to develop victim assistance processes that are as uniform and efficient as possible. In 2000 we launched, in conjunction with the Consumer Data Industry Association (CDIA), a series of voluntary initiatives designed to improve consumer fraud assistance. These include standardized, industry accepted, computer-readable security alerts and, victim-assistance best practices. Among the identified best practices are notices to creditors, automated systems enabling 24-hour, seven-day-a-week addition of fraud security alerts, and free credit report monitoring. *(Appendix C: CDIA Consumer Fraud Victim Assistance Initiatives, p. 23)*

Most recently, we announced a one-call fraud alert program. Today, victims need only contact one credit reporting agency to have a security alert added to all three credit histories. Consumers no longer need to call each of the three national credit reporting agencies to add fraud alerts, have a complimentary report mailed and activate the CDIA fraud initiatives. By simply notifying one of the agencies they will begin the fraud recovery process at all three, making the recovery process easier and faster.

Consumer reporting agencies are all committed to ongoing improvement of our victim assistance services *(Appendix D: Experian's Consumer Fraud Victim Assistance Process, p. 25)*, but the battle against fraud and identity theft can only be won by preventing the crime at its source.

What does not work in the fight against fraud

Our experience has also shown that many approaches perceived to increase fraud prevention and aid recovery actually result in neither. Those approaches include restricting data flows and providing free credit reports. At face value, both seem to promise greater fraud protection. In reality, they do little to protect consumers and in fact may make the fraud problem worse.

Restricting data flows

Access to and responsible use of information from a broad spectrum of sources is essential to our fight against fraud and identity theft. The success of sophisticated fraud detection and prevention tools depends on continued access to key identifying information and responsible information sharing.

This is especially true when considering the growing numbers of application fraud and transactional fraud, which occur most often when a credit card cannot be presented to the business, for example in tele-commerce and Internet transactions.

Solutions to these types of fraud demand tools that can utilize complete, accurate and current information from multiple sources. Eroding the ability of businesses to obtain and share information responsibly and to compare that information with consumer-supplied information will increase the risk of fraud and identity theft, reduce competition and drive up prices.[4]

[4] Fair Credit Reporting Act: Access, Efficiency & Opportunity; the Economic Importance of Fair Credit Reauthorization. Information Policy Institute; June 2003

Closing public records or limiting the information in them, deleting, truncating or redacting Social Security numbers, limiting or eliminating business-to-business uses of Social Security numbers and other information restrictions exacerbate the fraud problem.

Experian and other responsible fraud solution providers are dependent on public records as a source of accurate identifying information essential to victim assistance and fraud prevention services. Legislative restrictions on the use of information do little to deter serious identity thieves. They will simply obtain the information through other means, illegally if necessary. The effectiveness of victim assistance and fraud prevention tools, however, is seriously degraded because critical data elements are lost.

Social Security numbers (SSNs) often are described as the key to committing fraud. As a result of that characterization, deletion or redaction of SSNs from public records and closure of public records that include SSNs is threatening the availability of public records for fraud prevention. While it may seem counterintuitive, such actions actually result in greater exposure to fraud.

An alarming example now before Congress is a proposal sponsored by the U.S. Judicial Conference that would truncate SSNs in bankruptcy records, even when provided to consumer reporting agencies. Congress should reject or modify the proposal or the accuracy and completeness of bankruptcy information contained in consumer reports will be diminished.

Truncation of SSNs is as damaging to fraud prevention as complete deletion or redaction. The ability to match only a portion of an SSN is not sufficient for fraud detection or prevention. Variations or anomalies in the unseen portion of the number could indicate fraud that would go undetected. Equally important, truncated account

numbers are not adequate for differentiating between individuals, particularly if they share a common name, such as John Smith or Jim Johnson, for example, or a close relationship, such as twins, whose SSNs may vary by only a single digit. Also consider that 4.5 million consumers have one of two surnames (Smith or Johnson) and that 3 million people change their last name each year and SSN truncation becomes a very significant impediment to successful fraud detection and prevention. The result of truncation is the same as complete deletion of the number: increased fraud risk, not increased protection. Therefore, Experian respectfully requests that Congress review and comment on the U.S. Judicial Conference proposal.

Free Credit reports

Free credit reports also have been touted as a solution to the fraud problem. A free credit report actually has little impact on fraud prevention. As mentioned previously, by the time fraudulent accounts appear on a credit history the crime has already been committed.

Current FCRA provisions already provide free reports for virtually all consumers who need a credit report. For instance, federal law already requires credit reporting agencies to provide a free report to consumers whenever an adverse action is taken, whenever a consumer believes he or she may be a victim of fraud, and in situations where the consumer is either unemployed or receiving welfare assistance.

Credit reporting agencies also are mandated to provide toll-free consumer assistance after providing a free report. Costs of mailing a report and maintaining a call center, including staff and infrastructure such as telephone service, must be evaluated when considering the true cost of a "free" credit report. Furthermore, the $9 fee allowed

by the FCRA enables credit reporting agencies to recoup only a portion of the expense associated with providing the report and subsequent consumer assistance.

Those who promote free reports do so in order to enable consumer "access" to their reports, but this is a "red herring." Consumer reporting agencies readily grant access 24-hours-a-day, 7-days-a-week, every day of the year. There is no evidence that the $9 fee applicable when a free report is not otherwise mandated is a barrier to access.

Today, a serious but often overlooked factor associated with proposals to extend free reports to all without condition are the costs involved with providing trained consumer assistance professionals who can answer consumers' questions. While the cost of the actual report is one expense, staffing to meet this exposure is something we do not have the physical space or financial capacity to undertake.

Another challenge to us is meeting the exposure created by businesses and government agencies outside the credit allocation stream that direct hundreds of thousands of consumers to obtain a free report under the claim of fraud, when in fact no fraud or identity theft occurs. For example, in a recent case during just a few days, the credit reporting agencies were inundated with thousands of requests for free reports when computer equipment containing information about more than 500,000 consumers was stolen from Tri-West, a Department of Defense subcontractor in Arizona. Yet, not a single instance of fraud or identity theft associated with the theft has been reported.

Likewise, the concept of notifying consumers of computer security breaches will do little to protect them from fraud, but will likely result in unnecessary concern and fear.

Literally thousands of attempts to hack into computer systems are made across the country every day. Sophisticated firewall and security systems thwart virtually all of

those attempts. When an attempt does succeed, it does not always result in the information accessed being used for fraud purposes. Last year, for example, nearly 200,000 consumers were directed to ask for a free report when a State of California database of employee records was compromised.

Just as in the Tri-West case, there has been no evidence that fraud or identity theft has been committed. However, all of the employees were instructed to get a free report under the claim of fraud.

Still, under current notice proposals virtually every successful hacking incident would result in notices and free reports being sent to hundreds-of-thousands of consumers who are unlikely to become victims of identity theft.

Such instances impose tremendous costs on credit reporting agencies and harm consumers who have urgent needs by flooding our consumer assistance centers – at our expense, not at the cost of Tri-West, the State of California or other businesses responsible for security breaches. Adding a requirement to provide free reports and the associated consumer assistance responsibilities to 200 million consumers would simply be unmanageable in terms of our ability to control costs and meet currently required service levels.

Conclusion

As identity thieves become more "creative" in their attempts to commit fraud, the ability of organizations fighting fraud to access and utilize information from a range of sources becomes increasingly important.

We are allies in the war against fraud. Our enemy is the same. Unfortunately, currently popular legislative and regulatory proposals -- the legal bombs in the battle --

are being dropped on the wrong targets. By eliminating the ability of information solutions providers, like Experian, to access and utilize data from a broad range of sources, you inadvertently destroy the most powerful arsenal we have against fraud.

The key to Experian's fraud services, all fraud prevention tools for that matter, is responsible information use. The most effective fraud tools rely on many data sources to ensure accurate identification. Access to that data, and the ability to utilize it responsibly must be protected.

Appendix A: Experian's Business Fraud Services

Experian has long provided tools to identify increased fraud risk and has during the past several years introduced a number of groundbreaking services to help businesses prevent fraud and reduce fraud losses. The most powerful weapon against fraud is responsible data use.

Users of credit reports have long had the following services available:

Consumer fraud alerts: For many years, consumers have been able to add to their credit histories security alerts, indicating they may be a fraud or identity theft victim and victim statements stating that they are victims. A security alert on an Experian credit history remains for 90 days and warns lenders that the consumer may be a victim, enabling the lender to take additional precautions. The temporary security alert is added automatically when a consumer selects the fraud option on Experian's automated telephone system or Internet site. A credit report will be provided automatically, either by mail or online, which will include contact information to speak with a trained fraud representative. Consumers who know or believe they are fraud victims can request that a 7-year victim statement be added to their credit history after receiving their credit report. A victim statement indicates the consumer is a victim and asks that the lender contact them at a telephone number provided by the consumer before granting credit in their name.

FACs+: An automated system that identifies information in a credit history that indicates increased fraud risk. Indicators include addresses recorded as belonging to a business, Social Security numbers reported as belonging to a deceased individual, Social Security numbers that have not been issued, or variations in names or addresses, among

others. The FACs+ statements do not indicate fraud is occurring, but rather that information in the credit history suggests higher fraud risk.

Fraud Shield[SM]: A fraud prevention tool that goes beyond the simple single-element identifiers of FACs+ and compares data throughout the credit history to more accurately define fraud indicators. Like FACs+, Fraud Shield[SM] does not indicate fraud is or has occurred, but instead indicates to lenders that information suggests a higher fraud risk. Fraud Shield[SM] enables lenders to take additional precautions to protect consumers and themselves from fraud when considering applications.

More recently, Experian launched new fraud detection and prevention tools that utilize data beyond that in a credit report and that aid businesses in both online and offline environments.

Authentication Services: Experian's Authentication Services protect business and consumers from fraud and identity theft in the online environment. Authentication Services not only review common "in-wallet" identifying information such as name, address, date of birth and Social Security number and driver's license number. The system also requires "out of wallet" information that only the consumer would know, such as what lender holds a mortgage, balances (in a range) on credit cards, or what type of car an individual owns. Data is drawn from a variety of sources including credit histories and property records.

National Fraud Database[SM]: Experian stepped to the forefront of fraud and identity theft detection and prevention with the introduction of the National Fraud Database[SM]. It is the first industry-wide database of known and verified records of

fraudulent activities identified by National Fraud Database subscribers and consumer fraud victims.

National Fraud Database reports are used during the application process for credit or banking services, account reviews and other activities allowed under the FCRA. The information in a report helps lenders identify not only when fraud is potentially occurring, but also when they are working with a victim, enabling them to take appropriate actions for each circumstance.

Detect[SM]: A further advance in fraud detection and prevention, Detect[SM] provides on an online system that notifies credit grantors of potentially fraudulent or high-risk applications that would likely have been accepted through normal automated underwriting procedures. The system relies on incoming application information, past application data and credit bureau information to trigger fraud warnings. Detect[SM] identifies inconsistencies and anomalies in application information that indicate identity theft or other types of fraud.

Authoricheck[SM]: A class-leading business fraud prevention tool, Authoricheck[SM] provides an efficient, automated method for managing risk and eliminating fraud in a business-to-business environment by authenticating information in business credit reports and checking against historical application data for fraud indicators.

Appendix B: Experian Case Studies

Leading credit card issuer reduces fraud losses through implementation of Experian's Authentication Services

A major national credit card issuer with approximately 45 million accounts, growing by about 10,000 accounts a day, faced a significant application fraud challenge. The company needed to reduce application fraud losses, improve business efficiency and maintain customer service satisfaction, and it needed to do so cost-effectively. The company turned to Experian for help.

It chose to implement Level One of Experian's Authentication Services. The first of three increasingly sophisticated Authentication Services levels, Level One is powered by a database of more than 215 million consumers and 25 million businesses.

The credit card issuer, consulting with Experian, conducted a six-month test on 800,000 new applications before implementing the fraud prevention tool across its business. Utilizing the Authentication Services Level One has resulted in a 13 percent decrease in application fraud losses and an overall annual savings of $18 million.

The company is now exploring application of the service for risk assessment in prescreen credit offers and has taken its fraud prevention efforts a step further by becoming a subscriber to Experian's National Fraud Database.

National telecommunications provider benefits from Experian fraud solutions

The wireless communications industry faces exorbitant fraud losses – an estimated $275 million in 2003 alone. A national wireless telecommunications provider, challenged by fraud losses and high customer acquisition costs, turned to Experian for

help. The company recognized the need to protect both consumers and the company from identity theft and needed an aggressive fraud prevention strategy that was both highly effective and easy to implement.

After carefully reviewing other options, the telecommunications provider chose to share its fraud records with other organizations as a member of Experian's National Fraud Database (NFD). The NFD is a database of known, confirmed fraud information shared by members from multiple industries including online retail, bank card issuers, credit card providers, automotive lenders and telecommunications companies. The NFD alerts participants to confirmed fraud data as they process applications.

The wireless telecommunications provider tested the database for almost a year before proceeding with national implementation on all of its new accounts. The company reduced its fraud losses per handset by 55 percent and decreased the time it took to confirm fraud records by 66 percent.

In addition to cost savings, the company is able to detect attempted fraud much faster, protecting consumers from identity theft. Members of the NFD are able to stop identity theft at the point of application, notify the intended victim before fraud happens and prevent any harm associated with the crime.

Statistical analysis of shared fraud information in the telecommunications, credit card and online retail industries has proven that identity thieves cross industry lines when committing fraud. Equally important, identity thieves demonstrate predictable patterns of fraudulent behavior. As a result, all of the participants in the NFD benefit from responsibly sharing of verified fraud data from their respective industries.

Appendix C: CDIA Consumer Fraud Victim Assistance Initiatives

In 2000, the Consumer Data Industry Association (CDIA), then the Associated Credit Bureaus (ACB), announced a series of initiatives to more efficiently and effectively assist consumers victimized by fraud or identity theft. Those initiatives included:

- Improving the effectiveness of credit report security alerts through computer-readable codes. The codes notify creditors of the existence of potential fraud and help them avoid opening additional fraudulent accounts even when an automated review system is used. CDIA and its members strongly advocate use of the coded security alert system among creditors and other credit report users.
- Implementing new victim-assistance best practices to provide more uniform processes for victims working with personnel from multiple fraud units.
- Sending notices to creditors and other credit report users when a consumer doesn't recognize a recent creditor inquiry on their report and fraud is suspected.
- Implementing automated telephone systems that when reached by a consumer automatically add a security alert to a victim's credit history, opt them out of prescreened credit offers, and mail a copy of their credit report within three business days.
- Monitoring a victim's credit history for three months after correcting and eliminating fraudulent information. The agencies notify the victim of any

unusual patterns or activity during that time and provide fraud unit contact information.

- Launching new consumer education programs to help people understand how to prevent identity theft and what steps to take if they are victimized.

Most recently, Experian and the other national credit reporting agencies, working with the Federal Trade Commission, launched a new service eliminating the need for consumers to make multiple calls to have security alerts added to their credit history. Consumers now must call only contact one of the national agencies, in Experian's case, either by telephone or through its Web site. Their request will be forwarded to the other two and security alerts will be added automatically to all three of the person's credit histories.

Appendix D: Experian's Consumer Fraud Victim Assistance Process

STEP 1: Consumer contacts Experian's consumer assistance center

- Consumers can call Experian's automated voice attendant or logon to its Web site 24 hours a day, seven days each week, 365 days a year.
- A 90-day "Security Alert" is immediately added to the consumer's credit file. This alerts creditors to verify the identity of the consumer before extending credit.
- The consumer is put on the "opt-out" list for prescreened credit solicitations.
- The consumer is sent a complimentary consumer report within three business days.
- Experian's consumer education department developed and maintains a series of one-page educational fact sheets to help consumers better understand how credit reporting works and how to prevent ID theft or recover from victimization. In addition, Experian's Internet credit fraud center at www.experian.com provides a wealth of information to consumers and fraud victims.

STEP 2: Consumer receives report

- The consumer reviews his or her consumer disclosure for fraudulent data and calls a special telephone number listed on the credit report to speak with an Experian customer service representative specially trained in fraud victim assistance, or requests an investigation of any inaccurate information online.

- A seven-year "Victim Statement" can be added to the consumer's credit file if the report contains evidence of fraud. This asks lenders to contact the consumer by telephone before granting credit it his or her name.
- Together, the consumer and the customer service representative identify fraudulent items. Investigation, verification and removal of fraudulent items begin immediately. The creditors' addresses appear on the credit report to facilitate removal of the account information from the creditor's records.
- If a consumer elects to add the long-term victim statement, they are mailed two additional complimentary credit reports over a 90 day period enabling the consumer to monitor their credit history for additional fraudulent activity that may occur.

STEP 3: Investigation begins

- Experian notifies the creditors or data furnishers of alleged fraudulent items, typically through an immediate, automatic information transfer.
- Upon receipt of a valid police report Experian immediately blocks alleged fraudulent information from view by creditors and other users of the report. This allows a victim to continue to be credit active without being penalized for any fraudulent information on his or her report.
- Experian employs special system procedures and matching criteria to ensure that fraudulent data is removed as soon as possible.

- Experian attempts manual phone verifications and written proof documents from creditors, providing special services when appropriate for fraud victims to remove fraudulent data expeditiously.

STEP 4: Fraudulent data is removed

- Experian completes an investigation involving fraudulent information within 30 days. If the data contributor cannot verify information as accurate within the statutory deadlines, Experian's systems are designed to delete or update the information and prevent reappearance of the data.