

Before the Federal Trade Commission

**Workshop on the Costs and Benefits Related to
the Collection and Use of Consumer Information**

**Panel on the Costs and Benefits of the Collection
and Use of Consumer Information for Credit Transactions**

Testimony of Laura DeSoto
Senior Vice President
Credit Services
Experian

www.experian.com

Laura DeSoto
Experian
475 Anton Blvd.
Costa Mesa, CA 92626
714 830 5207
laura.desoto@experian.com

INTRODUCTION.....	3
THE ROLE OF INFORMATION SERVICES PROVIDERS	6
SOCIAL SECURITY NUMBERS	8
PUBLIC RECORD INFORMATION.....	9
CONCLUSION.....	9
<u>EXPERIAN CLIENT CASESTUDIES</u>	11
<u>LEADING CREDIT CARD ISSUER REDUCES FRAUD LOSSES THROUGH IMPLEMENTATION OF EXPERIAN’S</u> <u>AUTHENTICATION SERVICES</u>	11
<u>NATIONAL TELECOMMUNICATIONS PROVIDER BENEFITS FROM EXPERIAN FRAUD SOLUTIONS</u>	11
<u>APPENDIX A: INDUSTRY FRAUD INITIATIVES AND EXPERIAN CONSUMER ASSISTANCE..</u>	13
CONSUMER DATA INDUSTRY ASSOCIATION (CDIA) INITIATIVES	13
EXPERIAN’S CONSUMER FRAUD ASSISTANCE SERVICES.....	14
<u>APPENDIX B: “IN-WALLET” AND “OUT-OF-WALLET” INFORMATION.....</u>	16
<u>APPENDIX C: EXPERIAN’S BUSINESS FRAUD SOLUTIONS.....</u>	17
<u>ABOUT EXPERIAN.....</u>	20

Introduction

Economic crime cost U.S. businesses more than \$1 trillion dollars in the year 2000 (from studies by the American Bankers Association (ABA), BAI, Cellular Telephone and Internet Association (CTIA), Coalition Against Insurance Fraud (CAIF), UN). According to a study by Meridien (July 2002), institutions absorb approximately \$18,000 per identity theft including lost revenue and other costs associated with the crime. It is a serious crime that affects businesses across all industries, among them: financial services, health care, insurance, cellular services, utilities, retail, technology and online commerce.

Today, there are highly effective tools to fight fraud and identity theft. Information services providers are in a unique position to 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 victimization and eliminates the challenges of recovery.

Businesses have reported significant reductions in losses within the first year of implementing Experian's fraud detection and prevention tools. 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.

It is not uncommon for clients to experience decreases in fraud losses of 50 percent. A national telecommunications company reported a decrease in fraud losses of 55 percent. Equally important, the company reported a nearly 70 percent reduction in the time it took to confirm fraud records, helping them stop fraud and prevent victimization of consumers (*See Client Case Studies*).

Experian believes that investment in effective fraud detection and prevention tools is critical to the success of our economy. Demand for our industry-leading fraud services reflects the realities of today's marketplace and the need for effective tools to verify identities of customers that often are never seen. The success of those tools, however, depends on responsible information sharing and continued access to key identifying information and information sources.

Today, our economy is national. Businesses of all kinds compete daily for customers across the nation. It is common for a company based in Los Angeles to compete with one based in New York for a customer in Kansas – a customer they will know only through an application received through the mail, from an order placed by telephone or as the result of an online transaction. Responsible information sharing is essential in such a business environment to establish and maintain customer relationships, increase efficiency and prevent fraud.

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.

Unfortunately, Experian and other information solutions providers alone cannot erase fraud. Successfully fighting fraud requires integrating information from information solutions providers like Experian with that maintained by businesses and strengthening fraud prevention tools by sharing many kinds of identifying information from a broad spectrum of sources. Barriers to the ability of businesses and information solutions providers to integrate fraud prevention tools and actions that impede responsible data sharing among information service providers, businesses and their affiliates will perpetuate fraud and identity theft.

The fight against fraud also depends on enforcement of anti-fraud laws, which is very difficult for law enforcement agencies already strapped for resources. Fraud is often seen as a crime without consequence. There are few arrests and prosecution is rare. Without additional funding for law enforcement and prosecution of fraud cases, little progress will be made in reducing the crime.

Additionally, consumer education is a critical component of reducing fraud. Well-educated and informed consumers are better able to protect themselves from fraud and identity theft. Experian produces and provides a number of consumer education materials that include information about fraud and identity theft. We speak regularly to consumer groups, educators and government consumer protection agencies, and we support national consumer education programs in an effort to help people gain the knowledge and resources they need to better protect themselves.

Fraud is an information crime and information is required to fight it. Data must be available to legitimate businesses, law enforcement agencies and others to detect, investigate and prosecute the crime. Information -- in the form of education -- must be available to consumers to help them avoid victimization. It seems a contrary notion, but more information -- used responsibly -- is the solution to fraud and identity theft. Restrictions on information sources, collection and responsible use impair the ability of companies like Experian to fight fraud and identity theft.

However, in their well-intended efforts to protect consumers, regulators and legislators are proposing and enacting regulations and laws that restrict or eliminate access to data critical to the fight against fraud and identity theft. Public records, Social Security numbers and identifying information from financial institutions and other entities are all under scrutiny. Unfortunately, restricting or eliminating access to such data for legitimate business needs, including fraud prevention, results in greater exposure of consumers to fraud, not protection from it.

The role of information services providers

Information services providers, which include FCRA-governed consumer reporting agencies, are uniquely positioned to collect data from many sources and to analyze that data for indicators of fraud. They are the most experienced of any industry at ensuring data security and protecting consumer privacy. They have long led the way in both fraud prevention and consumer fraud assistance (*See Appendix A*).

Highly accurate, current identifying information is the most essential element of fraud prevention. Consumer identifying information from credit histories, such as name, address, date of birth and Social Security numbers, is one of the most accurate and

comprehensive sources of such data. In addition, information from credit histories enables the use of “out-of-wallet” information that is known only to individual consumers. Out-of-wallet information is a critical component of identity verification systems (*See Appendix B*).

Experian’s expertise in data analysis has enabled us to create and implement many fraud detection and prevention solutions in compliance with the FCRA. Our ability to collect and compile information critical to fraud detection and prevention, coupled with our expertise in data analysis including comparison of factors that are associated with fraud -- often reflected as a score indicating the risk level -- has enabled Experian to produce cutting edge fraud detection and prevention tools. Those tools include FACs+, Fraud ShieldSM, the National Fraud DatabaseSM and DetectSM (*See Appendix A*).

Development of Experian’s fraud prevention tools began more than a decade ago with the introduction of FACs+, a basic tool that alerts lenders to information in a credit report that indicates higher fraud risk, such as Social Security numbers that have not been issued. Since that time, our fraud services have evolved to utilize a much wider array of data sources and sophisticated analytics. Today, Experian’s National Fraud DatabaseSM, a cooperative database of verified fraud data, and DetectSM, a tool that enables comparison of shared application data to identify fraud indicators, represent the most sophisticated and effective fraud services available.

Today’s most successful fraud prevention tools depend on the ability of information solutions providers and businesses to share accurate, current and complete data. Restrictions on data sources and the ability to responsibly share data among information solutions providers, businesses and their affiliates renders sophisticated fraud

prevention tools useless. Data sharing and fraud detection system integration is critical to detecting and preventing fraud at its origin – the point of sale or application. Without the availability of data and the ability to share that data responsibly fraud cannot be stopped.

Social Security numbers

Social Security numbers (SSNs) often are described as the key to committing fraud. As a result of that characterization, the availability of public records for fraud prevention is being threatened by deletion or redaction of SSNs from public records and closure of public records that include SSNs. 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 must reject or modify the proposal or the accuracy of consumer reports may 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 the FTC review and comment on the U.S. Judicial Conference proposal.

Public record information

When carefully compiled and used responsibly, information from public records is essential to detecting and preventing fraud of all kinds. Yet state and federal regulation and legislation seriously threaten access to public record data associated with bankruptcy, liens, judgments, drivers' information, birth and death records and other information important for fraud prevention.

Public record data is an essential source of accurate identifying information. A key component of fraud detection is matching one source against others to identify anomalies that may indicate fraud. For example, comparison of birth dates among multiple public sources such as drivers' records and birth and death records might reveal indicators of fraud. Loss of data from one or more of those sources significantly impacts the effectiveness of fraud prevention tools.

Conclusion

Today, consumers expect instant access to 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 affordability and convenience while at the same time protecting consumers and themselves from fraud and identity theft. Successfully achieving both requires access to broad sources of information. Yet, regulators and legislators target information access in their efforts to attack fraud and identity theft.

That attack is inadvertently aimed at the wrong target and is resulting in friendly fire casualties. We are allies in the fight against fraud. Our enemy is the same. Unfortunately, regulation and legislation that target access to vital information can critically wound or even kill our efforts in that fight.

Restricting or eliminating access to and prohibiting the sharing of essential information among legitimate organizations impede the development and implementation of effective fraud prevention tools. As fraudsters become more sophisticated, the ability to access and responsibly utilize more data becomes increasingly important. While well intended, restrictions on sensitive data use exacerbate the problem by making it more difficult, if not impossible, for businesses to detect and prevent fraud.

Experian client 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 A: Industry fraud initiatives and Experian consumer assistance

Consumer Data Industry Association (CDIA) 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 one of the national agencies. 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.

Experian's consumer fraud assistance services

In 1991, Experian became one of the first national consumer reporting agencies to establish a dedicated fraud unit. Today, specially trained fraud representatives work throughout Experian's National Consumer Assistance Center, and career advancement incentives encourage employees to receive specialized fraud assistance training.

Fraud security alerts and victim statements protect consumers who have reason to believe or know that they have been victimized. A series of free reports are sent beginning with the addition of temporary security alert and followed by two additional reports at 45-day intervals after the addition of a victim statement, which lasts seven years. Today, consumers need only contact one of the national credit reporting agencies to have fraud alerts added to the credit histories maintained by each of the agencies.

Experian has worked with the FTC and our industry counterparts to create a uniform fraud affidavit so that consumers can submit only one form with relevant information to each of the national credit reporting agencies. Experian automatically

blocks accounts and other information reported as fraudulent when a consumer submits a police report.

Consumers who are not victims but are concerned about fraud can subscribe to Experian's Credit Expert service. The online tool provides notification of new credit history entries, unlimited access to their credit reports, risk scores and educational materials to help them better manager their personal finances.

Appendix B: “In-wallet” and “out-of-wallet” information

The key to fraud prevention, detection and recovery is accurate identification of the individual consumer. Identification data used for fraud detection and prevention services falls into two fundamental categories: in-wallet and out-of-wallet.

In-wallet data is any identification likely to be found in a person’s wallet or purse. It includes basic identifying information such as name, address, date-of-birth and Social Security number. It also includes other easily accessible information such as telephone and driver’s license numbers.

Out-of-wallet information is information not typically found in a wallet or purse and that is not readily accessible through other sources. It is information that should be known only to the consumer. Out-of-wallet information can include details about credit histories such as when an account was opened or what company holds the consumer’s mortgage or did at some point in the past. Credit histories are an important and reliable source of such information.

In-wallet questions establish baseline identification, but because the identifiers are likely in the possession of the identity thief, they are only marginally reliable. Out-of-wallet data is critical to identifying fraud and identity theft and for ensuring secure, safe transactions, particularly in an online environment.

Appendix C: Experian's business fraud solutions

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 ShieldSM: 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 ShieldSM does not indicate fraud is or has occurred, but instead indicates to lenders that information suggests a higher fraud risk. Fraud ShieldSM 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 DatabaseSM: Experian stepped to the forefront of fraud and identity theft detection and prevention with the introduction of the National Fraud DatabaseSM. 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.

- DetectSM: A further advance in fraud detection and prevention, DetectSM provides 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. DetectSM identifies inconsistencies and anomalies in application information that indicate identity theft or other types of fraud.
- AuthoricheckSM: A class-leading business fraud prevention tool, AuthoricheckSM 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.

About Experian

Experian provides strategic support to organizations around the world. It helps its clients target, acquire, manage and develop profitable customer relationships. It does this by combining its advanced decision support and outsourcing services with information on consumers, businesses, motor vehicles and property. Experian works with more than 40,000 clients across diverse industries, including financial services, telecommunications, health care, insurance, retail and catalog, automotive, manufacturing, leisure, utilities, property, e-commerce and government. Millions of consumers rely on Experian's consumer credit services to meet their financial management needs. Experian is a subsidiary of GUS plc and has headquarters in Nottingham, UK, and Costa Mesa, Calif. It has a 175-year history and unbroken sales growth over the past 23 years. Its 13,000 people support clients in more than 60 countries. Annual sales exceed \$1.9billion. For more information, visit the company's Web site at www.experian.com.