LOCKING UP THE EVIL TWIN

A SUMMIT ON IDENTITY THEFT SOLUTIONS

PERSPECTIVES AND RECOMMENDATIONS FROM
GOVERNOR ARNOLD SCHWARZENEGGER'S
MARCH 1, 2005 SUMMIT
SACRAMENTO, CALIFORNIA

GOVERNOR ARNOLD SCHWARZENEGGER

March 1, 2005

Dear Summit Attendees:

On behalf of all Californians, I am pleased to welcome you to California's first Summit on Identity Theft Solutions: Locking Up the Evil Twin.

As a leader in privacy protection, California continues to pursue new ways to stem identity theft crimes that victimize our citizens, businesses and government. We must take collective and aggressive action to prevent these crimes and make our state a safer place to live and raise families.

This Summit brings together experts from law enforcement, government, business and consumer organizations. Working together, we will develop better methods for fighting identity theft by clarifying major obstacles to prosecution and proposing solutions to help investigators and prosecutors enforce our laws and bring identity thieves to justice.

Thank you for helping us confront this important issue. Together we will work toward solving the problem of identity theft. Your work represents a great step forward.

Sincerely,

Governor Arnold Schwarzenegger

state capitol • sacramento, california (916) 445-2841

LOCKING UP THE EVIL TWIN
A SUMMIT ON IDENTITY THEFT SOLUTIONS

Perspectives and Recommendations from Governor Arnold Schwarzenegger's March 1, 2005 Summit Sacramento, California

CONTENTS

1. Introduction 1
   - The Crime of the 21st Century 1
   - Keynote Address 2

2. Summit Summary 3
   - Business Perspectives on Identity Theft 3
   - Government Perspectives on Identity Theft 4
   - Consumer Perspectives on Identity Theft 7
   - Law Enforcement Perspectives on Identity Theft 9

3. Recommendations 12
   - Legislation 12
   - Education 12
   - Victim Services 12
   - Research 13

4. Appendices 14
   - Keynote Address 14
   - Business Perspectives 18
   - Government Perspectives 30
   - Consumer Perspectives 45
   - Law Enforcement Perspectives 64

1. INTRODUCTION

The Crime of the 21st Century

Identity theft has been called the fastest-growing crime in the United States with over nine million victims annually in 2003 and 2004, including more than a million Californians.[1] Identity theft has been the number one complaint filed with the Federal Trade Commission for the past five years.[2] The term "identity theft" or "identity fraud" refers to crimes in which someone obtains and uses another person's personal identifying information to commit unlawful acts, usually for financial gain.[3] It is a very serious crime that cost consumers and businesses over $52 billion in 2004.[4] Not only do identity theft victims spend money out of pocket to clear up their records, but they also must devote their time – up to hundreds of hours in some cases – doing so. In the meantime, victims are unjustly harassed by debt collectors, denied credit or employment opportunities, lose their cars or their homes, or are repeatedly arrested for crimes they did not commit.

California leads the nation in providing legal rights and remedies for identity theft victims, many of which have been extended to other states by the 2003 amendments to the federal Fair Credit Reporting Act.[5] Yet victims, consumer advocates, financial institutions and law enforcement officials in California continue to report frustrations with bringing the criminals to justice, which is often the only way to end the victimization. Several factors are cited as making this crime difficult to investigate and prosecute, including its multi-jurisdictional nature, limited law enforcement resources, and inadequate penalties.

On March 1, 2005, Governor Arnold Schwarzenegger presented "Locking Up the Evil Twin: A Summit on Identity Theft Solutions," in Sacramento, California. The daylong Summit, which was attended by more than 500 people, focused on clarifying the major obstacles to the successful prosecution of the crime and on suggesting solutions to overcome those obstacles. Hosted by the California District Attorneys Association and coordinated by the State and Consumer Services Agency, the Department of Consumer Affairs and the Office of Privacy Protection, the Summit brought together those most knowledgeable about identity theft and particularly about prosecution issues. Speakers from financial institutions, online merchants, key government agencies, consumer organizations, and law enforcement shared their experience and their suggestions for further action.

---

1 See the "2005 Identity Fraud Survey Report," from Javelin Research and Strategy and the Better Business Bureau, available at http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html. The Federal Trade Commission 's "Synovate Report of Identity Theft Survey," September 2004, is available at http://www.consumer.gov/idtheft/stats.html. The California statistic is derived by applying the rate of identity theft in the adult population, 4.3% in 2004, according to the Javelin-BBB report, to the adult population of California, 26,927,116, according to the Department of Finance Demographic Research Unit.

2 See the Federal Trade Commission's "National and State Trends in Fraud and Identity Theft," February 1, 2005, available at www.ftc.gov.

3 California Penal Code section 530.5 defines the crime as when a person "willfully obtains personal identifying information…of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, or medical information in the name of the other person without the consent of that person…."

4 According to the Javelin-BBB survey report cited above.

5 The Fair and Accurate Credit Transactions Act (FACTA) of 2003 amended the Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681 et seq. Most of the new consumer and identity theft victim rights took effect in by December 1, 2004, although some are not yet in effect pending the issuance of regulations by the Federal Trade Commission. See the section on Consumer Perspectives for more information.

Keynote Address

The keynote address was delivered by Jan Scully, Sacramento County District Attorney and a recognized leader in victim rights. She began with the story of Sacramento's most famous identity theft case, in which the thief bought $17,000 worth of goods without anyone noticing that he was using the name and Social Security number of Eldrick "Tiger" Woods. She described criminal techniques that are becoming ever more sophisticated. From the simple method of stealing pre-approved credit offers from mail boxes, thieves are using technology to create convincing counterfeit checks, elaborate schemes to pose as fraudulent business with access to rich lines of credit, and treasure troves of personal information from credit brokers.

Scully said that law enforcement must meet the challenge of this criminal wave of the 21st century by being as creative as the criminals, identifying criminal trends and thinking in new ways to stay ahead of them. She called for partnerships between business, especially financial institutions, and consumers to work on new education and prevention strategies. She urged all present to consider themselves terminators – terminators of the would-be evil twins.

2. SUMMIT SUMMARY

Business Perspectives on Identity Theft

Howard Gould, California Commissioner of Financial Institutions, moderated a panel of representatives of companies upon which identity theft is having a significant impact.

- Ronni Burns, Senior Vice President, Director, Business Practices, Citi Cards
- Laurel B. Kamen, Vice President, Government and Consumer Affairs, American Express
- Gary Reynolds, Senior Vice President/Director of Financial Crime Investigations, Wells Fargo Bank
- Tom Sullivan, Director, Merchant Risk Council; Director of e-Commerce, Expedia

Definition of Identity Theft

Some business speakers believed that the definition of identity theft commonly used by news media is too broad: The term should not include just the use of someone else's existing credit card account, but should be reserved for instances when an imposter uses someone's identifying information to open up new financial accounts. The impact on victims is quite different. Credit card issuers generally remove charges the customer did not make after a single phone call from the customer, while clearing up new accounts that the victim may discover over a period of months is a much more difficult and time-consuming process.

Fraud Detection and Prevention

Identity theft has a significant impact on online merchants. According to industry studies, large online merchants are seeing that between 0.3% and 0.5% of sales are fraudulent, representing billions of dollars. Merchants put most of their efforts into prevention, knowing the difficulties in prosecuting and taking legal action. The increasing sophistication of fraudsters has forced merchants to adopt new fraud-prevention strategies and to devote more resources to the effort. Merchants may use third-party services that provide a "risk score" on transactions, on which the merchants can base their decisions. Larger online merchants have developed their own predictive models. Three California cities – San Francisco, Los Angeles, and Anaheim – are among the top ten cities with the most fraud, according to one online merchant. California cardholders are also slightly higher among those being victimized.

Enhanced Victim Assistance

Financial institutions have enhanced the assistance they offer customers who experience identity theft. Some institutions have created specialized service centers that help identity theft victims go through the process of clearing up their credit records.

Consumer Education Needed

Financial institutions believe in the importance of educating consumers on how to protect themselves against identity theft. Many provide brochures and use their Web sites to provide consumer tips on protecting personal information. So-called "phishing" scams are of particular concern, since banks are the frequent targets of fraudsters who create fake Web sites to lure consumers into giving their personal information. Institutions also provide their customers with information on how to recognize the signs of identity theft and what to do if they should become victims.

Collaboration in Addressing the Problem

Industry groups are working together to address the problem of identity theft. The Merchant Risk Council, whose 7,500 members include the top 50-60 e-commerce companies, collectively gathers fraud data so they can offer a larger case to law enforcement. The Council works with law enforcement, such as the FBI on physical goods and the Secret Service on digital goods.

Major financial institutions are collaborating through the Financial Services Roundtable and the Banking Information Technology Secretariat to ease the burden of identity theft on victims. Together they formed the Identity Theft Assistance Corporation, which is being phased in by members. The victim assistance program includes a single point of contact at the company to whom victims report identity theft, the use of an industry-wide uniform affidavit of identity theft, and other recommended best practices such as a streamlined internal reporting process that save the victim from having to repeat the same facts to different departments of the same company.

Financial institutions are also collaborating with other companies to take action on fraud and are changing their processes to prevent it in the future. An example of this is the recognition by one credit card issuer of a spike in fraud related to rental car transactions. It was found that fraudsters were finding the back copies of credit card receipts, which contained dates of birth, Social Security numbers and credit card numbers, in dumpsters. The card issuer convinced the rental car company to change its forms so that the last two copies no longer contained personal information, which caused the incidence of fraud to plummet. This soon became an industry standard, essentially eliminating this form of fraud.

Partnering with law enforcement is also producing positive results. A committee of credit card issuers worked with the U.S. Postal Inspection Service to address the problem of credit cards stolen from the mail. This group came up with the process of having new cards activated by a call from the card holder's home phone, a practice which became an industry standard and reduced this type of fraud by 80%.

Government Perspectives on Identity Theft

Senator Debra Bowen moderated a panel of representatives of state and federal government agencies that are responding to identity theft.

- Patrick Henning, Director, California Employment Development Department
- William P. Wood, Acting Commissioner, California Department of Corporations
- Joanne McNabb, Chief, California Office of Privacy Protection, California Department of Consumer Affairs
- Sylvia Kundig, Staff Attorney, Western Region, Federal Trade Commission
- Gregory Campbell, Assistant Inspector in Charge, San Francisco Division, U.S. Postal Inspection Service

Unemployment Insurance Fraud

The California Employment Development Department (EDD) has found that thieves are using stolen identities to fraudulently claim unemployment benefits. This fraud is harmful on several levels. Individuals whose personal information was used are unable to get benefits to which they are entitled and may incur tax obligations, employers pay for the unearned benefits, and taxpayers ultimately pay the cost of fraud against government agencies.

EDD has instituted several measures to detect and prevent this kind of fraud. Procedures include verifying Social Security numbers with the Social Security Administration and flagging suspicious claims for additional verification. EDD has set up a toll-free hotline and a Web site reporting system for individuals and employers to report allegations of fraud. An internal anti-fraud workgroup continually explores new ways to identify fraud patterns and trends, and updates the Department's processes to stay current with the fraudsters. EDD provides educational materials for individuals and employers and meets with employer groups to provide training on how to protect confidential payroll records and how to manage unemployment insurance accounts in order to prevent fraud.

EDD's investigators also work closely with federal and local law enforcement, resulting in a number of prosecutions. Media coverage of the prosecutions has helped to alert employers to notify EDD whenever they believe their records have been compromised.

Fraudulent Online Escrow Services

The California Department of Corporations (CDC) is dealing with online escrow fraud, a new online scam. It is a significant concern to CDC, because CDC regulates independent escrow companies. Online escrow companies, which act as independent third parties between buyers and sellers, can make shopping online safer. They are used for payments for items sold on online auction sites and marketplaces.

Fraudulent escrow sites are set up using stolen identities and credit card numbers. These fake sites often claim to be licensed by CDC, sometimes providing a link to the Department's Web site. (CDC, however, currently licenses just one online escrow service.) These fake services victimize both buyers and sellers, stealing their money or their goods and at times their personal information as well.

Since May 2004, CDC has taken enforcement action against 46 online escrow services, shutting down their sites. In addition to continuously monitoring for new fraudulent escrow sites, the Department has formed an Online Escrow Fraud Task Force. This task force is comprised of CDC, the Federal Trade Commission, the FBI, the Southern California High-Tech Crimes Task Force and the Escrow Institute of California. The Task Force will coordinate information and fraud prevention programs to improve the rapid detection, prevention, investigation and prosecution of escrow fraud in California.

Identity Theft Information and Assistance: California Office of Privacy Protection

The California Office of Privacy Protection (COPP), in the California Department of Consumer Affairs, is the only state agency in the country dedicated to consumer privacy. Created by legislation enacted in 2000, the four-year-old Office undertakes many activities to address identity theft.

One of the primary functions of COPP is to assist consumers who contact it with privacy concerns or complaints. Individuals contact COPP on its toll-free phone line, 866-785-9663, or by e-mail to privacy@dca.ca.gov. Identity theft is the most common concern of those who call or email the Office, representing 61% of all contacts: 9% are identity theft victims and 52% are concerned about becoming a victim.

COPP also provides consumers with information and education on identity theft and other privacy issues. The primary vehicle for disseminating information is the COPP Web site, www.privacy.ca.gov, which contains materials for consumers, business and law enforcement. The Web site includes a page devoted entirely to identity theft, containing COPP 's consumer information sheets and links to other resources. There are also Web pages on California and federal privacy laws, pending California privacy and identity theft legislation, and other privacy

topics. COPP's consumer information sheets, which are written in plain language at an 8th grade reading level, include several on identity theft.

COPP also issues "Recommended Practices" documents, which contain recommendations to organizations for managing personal information to protect consumer privacy. The "California Business Privacy Handbook" provides smaller and medium-sized businesses with basic information on privacy laws and good practices for preventing identity theft.

COPP coordinates with law enforcement, principally the regional High Tech Crime/Identity Theft Task Forces, and works with the State Chief Information Officer and Information Security Officer on privacy and information security practices for state agencies.

The Federal Trade Commission's Identity Theft Program

Since the passage of the Identity Theft Assumption and Deterrence Act in 1998, the Federal Trade Commission (FTC) has had a specific role in combating identity theft. The FTC collects consumer complaints and provides victim assistance through a telephone hotline and a dedicated Web site; maintains and promotes the Clearinghouse, a centralized database of victim complaints that serves as an investigative tool for law enforcement; and provides outreach and education to consumers, law enforcement and industry. In February 2005, the FTC announced that, for the fifth year in a row, identity theft topped the list of complaints, accounting for 39 percent of the 635,173 consumer fraud complaints filed with the agency in 2004.

The FTC published the first comprehensive national survey of identity theft in September 2003. The survey revealed that nearly 10 million Americans were victims of identity theft in the previous year, with a cost to victims and business of over $50 billion. It found that 51% of the victims did not know how their personal information had been stolen. The survey also found that 22% of victims said their information was acquired through theft of wallet, checkbook, credit card or mail; 13% said it was during a transaction such as payment by credit card; and 14% said someone who had access to it in their household or in an organization stole it.

The U.S. Postal Inspection Service

Another federal agency, the U.S. Postal Inspection Service, is also very involved with identity theft. The Postal Inspection Service, the law enforcement arm of the U.S. Postal Service, investigates identity theft cases involving the mail. Some identity thieves steal mail and use the personal information on checks, bills and other documents to commit identity theft. Thieves also change their victims' addresses to prevent them from receiving bills and use the mail to order and receive goods purchased using stolen identities.

As a federal agency, the Postal Inspection Service can often overcome jurisdictional challenges facing local law enforcement in some identity theft cases, and the penalties for mail theft are substantial.

The Postal Inspection Service reports significant increases in volume mail thefts, in which high-volume receptacles, such as postal vehicles, collection boxes, and apartment mailbox panels, are targeted. The number of such attacks more than doubled from 3,400 in 1999 to 8,200 in 2003. The number of arrests and convictions of mail thieves also increased significantly in the same period.

In response to identity theft, the Postal Service has instituted preventive measures. One is the change-of-address procedure adopted in 1996, in which a post office sends a "Move Validation Letter" to both the old and new addresses in an effort to confirm the legitimacy of the change submitted. The Postal Inspection Service has also

mounted a public education campaign on identity theft, including tips on protecting mail and other preventive strategies. Identity theft information for consumers is available on the Postal Service's Web site, at www.usps.com/postalinspectors/idthft_ncpw.htm, and at local post offices.

Consumer Perspectives on Identity Theft

Charlene Zettel, Director of the Department of Consumer Affairs, moderated a panel that discussed identity theft from the perspective of victims and those who assist them.

- Tracey Thomas, Volunteer, Identity Theft Resource Center
- Robin Fifield, identity theft victim
- Beth Givens, Director, Privacy Rights Clearinghouse
- Mari Frank, Esq., Author of Identity Theft Survival Kit
- Tony Hadley, Vice President, Government Affairs, Experian

Victims As Their Own Investigators

Victims of even the more common credit-related forms of identity theft report that they have to shoulder the burden of clearing up their records and perform much of the investigation of their own cases. This can involve hours of phone calls and letter writing over months and even years; victims have said that it's like having a second job. Because of a lack of adequate law enforcement resources to investigate identity theft cases, some victims report that they had to track down the thief themselves and then provide the information to law enforcement. This process was aided somewhat with the passage in 2001 of a California law that gave identity theft victims who have a police report access to applications and other records on fraudulently opened accounts. An identity thief who remains at large can continue to use the victim's information, requiring the victim to go through the process of clearing up records over and over again.

In criminal identity theft cases, an at-large thief can nearly bring the victim's life to a halt: preventing the victim from driving, being insured or working, from having custody of his or her children, or from moving about without being arrested. The time and expense necessary to deal with the situation are significant.

The Worst-Case Scenario: Criminal Identity Theft

Victims and victim advocates described what is possibly the worst type of identity theft: "criminal" identity theft. Criminal identity theft occurs when an imposter gives another person's name and personal information to a law enforcement officer upon arrest or during an investigation. Or the imposter may provide a counterfeit driver's license or other identification card. The victim of this kind of identity theft may lose his or her driver's license, be arrested repeatedly, and be unable to get work, sometimes for years. The FTC found in its 2003 survey that 4% of identity theft victims are victims of criminal identity theft. That would mean there were nearly 400,000 such victims nationwide in 2003, including at least 45,000 in California.

California Identity Theft Registry: Is It Working?

To address the extreme difficulties faced by criminal identity theft victims, legislation created the California Identity Theft Registry in the Department of Justice, along with court processes for getting into the Registry and

for sealing or destroying wrongful criminal records. Victims of criminal identity theft who provide fingerprints and a Judicial Finding of Factual Innocence from a court can apply to enter the Registry. They are then given a PIN number and the Registry's toll-free number, which the victims can use to clear themselves when stopped by police. Registry staff members also send letters to employers verifying a victim's status.

The Registry has been available since 2001, and while registration has increased by 400% since the publication of the California Office of Privacy Protection's guide to getting into the Registry, it still contains only 30 people. The primary reason cited for the low number of registrants is the lack of knowledge of the Registry and the process for getting into it not only among victims, but also among those who should know: judges, court clerks and administrators, law enforcement, prosecutors, criminal defense attorneys and others. There may also be problems with the registration process itself, but research is needed to determine what those problems might be.

New Tools for Victims

A key defensive tool that has been available to California identity theft victims for several years is the fraud alert. A fraud alert is a message that an identity theft victim can place on his or her credit file, which alerts credit issuers who are doing a credit check in response to an application for new credit in the victim's name to fraud associated with the account. An initial fraud alert lasts 90 days and is intended to prompt the credit issuer to call a given phone number or ask for additional proof of identity to verify that the applicant is not the imposter. Some victims reported that fraud alerts were not effective and that new accounts were opened in their names even though fraud alerts were in place. California's security freeze law, which took effect in July 2002, gives victims and other consumers the ability to control access to their credit files. A freeze stops essentially all access to a credit file and lasts until the consumer removes it or "thaws" it temporarily.[6]

Other new victim rights and tools, most of which originated in California, were extended nationwide with the FACTA amendments to the federal Fair Credit Reporting Act passed in 2003.[7] Some of these provisions simply codified existing practices of the credit bureaus, such as the single-call process, where a call to the fraud number of one credit bureau also notifies the other two, and the initial fraud alert. There is now an opportunity for the victim or potential victim to add his or her phone number to the fraud alert, indicating that a creditor should not issue new credit unless the victim is called to authorize it. California rights that were amended into the Fair Credit Reporting Act include the requirement that credit bureaus block or remove from credit files information resulting from identity theft, the requirement that businesses shred or otherwise properly dispose of consumer report records, and a broader version of the important right of an identity theft victim to get records on accounts opened or accessed by the imposter in the victim's name.

Among the new identity theft provisions in the Fair Credit Reporting Act that are still pending are "red flag" guidelines, procedures for creditors intended to allow them to spot and prevent fraudulent transactions before they are completed.

---

6 A consumer whose file is frozen is given a PIN number to use to temporarily thaw or lift the freeze in order to seek new credit. When a security freeze is in place, access to the credit file is still available to the consumer, the consumer's existing creditors for account monitoring purposes, and debt collectors. See Civil Code section 1785.11.2 et seq.

7 Most of the new consumer and identity theft victim rights added to the Fair Credit Reporting Act took effect in by December 1, 2004, although some are still pending the issuance of regulations by the Federal Trade Commission.

Law Enforcement Perspectives on Identity Theft

Senator Charles Poochigian moderated a panel of law enforcement officials who explained the challenges investigators and prosecutors face in dealing with identity theft and proposed new approaches.

- Jonathan Fairtlough, Deputy District Attorney, County of Los Angeles
- Lt. Robert Lozito, Project Director, Identity Theft Unit, Sacramento Valley Hi-Tech Crimes Task Force
- Edward S. Berberian, District Attorney, Marin County
- Lawrence Brown, First Assistant U.S. Attorney, Eastern District of California
- Robert Morgester, Deputy Attorney General, Special Crimes
- Jerry Coleman, Assistant District Attorney, San Francisco

The Task Force Approach

California has been innovative in addressing high tech crime and identity theft. When the dramatic increase in identity theft became apparent in recent years, the California Legislature expanded the existing system of five regional, multi-jurisdictional High Technology Theft and Apprehension Program Task Forces in 1998. State funding was provided to add special Regional Identity Theft Units that focus solely on identity theft crimes. Based in Los Angeles, San Diego, San Jose, Napa and Sacramento, the task forces were budgeted in 2004-05 at $1.9 million each for high-technology crimes and $435,000 for identity theft. Each task force is made up of law enforcement officers from major police agencies in at least two counties, local prosecutors, and state and federal investigators and prosecutors.

The Task Forces use different strategies, some focusing on large-scale identity theft crimes involving organized rings, while others direct their efforts to sweeps of probationers in an effort to stop the cycle of repeat offenses.

Several speakers discussed the challenges unique to investigating and prosecuting the crime of identity theft. The first challenge is the overwhelming volume of cases, each with many different victims and suspects. Over 20,000 cases were reported to the Los Angeles County Sheriff last year, and 1,200 were filed by the Los Angeles District Attorney's office. The Los Angeles-based Task Force did not handle most of these cases, but rather supplied the expertise and training to local agencies so that they could respond to the smaller cases involving $3,000 to $4,000 and one or two victims. This frees the Task Force to take on the large rings and organized identity theft operations that harm many victims and do serious damage to our credit and business infrastructure.

Challenges to investigation of the crime include its multi-jurisdictional nature, the volume of evidence in many cases, the frequently late discovery of the crime, and the amount of time required for communicating with victims.

Following Cold Trails

Identity theft victims, unlike robbery or burglary victims, often do not know they are victims until months after the crime has occurred. This time lag can give the thief the opportunity to move on, perhaps to another locale or state, leaving a cold trail of evidence. Communications with victims requires considerable time because the victim is the source of much of the evidence – bills, letters from collection agencies, credit reports, and so on. Victims also have to do a lot of paperwork, both to collect necessary evidence to turn over to law enforcement and to clear up their own credit and other records. Additionally, instructing victims in how to get needed documents and how to repair their records can take up a lot of law enforcement time.

Other Investigation Challenges

The volume of physical evidence in many identity theft cases also presents problems to investigators. The products purchased using stolen identities – computer equipment, furniture, sometimes an entire house full of products – must be collected and stored.

Another challenge is presented by inadequate police reports of identity theft. Not all police agencies have the personnel or the experience to take the kind of comprehensive police report that is necessary for an identity theft victim to be able to clear up his or her records and for an investigator to follow up.

Jurisdictional Problems

An identity thief may steal a victim's personal information in one county, use it to obtain credit or purchase goods in other counties, and have the fraudulently obtained products delivered in yet other counties – or these events may occur in different states or different countries. Such scenarios require coordination between multiple investigative and prosecutorial agencies, which is one of the benefits of the task force approach. A Deputy Attorney General assigned to each Task Force can assert jurisdiction in some multi-jurisdictional situations, and the U.S. Attorney can do so in others. Both agencies, however, have limited resources devoted to identity theft cases and must impose thresholds for involvement.

In California, an identity theft case may be prosecuted in the jurisdiction where the personal information was stolen or in any jurisdiction where it was used for an illegal purpose. But unlike in New York, Florida, Utah, Vermont and Wisconsin, in California jurisdiction does not lie where the victim lives. While current law mandates local law enforcement where the victim lives to take a report of identity theft, the local jurisdiction often does not have the ability to prosecute. Consider the example of a Sacramento resident whose wallet is stolen in Los Angeles and whose identifying information is used to purchase a computer delivered to an address in Los Angeles. A Sacramento police detective is required to take a report, but not to investigate. Law enforcement in Los Angeles cannot meet the needs of their own county residents, let alone those of an out-of-county victim. If a suspect should be identified, any subsequent prosecution would have to occur in Los Angeles, where prosecutors are similarly overburdened with their residents' cases.

Out-of-state cases pose even greater problems. Even in a case where several thousand Californians' identities were compromised, if the suspect is in another state and the information is used to purchase goods in another state, California cannot prosecute the case.

Trafficking in Stolen Identities

Identity theft has become more organized and is often associated with other criminal schemes. Law enforcement on the West Coast knows that many identity thieves are connected with methamphetamine abusers. The ringleaders hire addicts and pay them, in drugs or cash, for stolen identifying information, often from checks, bills and other documents found in dumpsters. It's a vicious cycle: dope is traded for stolen checks, which beget counterfeit checks, which when cashed provide the funds for more dope or are used to buy the computer equipment used to make more and better counterfeits.

Business Identity Theft

Identity thieves don't just target individuals. They also impersonate businesses, using their identifying information to gain access to their larger lines of credit. Businesses have the same problems individual victims have: They have to file a police report and get the attention of investigators and prosecutors. But businesses in California have an additional hurdle that individuals don't have. California's identity theft statute, Penal Code § 530.5, applies to a "person" whose personal identifying information is used for an unlawful purpose. The Penal Code definition of "person," at section 7, also includes a corporation. Some district attorneys, however, do not read it that way and will not charge identity theft when the victim is a corporation, and other entities, such as a limited liability partnership or an association, are outside the definition.

Business victims that do not meet the definition of a "person" cannot avail themselves of the rights dependent on having a police report of identity theft. One such right is the ability to get copies of applications and other documents on fraudulent accounts. Because of law enforcement's resource limitations, this investigative tool is critical to victims and often provides the only avenue to catching the thief. Business victims today are where individual victims were four years ago.

Resource Limitations

Even with prosecutors paid by state grant funds assigned to the task forces, the volume of cases investigated does not allow for a prosecutor for every case. Prosecutors on the task forces become knowledgeable about the crime and have the opportunity to learn the details of a case, and thus are able to get the biggest prosecutorial bang for their efforts, often resulting in longer sentences. When the task forces have to go to outside district attorneys, they report that they tend to get lesser sentences and more probation, putting the criminals back on the street where they are likely to re-offend almost immediately.

While federal penalties for identity theft are generally higher than state penalties, federal law enforcement resources are limited, leading to high dollar thresholds for involvement.

3. RECOMMENDATIONS

The panelists made several recommendations for addressing the challenges in investigating and prosecuting identity theft cases.

Legislation

- Legislation to expand the definition of "person" in Penal Code identity theft statutes to include a corporation, a limited liability partnership, an association, and other types of business.
- Legislation to extend the jurisdiction for identity theft cases to the county in which the victim resides.
- Legislation modeled on drug trafficking laws to make the possession of multiple persons' profiles and the trafficking in such profiles a felony.
- Legislation to make it a felony to abuse the identities of our most vulnerable: children under 18, seniors, and those serving in the armed forces.
- Legislation to enhance penalties for "criminal" identity theft: the use of someone else's personal information when arrested, cited, and convicted of a crime. Require those convicted to pay the victim's attorney's fees and court costs, and to serve time.

Education

- Consumer education on protecting personal information, and particularly on avoiding phishing scams.
- Additional focus for law enforcement education on the nexus between methamphetamine and identity theft connection. Train police to use their drug informants to find the identity fraud factories.
- Targeted education on "criminal" identity theft and the procedures for entering victims in the Identity Theft Registry for law enforcement, prosecutors, court clerks and administrators, judges, victim-witness assistance programs, and others.
- Training specific to investigating and prosecuting identity theft cases for law enforcement and prosecutors.

Victim Services

- Provide special assistance to victims of "criminal" identity theft, including the availability of counseling.
- Coordinate a working group of business, credit bureau, law enforcement, and identity theft victim assistance representatives to draft a uniform "Identity Theft Report" for use by victims.

Research

- Conduct research on "criminal" identity theft: how many victims are there? How does it happen? How does it affect victims in the short and long term? Is there a disparate impact on individuals of certain ethnicities, income levels, or other characteristics?
- Conduct research on the effectiveness of the (Criminal) Identity Theft Victim Registry and related court processes. Why are there so few people in Registry? How can the court process be made simpler? How much time does it take to get into the Registry? What uses are made of the Registry?
- Conduct research on the information broker industry's role in disseminating inaccurate information resulting from "criminal" identity theft. How do records flow from law enforcement and the courts to data compilers and beyond to the information brokers? What happens in the data flow when a victim's criminal records are expunged?

4. APPENDICES

Keynote Address

Jan Scully, Sacramento District Attorney

Good Morning everyone, we're here today to spend some time talking about Identity Theft. None of us are immune from victimization. Twelve years ago, it took me over a week to realize that the only person getting mail in our mailbox was my husband. By the time I recognized it, new credit card accounts had been opened up in my name and charges were already accruing. But, enough about me. As a prosecutor, I love to talk about cases.

Consider the case of Anthony Taylor. Prosecuted by my office just a few years ago, Taylor had a criminal record of 20 convictions, going back to the age of 14. At age 20, he had been convicted of two counts of home invasion robbery. But after serving his prison time, he learned that he could make much more money, without the physical danger, by going white collar. So in 1999, he located the Social Security number of a man he had never met, got a driver's license in that man's name – Eldrick T. Woods – and then used this information to go on a buying spree. He went into stores offering "instant credit," and bought furniture. At Good Guys he got electronics equipment. Putting just $100 down because of his good credit, he drove away from the dealership with a used Lexus.

It was easy, because when the computer check was done against the name of Eldrick T. Woods, with that Social Security number, he had excellent credit. And well he might. You probably have heard of Eldrick by another name – Tiger Woods, golfer extraordinaire, Sports Illustrated's Athlete of the Year, and corporate spokesman for Disney, Nike sportswear, Rolex watches, American Express Credit Cards, and Buick Automobiles.

In just a short time Mr. Taylor – who was on parole – netted $17,000 in merchandise and services. He was caught when a routine parole search turned up some of the property. Of course, an avid golf fan might have picked up the clues sooner, but while most people recognize the golfer Tiger Woods, not many would recognize the name Eldrick. Tiger hadn't been in Sacramento recently, as Deputy D.A. Nicole Liem established when Mr. Woods was on the witness stand – not since he was 13 years old, when he competed in a junior golf tournament (which he won). When asked on the witness stand if he had bought that used Lexus, and being the good spokesperson he is, Tiger answered, "No. Are you sure it's wasn't a Buick?"

Anthony Taylor, aka Eldrick Woods was convicted under the Three Strikes law because of his prior home invasion robberies and received a life sentence. But his $17,000 take represents, by the standard of some identity thieves, only a modest haul.

A recent report by the Federal Trade Commission shows just how big the identity theft problem is. The Consumer Sentinel database, maintained by the FTC, collects information about consumer fraud and identity theft complaints from over 150 organizations. In 2002, the database recorded 161,896 identity theft complaints. By 2004, that number had climbed to 246,570 – an increase of over 50% in just two years. Credit card fraud is the largest single category of identity theft, accounting for 28% of the complaints over this three-year period. Also high on the list are telephone or utilities fraud at 19%, and bank fraud (including electronic fund transfer fraud) at 18%. Employment fraud, government benefits fraud, and loan fraud are other notable categories.

This Summit today is important because California has more than its share of this problem. If you rank the major

metropolitan areas in the United States by the number of identity theft complaints per 100,000 population, five of the top fifteen areas, I repeat, five of the top fifteen areas are in California – the San Bernardino/Riverside "inland empire," the Los Angeles area, the San Francisco area, the San Diego area, and the Sacramento area. If you rank the states by complaints per 100,000 population, California ranks third. In raw numbers, California comes in first, with 65% more identity theft victims than runner-up Texas. In California we always like to think that we lead the nation, but in this kind of comparison, beating the Lone Star state is a dubious honor.

These statistics, as shaking as they are, only tell part of the story. Experts believe that identity theft crimes are greatly under-reported. That's, in part, because identity thieves often create a financial profile in someone else's name without that person's knowledge and the offense can go undetected for years.

While we often think of identity theft as being fostered by consumers making Internet transactions, that is not necessarily so. A Better Business Bureau survey released just last month shows that in cases when it is known by what means an identity thief came to possess the victim's personal information, it was most commonly from a lost or stolen wallet, checkbook or credit card; from a relative or acquaintance with access to the information; from a corrupt employee who had access, and of course, there is always the dumpster diver. And, we shouldn't ignore the fact that, of the cases where the identity thief is identified, half of those cases were committed by someone the victim knew.

Very often, however, the perpetrator remains unknown. Overall, law enforcement agencies estimate that only 11% of identity theft cases reported to them are solved. In Sacramento, we are fortunate to have a multi-agency regional task force that does significantly better – in the last six months of 2004 about 17% of the cases investigated led to prosecution. That is 50% more than the average, but hardly a comforting statistic.

Sometimes the criminal technique is surprisingly uncomplicated. The marketing methods for new credit cards, and competition in the credit industry, provide much of the fodder. We all receive applications for credit cards that are "pre-approved." Snatching a pre-approved credit card application from the victim's mail, an identity thief may simply create a new account with a new address, taking advantage of the offer that you never got, or that you threw away.

But that is only one of the methods used by identity thieves, and not the most common one, at that. With just a little personal identifying information and a little creativity, a thief can accomplish – or should I say steal – a lot. My office is currently prosecuting one defendant who used his father's Social Security number to obtain one fraudulent $12,000 loan, and the Social Security number of his twelve-year-old sister to obtain seven cars from six different car dealerships in the area. And he went after a wide variety – Honda, Dodge, Ford, Mercedes, Mitsubishi, and Chevrolet were among the nameplates he collected.

Even though consumer Internet transactions may not lead to most identity theft, that does not mean that technology is foreign to identity thieves. In fact, modern identity thieves are smart, resourceful, innovative, and often surprisingly adept with both technology and business practices. Sometimes working alone, and sometimes in groups or rings that share information, techniques, and the stolen identities, they are capable of inflicting a great deal of financial damage.

Our thief with the seven cars used a debit card to make the down payment on a $40,000 Chevy Tahoe. The debit

card was linked to a bank account that was closed, but he managed to use a special override or authorization code so that the transaction went through. We have prosecuted cases where defendants were making or possessed counterfeit driver's licenses, and also where they obtained merchants terminals for credit card transactions.

Another fertile area is the production of checks. Modern computer software and printers allow identity thieves to produce checks that appear in every way to be legitimate. Once they have a victim's checking account information they can produce checks that will drain the victim's account.

Of course the problem with doing that with an ordinary consumer victim is that most of us don't have checking account balances that will sustain a ring of criminals for very long. And if we are hit by just one or two fraudulent checks for even small amounts, the bank will simply close our checking account and open another for us. But there is another way that creative and ambitious identity thieves can go about their work.

One resourceful identity thief created a new account in the name of his citizen victim, but he did not fund it with that person's money. Instead, he bought a computer printer from Hewlett Packard that had a small rebate. When he got the rebate check, he had all the checking account information for one of HP's corporate accounts that often had a balance in the millions of dollars. He then created an HP check in seven figures to his citizen victim, and deposited it into the account that he had created using the citizen victim's name. The citizen victim never knew any of this was going on, since the transactions were going on in accounts that he had no knowledge of.

The key to most identity theft is for the perpetrator to get the personal identifying information of a regular person who has legitimate financial accounts and a credit history. One scam to get at such personal information is known as "Phishing." The perpetrator will send out an email to thousands of email addresses, purporting to be from a financial institution, or a business with which many people might have an account, such as eBay. The email has all the proper logos, and looks very official. It states that the business is updating its accounts, or checking for fraud, or some other such excuse, and asks the recipient to respond with their personal information, including their account numbers, so that their account can be confirmed, or updated. Most people simply don't respond. But the odds are in the crook's favor. Email is virtually cost free. If the thief can get a list of 10,000 email addresses, and send them out by way of an automated program, and if only 1 in 1000 people responds, then for very little investment, the crook now has the personal information and account numbers of 10 people.

Last year, in just one month, over 1000 unique phishing attacks were identified. In one single week, over 321 separate and unique attacks were reported. Each of these sent "phishing" emails to thousands of individuals.

But "phishing" is inefficient and crude compared to the techniques some thieves use. The identity theft task force in the bay area uncovered a ring that was stealing credit applications from an automobile dealership. The information from these applications was being used to install the consumers as officers and employees in a fraudulent corporation, completely without their knowledge. With such credit-worthy citizens at the helm, this corporation then obtained a line of credit that led to fraudulent loans.

Similar tactics can be used in a more sophisticated way, and on an even greater scale. ChoicePoint, a Georgia company, is a leading U.S. firm for compiling credit and financial data used by legitimate businesses, such as banks, credit companies, and insurance companies. Last fall, a group of con artists used previously stolen IDs to create several seemingly legitimate businesses, and then used these phony businesses to pose as legitimate business customers, buying consumer background information from ChoicePoint, just like any business might do. Less

than two weeks ago, ChoicePoint revealed that it unwittingly sold over 140,000 records of individual consumers to this group of criminals.

In like fashion, Abraham Abdallah, a master identity thief from New York, posed as an executive for Sprint when he contacted a private detective firm in Texas. He said he needed someone to do background checks on Sprint customers. He asked for the firm's rates and their private investigation license. Hoping to do business for Sprint, they sent him the information. He used it to pose as a private investigator, and set up his own account with an online database firm that specialized in financial checks for PIs. For only $300 per month, he got unlimited access to names, addresses, and Social Security numbers. From there, he could pick and choose the victims whose identities – and money – he would steal. He thought big, targeting the Fortune Magazine list of the 400 wealthiest Americans. When he was finally caught, he had stolen over $80 million, had bought a credit card manufacturing machine for $25,000 to make his own credit cards, and was in the process of creating his own off-shore bank, chartered in an African country, where he could launder money and cut off any audit trail.

To meet the challenge that identity theft poses, we need to be just as creative as the criminals, thinking in new ways about how we approach law enforcement. We need to identify the criminal trends, so that we can stay one step ahead of the crooks, and give Anthony Taylor some company in prison, as he rues the day he decided to target the identity of Eldrick Tiger Woods.

Because these crimes are multi-jurisdictional, we must not only think multi-jurisdictional, we must act multi-jurisdictional. We must work together not only in identifying and apprehending the thieves, but also in creating new education and prevention strategies, within the law enforcement community, and in partnership with the business community, especially our financial institutions, and consumer advocates. But, we need to go even further than that. When it comes to identify theft, instead of businesses and consumers being at different ends of the sales transaction, they need to work side by side to prevent and minimize the ever-sophisticated criminal enterprise that keeps all of us on our toes. Working together, we can rise to the challenge of this criminal wave of the 21st century. There is no way we in law enforcement can do it alone.

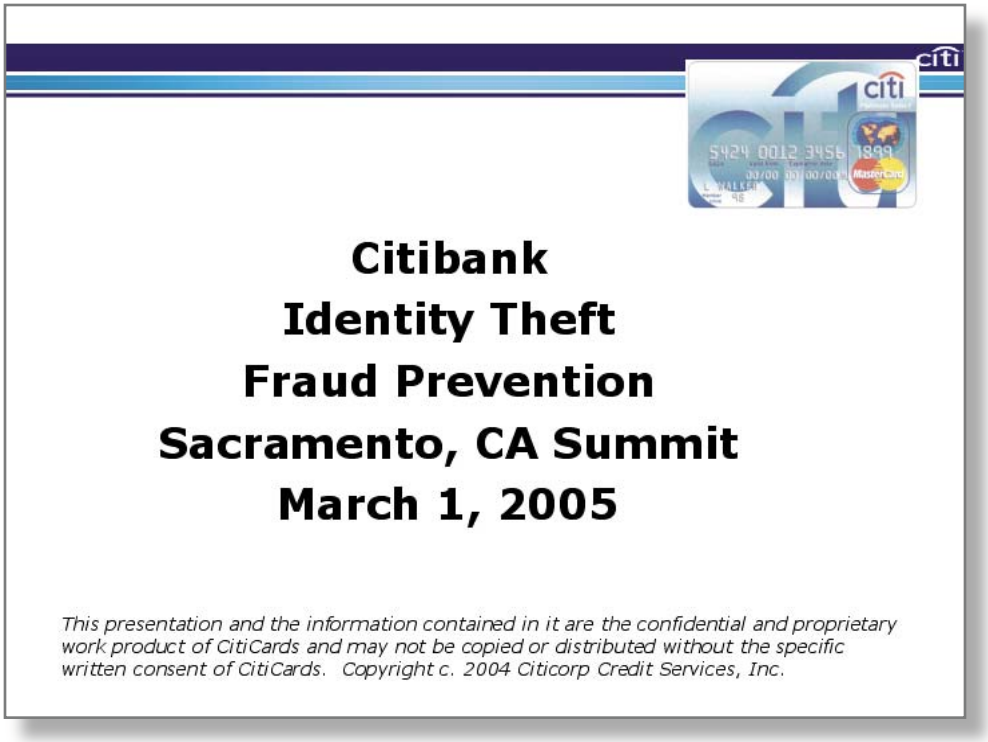
And that's why today's Summit is so exciting. We are all here today as partners and we have some great opportunities today to gain some new knowledge, some great perspectives, and forge some new partnerships.

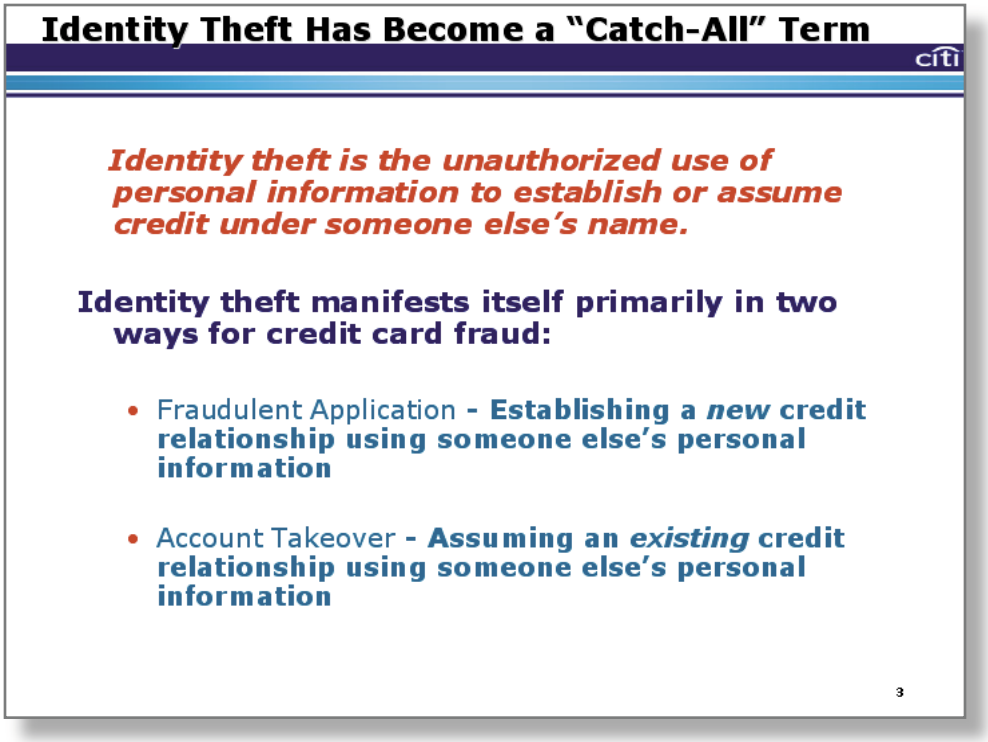
Thank you to Governor Schwarzenegger, the State and Consumer Services Agency, and its Department of Consumer Affairs, the event advisory members and all those who have partnered to make this day possible. For purposes of identity theft, we should all consider ourselves…terminators. Terminators of those would be evil twins.

Have a great day!

Business Perspectives

Ronnie Burns, Senior Vice President, Director of Business Practices, Citi Cards





ID Theft - Myth vs. Fact

citi

Myth: Financial institutions cause ID theft.

- Fact: **Sources of ID theft: unauthorized credit bureau access, Internet hacking, illegal sale of personal information, and "dumpster diving."**
- Fact: **Sharing information among financial institutions greatly assists in prevention & detection of ID theft**

- **helps detect irregularities in spending patterns**
- **helps alert consumers to potential fraud or ID theft**
- **helps with apprehending criminals**
- **helps us to meet or surpass the thresholds established**

4

ID Theft - Myth vs. Fact

citi

Myth: Identity theft is the majority of credit card fraud.

- Fact: **Majority of fraud stems from Lost, Stolen, and Counterfeit cards and checks.**
- Fact: **ID theft fraud represents only 0.30% of all Citi Cards new credit accounts established. The other 99.70% are *valid* requests for credit.**

5

ID Theft - Myth vs. Fact

citi

Myth: The vast majority of ID theft is caused by fraud rings.

- Fact: **A significant amount of ID theft is perpetrated by family and acquaintances "friendly fraud"**

  -perpetrator knows the victim's personal information.

  -perpetrator has access to the victim's mail, making ID theft hard to prevent/detect.

6

Consumer Prevention Tips

citi

- **Protect your mail/mailbox**
- **Safeguard your wallet and personal information**
- **Destroy all receipts you no longer need**
- **Monitor and review your credit reports regularly**
- **Look over your monthly billing statements**
- **Sign your cards immediately**
- **Never lend your card to anyone**
- **Notify your bank when you change your address**
- **Report all lost or stolen cards immediately**
- **Never put your account number on the outside of an envelope**
- **Be prepared – Write down card issuers customer service number for future reference.**
- **Don't leave receipts in shopping bags from stores**

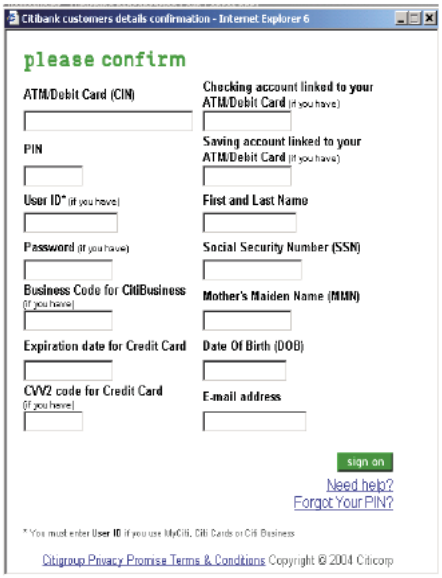
9

What is Phishing?

citi

Theft of customer personal information via social engineering (email/spoof website, fax, phone).

- email alerts recipient to confirm "vital" information:
  - "Verify your email address"
  - "Citi has experienced a server problem"
  - "Your identity may have been compromised"
- email contains a URL link to a spoofed Citi page requesting:
  - Account number, PIN, mother maiden name, card number, expiration date, CVV2/CVC2, date of birth, etc.



Phishing Email Attempt

citi

Typical phishing email message to customers:

Note IP Address and creative...

"CitiSafe"??????

Enviado el: sábado 3 de julio de 2004 1:34
Para: webmaster
Asunto: Please update your account details with Citibank

Dear Citibank Customer,

We recently noticed one or more attempts to log in to your Citibank account from a foreign IP address and we have reasons to believe that there was attempts to compromise it with brute forcing your PIN number. No successful login was detected and you have full protection by now. If you recently accessed your account while travelling, the unusual login attempts may have been initiated by you.

The login attempt was made from:
IP address: 173.27.187.24
ISP Host: cache-82.proxyserver.cis.com

By now, we used many techniques to verify the accuracy of the information our users provide us when they register on the Site. However, because user verification on the Internet is difficult, Citibank cannot and does not confirm each user's purported identity. Thus, we have established an offline verification system to help you evaluate with whom you are dealing with. The system is called CitiSafe and it's the most secure Citibank wallet so far.

If you are the rightful holder of the account, click the link bellow, fill the form and then submit as we will verify your identity and register you to CitiSafe free of charge. This way you are fully protected from fraudulent activity on all the accounts that you have with us.

Click to protect yourself from fraudulent activity! <<http://219.148.127.67/scri

To make Citibank.com the most secure site, every user will be registered to CitiSafe.

NOTE! If you choose to ignore our request, you leave us no choice but to temporally suspend your account.

* Please do not respond to this e-mail, as your reply will not be received.

Regards, **Citibank Customer Support**

Phishing – What is Citi doing?

citi

- Educate customers via brochures, web pages, and additional training of our customer service personnel.
- Created a specialized servicing role that customers can contact regarding an Internet concern or question.
- Increased staff responsible for investigating and disabling phishing sites.
- Established a suspicious email website where customers can send suspicious emails – spoof@citicorp.com
- Creating a standardized template for outbound emails with information that will typically not be in the hands of frauds.
- Enhanced detection formulas to target specific fraud behaviors.
- Partnering with a virus software company to ensure customers have the latest virus detection software.

10

Suggestions for Collaboration with Law Enforcement

citi

- View financial institution as the other victim who can file a police report.
- Allow police reports to be filed over the phone.
- View ID Theft fraud as a criminal as well as a civil matter.
- Work collaboratively across the industry to develop better case information
- Provide the financial institutions the criteria Law Enforcement will use to prosecute the case (dollar threshold, required evidence, case characteristics or criteria).
- Public service education messages.

14

Potential Legislative Provisions

citi

- General – Broadly define identity theft as a crime, including but not limited to phishing and spyware.
- Jurisdiction – Recognize that identity theft can occur in several jurisdictions and should be able to be prosecuted in any one of them.
- Standing – Recognize that financial institutions suffer financial loss from identity theft and allow them to file a criminal or civil complaint.
- This proposed act should work in conjunction with and closely resemble the Racketeer Influenced and Corrupt Organizations Act.

15

ID Theft Summary

citi

- Citi is committed to developing the tools and strategies that are necessary to prevent and detect identity theft, and to continue to assist victims of ID Theft.
- Citi along with other issuers work collaboratively to share fraud information and best practices – this enables quicker detection of ID theft and minimizes effect on the victim.
- We need to continue to partner with law enforcement and legislators in the detection, prevention and prosecution of criminals

16

Laurel B. Kamen, Vice President, Government and Consumer Affairs, American Express

American Express has a 154-year history of standing by our customers, whether cardmembers, merchants or others. While cardmembers are never liable for any unauthorized charges on their cards, protecting their good name and helping them when a problem such as identity theft occurs are a top priority for our company.

American Express has deployed a truly holistic approach to ID theft prevention, detection and recovery – and we have done this over many years. As the fraudsters have gotten more sophisticated and technologically savvy, so have we. And we have done this through a broad partnership of law enforcement agencies, government entities, merchant partners, and consumer advocacy groups.

Last year, we did a survey of our cardmembers to understand how well consumers understand the overall risk of identity theft, and what they are doing to reduce their own risk.

We found that despite dramatic reports about ID theft, consumers still have a lot to learn and even more to do – to protect themselves from this crime. For instance, two thirds of consumers understand that their Social Security number is the key to stealing their identity, but nearly half of those same people were carrying their Social Security cards in their wallets.

As a result of the survey, we initiated a national campaign to make people aware of a few simple steps to take to prevent ID theft. The top three are:

Secure: Do not disclose personal information unnecessarily, especially the Social Security number

Study: Monitor all statements and view credit bureau reports

Shred: all discarded personal information

We also offer a full suite of products to help cardmembers protect themselves. But if an incident does occur, we have a free Id Theft Assistance center where trained counselors are available to literally walk our cardmembers through the restoration process.

Everyone has seen the reports, the funny commercials and the statistics that ID theft affects 10 million people a year. But what goes on behind the scenes is truly fascinating. And here is where I believe American Express has provided decades of leadership.

Because financial institutions are paying the cost of identity theft fraud, law enforcement agencies were initially reluctant to see the consumer as the victim. The dozens of hours that people lost in restoring their credit, the hours lost from work and the attorneys' fees required were hard to measure. In addition, ID theft is committed across state lines and across international boundaries. How do you establish jurisdiction, cooperation, and do something significant to stop the problem?

The answer is: form co-operative public/private partnerships. Because American Express has a closed system in which we issue and process credit card transactions all over the world, we have had an international fraud group in place for over 25 years. We learned that by detecting patterns and practices of fraud (not personal information but patterns) with government, law enforcement and industry partners, we could dramatically reduce fraud.

Let me give you two examples of innovative co-operation. In 1994, American Express saw a spike in fraud that was coming from rental car companies. Fraudsters were "dumpster diving" and finding credit card receipts that had date of birth, social security numbers and credit card numbers. We went to Avis and explained the problem.

We convinced them that all those receipts in their garbage cans were creating fraudulent customers who would not be inclined to bring the cars back. They really ran with the ball. They re-engineered their transactions so that the last two copies had no personal information. Their fraud plummeted. Within three years all the credit card companies had made this the industry standard and fraud from this source dried up almost entirely.

Likewise, the credit card industry, in the early 1990s, was hit by rings of thieves who were stealing credit cards out of the mail system. Again, American Express went to the Postal Inspection Service for help. They assembled a committee of financial service companies and banks to discuss the problem. Imagine all those competitors in one room.

Slowly we began to share best practices and trend data. It was discovered that much of the problem was in a few airports where mail was loaded onto planes. Even after the airport rings were broken up, the problem persisted. It was the brainstorming of this task force that came up with the idea of having cards authorized by calling an 800 number after people received them. The idea soon became an industry standard and fraud dropped 80% in this category.

To conclude, ID theft is a difficult, ever-changing, and frustrating problem with no easy or economical solution. Yet the industry has made great strides by working with the Postal Service, the FBI, the Secret Service, the Federal Trade Commission – and yes, even with competitors – to solve the problem. The on-line explosion has created new challenges. We all have to work together to protect our customers.

Gary Reynolds, Senior Vice President/Director of Financial Crime Investigations, Wells Fargo Bank

Recognizing that identity theft is one of the fastest growing crimes in the nation, the Financial Services Roundtable (www.fsround.org), the Banking Information Technology Secretariat (BITS) (www.bitsinfo.org) and 47 of the nation's largest financial institutions formed the Identity Theft Assistance Corporation (ITAC) in January of 2004. The ITAC's efforts are focused on easing the burden of identity theft on the victims.

From the BITS Financial Institution Voluntary Guidelines (The Financial Services Roundtable and BITS, 2003) the participating financial institutions agree to:

- Establish an internal system that provides victims a "single point of contact" within the financial institution.
- Provide each victim with educational materials to assist in preventing further instances.
- Utilize an industry – wide Uniform Affidavit.
- Send the completed Uniform Affidavit to other organizations, creditors, and law enforcement as appropriate.
- Establish a system for disseminating the Uniform Affidavit, as appropriate to law enforcement, industry organizations, and other creditors.
- While reserving the right to receive additional information from the victim, receive and use a completed Uniform Affidavit from other financial institutions.
- Upon receipt of a completed Uniform Affidavit, contact the victim to seek resolution of affected accounts within their own institutions.

The pilot program became operational at Wells Fargo and Wachovia in August of 2004. The other members are phasing in their active participation. As part of the program Wells Fargo created our own internal team known as Identity Theft Operations (ITO).

The goal of the ITO is to aid all Wells Fargo identity theft victims. One of the concerns customers have is to have to tell their story over and over as they are transferred from department to department. Each area of the institution that the customer has an account relationship asks the same questions and presumably is taking steps to protect the consumers' accounts. Any department in the pilot program who is notified by a customer of an identity theft problem is transferred or reported to the ITO. It is the job of the ITO to research all of the customer's business relationships and notify those departments of the identity theft and begin to protect all the customer's accounts. The customer has had to make only one call.

The ITO is a best practice from the Financial Services Roundtable, BITS, and the 47 participating financial institutions. There are two principle guidelines:

- A single point of contact at financial services companies to whom victims can report cases of identity theft, and
- The use of consistent forms such as a standard affidavit to record information about the fraud.

You don't have to be a victim of identity theft for personal information to fall into the wrong hands. In the course of a busy day, how often might you share information about yourself in person, on the phone, or over the Internet? Although it is impossible to guarantee that identity theft won't happen to you, there are ways to reduce your chances of becoming a victim.

Most victims don't discover the crime until it is too late. And it can take a long time to reverse the damage these criminals can do to your credit ratings. Any of these indicators could mean that you have become the victim of identity theft.

- Mysterious bills for accounts you are not aware of.
- Phone calls from creditors about delinquent payments that you don't recognize.
- Mail from unknown lenders asking for additional information.
- Monitor your account balances and activity electronically (at least once per week).
- Use e-mail – based account alerts to monitor transfers, payments, low balances and withdrawals and review your credit report (now available for free annual review).
- If you don't have access to online accounts, review paper bank and credit card statements monthly and monitor your billing cycles for missing bills or statements.

If you become a victim of identity theft notify law enforcement and:

- Notify your financial institution and ask if they have an identity theft assistance program (ITO). As discussed earlier, they will assist you.
- If you are going to handle the situation yourself

- Contact the three major credit bureaus and request a Fraud Alert be placed on your report.
- Contact the fraud unit of the company that opened the fraudulent account. Request copies of documentation related to the account, such as a copy of the contract, statements or transaction records, and signatures.
- Keep copies of all documentation. The investigating agency will need this documentation for evidence.
- Contact the police agency where the service or account was established. Most law enforcement agencies can only investigate crimes that happen in their city.
- If you feel any legitimate accounts have been compromised, contact the financial institution right away.

Avoiding identity theft is not simple but there are several common sense things that consumers can do. The identity theft problem has been studied now for several years and there are some additional suggestions for consumers.

- ✶ Keep personal information in a safe place and avoid storing documents in easily accessible places like vehicle glove boxes or day planners.
- ✶ Don't give your social security or account numbers over the phone to anyone who has called you, or to anyone you don't know. (Don't be afraid to ask why your information is needed and how it will be used).
- ✶ Shred documents that contain personal information (bank statements, credit solicitations, tax notices, etc.).
- ✶ Cancel your paper bills and statements wherever possible and instead check your statements and pay bills online.
- ✶ Refrain from carrying unnecessary information such as PINs, passwords, or Social Security numbers in your wallets or purses.
- ✶ Keep highly sensitive financial information (such as bank statements, log-ins for online banking accounts, ATM card PINs or paper checks) away from where others, including family members, friends, neighbors, and domestic employees, who could potentially access it.
- ✶ Retrieve paper mail promptly and deposit mail with sensitive information in a secure outgoing mailbox.
- ✶ When responding to e-mail from financial institutions, ignore any Internet links provided and type the known address instead.
- ✶ Use and regularly update firewall, anti-spyware, and anti-virus software.

Companies expend significant resources for detecting fraud. Victims are actually the first to detect fraud in a majority (54%) of cases. Consumer safety is significantly determined by the decision regarding how to manage personal finances. (Javelin Strategy & Research 2005). "Identity theft affects all financial institutions and causes serious harm to their customers. The financial services industry is taking steps to curb the growth of this kind of crime and to assist those who may fall victim to it." (The Financial Services Roundtable and BITS, 2003)

Tom Sullivan, Director, Merchant Risk Council/ Director of e-Commerce, Expedia

One of the big challenges merchants face today is consumer fear generated by the confusion between "identity theft" and "credit card fraud." This is driven largely by the combining of these two types of fraud in crime reporting by the FTC and law enforcement, and by media's coverage of true identity theft victims - people who may suffer for years trying to get their credit records repaired from credit accounts fraudulently opened in their names. While being a victim of fraud is always a serious incident, the reality is that the majority of fraud merchants and consumers experience is not identity theft, but rather is credit card fraud or the use of someone's credit card number or card plus name and address to make fraudulent purchases. In these cases, the fraudsters are not overly interested in the consumer's identity except for the purpose of providing enough information to facilitate the acceptance of the credit card. The fraudsters will cycle through credit card numbers, looking for valid cards with available credit and will make purchases until the card no longer works. They will then move on to the next card number. As was pointed out, in most credit card fraud cases one call to the bank and the completion of a form or statement by the victim will remove those charges from their account. Identity theft, the focus of today's conference, is the use of someone's personal information to establish new lines of credit or take over an existing line of credit. The problem with the 10-million victim "identity theft" figure we've heard about today as reported by the FTC is that it doesn't distinguish between these two types of crime. So while the total number of victims of both crimes is probably understated – all credit card fraud victims probably don't report the crime; the number of true "identity theft" victims is certainly overstated by including cases where just a credit card number was used.

Shopping online is safe. There are studies showing that it's safer than shopping offline because on-line merchants generally take protection of personal data more seriously, and they have more incentive to protect themselves and consumers against fraud. This is because on-line merchants are fully liable for losses due to fraud while off-line merchants are not, assuming they take minimal steps to protect themselves.

So what does fraud cost on-line merchants? There are a number of industry studies done annually, with results ranging from 0.3% to 2% of sales being fraud. The large on-line merchants who are paying close attention to the problem are probably seeing between sub-0.3% to 0.5%, which is billions and billions of dollars. Smaller and medium-sized merchants and some larger merchants in higher risk categories, such as gambling and pornography, represent the higher end of these studies. I looked at some of our data to see how California stacks up against other states for our online business. I found that San Francisco, Los Angeles and Anaheim are three of our worst cities for where fraud is committed. California cardholders also look to be victimized at a slightly higher rate than other states.

Merchant size generally dictates how fraud is managed. In our three companies – Hotels.com, Expedia and Hotwire – we have more than 40 people dedicated to preventing fraud. Mostly they are manually processing transactions, which have been flagged as high risk, looking for the suspicious ones, contacting financial institutions and consumers to insure that the transactions are authorized. Smaller merchants simply can't dedicate those types of resources to the problem. True identity theft has made the process of identifying fraud more difficult. Four to five years ago you could simply triangulate on name, address, and phone number data – if all matched then chances were very good that the transaction was good. Today that's no longer the case because the fraudsters have more real information about the cardholder. As a result we have to change our methods for preventing fraud.

Prevention means different things. Small merchants may look at every single transaction and call the bank or card company to ask if they authorized the transaction. Medium and larger merchants can't do that. So there are third-party services you can use that return a "risk score," similar to a credit score, on which they can then base their decision to manually review a transaction. Larger merchants, like us, have developed homegrown predictive models. We take every aspect of a transaction and run them through these models based on what fraud looks like to us. On average a merchant will flag 10% of transactions. When you have a lot of transactions – we have more than 75,000 per day – that means you have a lot of people doing nothing but looking at these flagged transactions and the vast majority of the time, more than 80%, the transactions is perfectly legitimate. It's just the way the customer made the purchase that made it look more like fraud. If you're selling travel, it may be that they are traveling the next day. If you're selling computers it may be that you want 5 laptops. What's clear is that the cost of managing the problem is a multi-million dollar investment, in addition to the losses due to fraud – you can't eliminate the problem without dramatically affecting sales. You can only manage it.

As merchants, we put most of our efforts into prevention, but most merchants also dedicate some resources to gathering data, finding fraud rings, and going after the larger frauds that we're seeing. There are difficulties with that from our perspective. It's not really clear to law enforcement who's the victim: the cardholder, the merchant, or the financial institution. It raises jurisdictional problems that aren't easy to deal with. I also sit on the board of a group called the Merchant Risk Council, which has 7,500 members including the top 50 or 60 e-commerce companies. We try to gather data collectively so that when we reach out to law enforcement, we can offer a much larger case. We know that these frauds are crossing over between travel sites, between travel and retail and other companies. We work with law enforcement to try to solve some of these problems –the FBI and local law enforcement take the lead on physical goods fraud, and we work with the Secret Service and local law enforcement on digital goods fraud. I wouldn't say we've had overwhelming success, but there have been several highly successful cases, and the cooperation between the MRC and law enforcement is improving every day. It's a great story.

In closing, there are things consumers should do to protect themselves. If you've made a purchase and you get a call asking you to confirm the purchase, don't be alarmed. We won't ask for any personal information, so just confirm it if you made the purchase. Don't pay cash for something you know you shouldn't pay cash for. There are a lot of schemes. If it looks too good to be true, it is too good to be true.

Not all criminals are stupid, and the smart ones are becoming more sophisticated. There are phishing schemes that capture personal information that are scary. As consumers, you always have to be on the lookout, asking the question "is there a legitimate reason this bank or this merchant needs this information?" Most financial institutions and merchants will avoid asking for any information via email. If you're in doubt, pick up the phone and call them.

Government Perspectives

Patrick Henning, Director, Employment Development Department

Background on EDD

Benefit Programs: Provide income replacement benefits to individuals who have lost their jobs, or are not working because of an injury or illness, or are taking time off to care for a family member or bond with a new child.

Payroll Tax Collection: The primary employment tax collector for the state, collecting Unemployment Insurance (UI), Disability Insurance (DI), Employment Training Tax (ETT) payroll taxes, and Personal Income Tax withholding from California Workers' pay checks.

Employment and Training Programs: Provide job services that match job seekers with job openings. Also administer the federal Workforce Investment Act and Employment Training Panel program, federal programs to provide job training and assistance at the local level.

In administering the EDD's programs, EDD collects and maintains confidential wage records on approximately 15 million workers, employer records on over 1 million employers, and UI and DI claim information on over 3 million unemployed or disabled workers.

UI Fraud Overview

While identity theft continues to rise across the country and remains a major issue of concern for both the private and public sector, Unemployment Insurance Imposter Fraud in California became prevalent in early 2002. Imposter fraud occurs when someone other than the legitimate worker establishes a fraudulent UI claim using a legitimate worker's Social Security number (SSN), personnel and wage information. Identity theft and UI fraud is an important issue for EDD and we have taken many successful steps to detect and prevent fraud so that we can protect employers' reserve accounts, consumers' confidential information and the integrity of the UI program. Through our continued cooperation with the employer community, state, and federal organizations, EDD continues to actively profile new fraud schemes through the use of various mechanisms in order to combat UI fraud.

In most cases of UI fraud, we have linked the identity theft with the theft of payroll records from employers or payroll processing companies. Perpetrators have been known to obtain this employment and identity information through "dumpster diving" and similar techniques. Most recently, these perpetrators have also obtained confidential data from other types of businesses that commonly deal with credit card applications, business memberships, and enrollment applications used by mortgage companies, auto malls, video rentals etc.

Measures to prevent, detect, and prosecute UI Fraud:

- Social Security Number Verification – During the initial claim filing process, UI records are cross-matched with the Social Security Administration's (SSA) records. If an SSN is not verified with SSA, further investigation takes places to verify identity and subsequent claim eligibility.
- Identity (ID) Alert Process – If EDD receives information from employers/employer's payroll agents, EDD's Investigation Division, or during claim filing that an individual's identity may be compromised or is potentially being misused, the claim is flagged for additional follow up with the applicant. In addition, information is mailed to base period employers and the last employer, in order to resolve the identity issue before authorizing any payments on the claims.

- Initial Claimant Screening – The Department implemented new screening procedures during the claim filing process to better authenticate the identity of claimants and to ensure only the true owner of the identity will receive UI benefits.
- Internal data matches are initiated in order to determine the identity of a claimant when filing a UI claim. Such cross-matches include matching base period employer wage information, prior UI or Disability claim information, date of birth and gender matching.
- EDD offers a 1-800 Fraud Hotline for reporting allegations and we recently launched an Internet fraud-reporting feature on our EDD home page.
- EDD has also initiated an Internal Anti-Fraud Workgroup that continuously evaluates the effectiveness of existing anti-fraud systems, identifies enhancements, and is researching new methods for detecting, deterring, and preventing UI fraud. Currently, EDD is exploring ways (data mining tools) to actively identify patterns, data elements, and trends to detect and prevent potentially fraudulent UI claims earlier in the process. With these tools, EDD has been able to stay current on recent fraud schemes and continually update and improve our fraud prevention processes. Recent UI identity theft schemes used a hierarchy of co-conspirators who stole payroll documents, filed fraudulent UI claims via telephone, rented numerous P.O. boxes, and cashed the fraudulent UI checks at local markets in the Central Valley (Please see Attachment A for more information).
- EDD continues to work closely with the employer community, other states as well as state and federal partners to investigate and prosecute perpetrators. In 2001, EDD's Investigation Division noticed a number of claims filed with similar traits within a specific geographic location, namely the Central Valley. Two major Central Valley cases in the Fresno area involved: (1) the illegal acquisition of payroll and personnel records of approximately 400 employers and 50,000 employee Social Security numbers; and (2) misuse of Post Office (P.O.) Boxes and business bank accounts. The Department worked closely with both federal and local law enforcement agencies to bring about prosecution. To date 22 individuals have been prosecuted. Extensive media attention was given to both of these cases and as a result, various employers throughout the state have immediately notified the Department whenever they believe their records have been compromised.

  Most recently, states such as Washington and Pennsylvania have contacted the Department to inform us of fraudulent claims being filed using out of state employers with the fraudulent claim containing a California Central Valley residential and/or P.O. (P.O.) Box address.
- Employer education and outreach – EDD meets with various employer groups across the state to provide information on the need for employers to protect their confidential payroll records from theft or disclosure, and to actively manage their UI accounts to identify claims that are fraudulent.

  From April 2003 through May 2004, EDD conducted a targeted marketing campaign to California employers and the public about UI fraud. Brochures were developed to assist employers in preventing UI fraud while controlling their costs as well as informing employees/individuals about how to protect their identities and prevent UI fraud. These brochures are located on our EDD Web site. This marketing campaign included conducting press conferences and multiple educational mailings to employers, enhancing the EDD Web site with fraud prevention materials, and featuring articles in the California Employer as well as other publications.

  The Department is aggressively pursuing these perpetrators through the continued cooperation from the public, the employer community, and both State and Federal law enforcement agencies.

William P. Wood, Acting Commissioner, Department of Corporations

Online escrow fraud is a new and growing problem on the Internet. It both requires ID theft to start up, in many cases, and is also used as a mechanism to steal ID. It is a significant concern of the Department of Corporations because it involves activity that is required by law to be licensed by the Department.

First, some background on the Department:

The Department of Corporations is California's investment and financing authority. We regulate and license a wide variety of businesses that affect the lives of Californians every day. We are responsible for the regulation, enforcement and licensing of securities, franchises, off-exchange commodities, investment and financial services, independent escrows, consumer and commercial finance lending and residential mortgage lending.

This diverse and wide ranging portfolio means that in 2004 my Department regulated about 3,400 broker-dealers, 225,000 agents and registered representatives, 2,900 investment advisers. And 31,000 investments adviser representatives.

What is an online escrow company?

Online escrow companies are used to pay for items found through online auction sites and marketplaces that advertise classified ads, usually for expensive items like computers, electronics, cars, and jewelry. Some Internet auction sites, like eBay, recommend that their users pay for purchases over $500 through an online escrow company.

Escrow providers help prevent fraud by acting as independent third parties between buyers and sellers. After the escrow company receives the buyer's check, money order or credit card payment, the company notifies the seller to ship the purchase to the buyer. The escrow company does not forward the buyer's payment to the seller until the buyer receives the item. Buyers usually pay the escrow service fees, which are generally a percentage of the purchased item's cost.

How are online escrow companies licensed and regulated in California?

Persons or companies performing escrow services over the Internet in California, or performing escrow services for consumers in California, must comply with the licensing requirements of the California Escrow Law. The licensing and regulatory process ensures that companies' owners and key employees have been subject to background checks performed by the California Department of Corporations, that the company's financial condition and records are adequate, that the company is properly bonded, and that all customer funds are segregated in trust fund accounts until the terms of the escrow are met.

How many escrow companies are licensed by the Department of Corporations?

There are about 650 independent escrow companies in California licensed by the Department of Corporations. The Department licenses only one online escrow service: www.escrow.com.

How are fraudulent online escrow Web sites set up?

Stolen identities and credit card numbers are used to open a Web hosting account, and the scammers upload content files to the Web hosting server to create a fake escrow service Web site. Sometimes a phony escrow company site can be detected by it sloppy content, with spelling and grammar errors and inconsistent information. Other times, the site's information may have been copied from legitimate escrow company Web sites.

Fraudulent escrow company sites often claim to be licensed by the California Department of Corporations and may provide a link to the Department's Web site. The sites use a phony license number or use one of the Department's current licensee's license number and address.

Fake escrow company sites often display logos from the Better Business Bureau, VeriSign Secure, TRUSTe, and even the Internet Fraud Complaint Center.

When fraudulent escrow company sites are detected and shut down, the scammers copy the defunct site's files and create a new site, changing little more than the domain name, and are quickly back in business.

How do fake online escrow companies victimize consumers?

The scammers trick online auction or classified ad buyers by setting up phony auctions or posting fake ads. The "seller" tells the interested buyer to use a particular online escrow company to complete the transaction. The buyer sends the payment to the phony escrow services site, but never receives the promised merchandise in return.

Sellers can be victims, too. The scammer may pose as a "buyer" or the winning bidder in an online auction and tells the seller to use a particular online escrow company. The seller receives an e-mail from the fraudulent escrow company indicating the buyer has sent the payment to the escrow company. The seller ships the merchandise to the address provided by the scam artist – often a hotel lobby or mailbox rental store – but never receives payment.

How widespread is fraudulent online escrow activity?

The Department has taken enforcement actions against 46 Internet escrow providers to shut down fraudulent escrow sites since May 2004. None of these online escrow companies applied for licenses to operate legitimately in California. This is a continuous monitoring effort by the Department of Corporations, as well, as other government agencies. To get at the widespread abuse of online escrow services, a coordinated state and federal effort is necessary.

In December we formed such a coordinated response, the Online Escrow Fraud Task Force.

Who are the members of the Online Escrow Fraud Task Force?

Members include the California Department of Corporations, Federal Trade Commission (FTC), Federal Bureau of Investigation (FBI), Los Angeles County Sheriff's Department's Southern California High Tech Task Force and Escrow Institute of California.

How much money is lost in California due to fraudulent online escrow activity?

It is very difficult to determine at this point but we hope that the combined resources of the Online Escrow Fraud Task Force may get a better sense of the loss. Right now we do know that there are literally hundreds of fraudulent and/or unlicensed escrow sites online. The Task Force members suspect that the losses could be very significant and involve thousands of people.

What is the purpose of the Online Escrow Fraud Task Force?

The Online Escrow Fraud Task Force will coordinate information and fraud prevention programs between state and federal regulators, law enforcement, industry groups, and businesses. This exchange of information will assist in the effective and rapid detection, prevention, investigation, and prosecution of escrow fraud in California.

The Department of Corporations, as the state regulator of escrow companies, will help coordinate communications among Online Escrow Fraud Task Force members to share information or ask questions. The task force will also make timely announcements about enforcement actions and consumer alerts.

What can California consumers do if they think they've been taken by an online escrow scam? How can California consumers protect themselves against online escrow fraud?

If you think you've fallen victim to an online escrow scam, you should file a complaint with the California Department of Corporations. Complaint forms can be found at **www.corp.ca.gov**, or call 1-866-ASK-CORP (1-866-275-2677) to have a complaint form sent to you.

Californians can call the California Department of Corporations toll-free to make sure the online escrow company or any escrow company you plan to use is properly licensed.

You should also file a complaint with the Internet Crime Complaint Center (IC3) by going to http://www.ic3.gov. The IC3 is a partnership between the FBI and the National White Collar Crime Center created to address fraud committed over the Internet.

If you've given personal information such as your bank account or credit card number to a fraudulent Internet escrow company, you need to take steps to resolve potential identity theft-related problems. The California Department of Consumer Affairs' Office of Privacy Protection offers information about what to do if you believe you may be a victim of identity theft: http://www.privacy.ca.gov/cover/identitytheft.htm.

Joanne McNabb, Chief, California Office of Privacy Protection, California Department of Consumer Affairs

The California Office of Privacy Protection's Role in Fighting Identity Theft

The California Office of Privacy Protection was created by legislation enacted in 2000, and started operation in November 2001.

Statutory Purpose of the Office of Privacy Protection

The enabling statute provides that the Office's purpose is "protecting the privacy of individuals' personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy area and facilitating the development of fair information practices…" (Business and Professions Code § 350a)

Identity Theft Specifically Mentioned in Statute

- Assist consumers with privacy complaints – including identity theft
- Assist law enforcement in the prosecution of identity theft and other privacy-related crimes

Functions of COPP: How We Carry Out our Mandate

CONSUMER ASSISTANCE

Identity theft is the most common topic of contacts to the California Office of Privacy Protection, representing 61% of total calls and e-mails. Most of those calls are from people concerned about identity theft, but 9% are from victims.

Some have just discovered they're victims: Maybe they got a call from a debt collector or maybe they saw something on bill or bank statement that wasn't theirs. Some (0.33%) found out when they were arrested.

Others have been wrestling with clearing it up for some time and have hit a roadblock and need help.

The next biggest category of calls (11%) is about privacy laws and practices. For example, many people ask, "Isn't there a law that says a company can't ask for my Social Security number?" Our answer is no, there isn't and you don't have to give your SSN, but you may not get what you want. We encourage people to ask questions whenever they're asked for personal information that seems to them to be inappropriate to the transaction. Why do you need it? Is there an alternative? What will you do with it? How will you protect it? If you can't negotiate something you're satisfied with, consider taking your business elsewhere. People also call to complain that a particular company isn't truncating credit card numbers on receipts or is collecting additional personal info on credit card transactions. We send a letter in such cases, informing the company of the complaint and enclosing a copy of our California Business Privacy Handbook.

CONSUMER INFORMATION AND EDUCATION

Our Web site is our primary channel for information and education. It contains information for consumers, business and law enforcement, including California and federal privacy laws and pending California privacy and identity theft legislation. There are Web pages dedicated to Identity Theft, Online Privacy, Financial Privacy, Social Security Numbers, and Health Privacy, all of which contain our information sheets and links to additional resources.

We have published 10 consumer information sheets, providing information in plain language at an eighth-grade reading level. Five of the 10 information sheets are on aspects of identity theft.

- Top 10 Tips for ID Theft Prevention
- Identity Theft Victim Checklist
- Your Social Security Number: Controlling the Key to ID Theft
- Guide for Victims of "Criminal" Identity Theft: How to use the registry
- How to Freeze Your Credit Files

In addition to the Web site, we also conduct consumer workshops and make presentations at community meetings. Last fiscal year we spoke to consumers at 38 such meetings, with an average attendance of 81.

COORDINATION WITH LAW ENFORCEMENT

COPP's primary role in coordinating with law enforcement has been to offer victim assistance, helping to free up law enforcement officers to conduct investigations. Identity theft victims have a lot of work to do and need frequent communication and assistance in wending their way through the process of clearing up their records.

We provide law enforcement with basic information for victims on a Law Enforcement Web page. In response to a request from law enforcement, we developed forms to facilitate victims' (and law enforcement's) access to applications and other records on accounts opened or used by an identity thief. Originally developed when Penal Code § 530.8 first went into effect in 2002, we've just updated the form to reflect the new federal law on this issue enacted with the 2003 amendments to the Fair Credit Reporting Act.

The Office also has a statutorily designated membership in the High-Tech Crimes Task Force Advisory Committee, and we work with the five regional task forces in various ways.

RECOMMENDED PRACTICES

Eleven percent of the calls and emails to the California Office of Privacy Protection this fiscal year have been from business and government, up from 5% in the first years. These callers are generally asking about new California privacy laws.

COPP periodically issues Recommended Practices documents, in accordance with the statutory requirement to "make recommendations to organizations for privacy policies and practices that promote and protect the interests of CA consumers"(Business and Professions Code § 350(c)). These recommendations are usually in relation to new laws, but they are not legal interpretations or regulations. They are written from a "best practices" perspective, with the input of an advisory group for each project. The advisory groups are made up of representatives of the different stakeholders interested, including consumer and privacy advocates.

The following Recommended Practices have been issued to date and are available on our Web site:

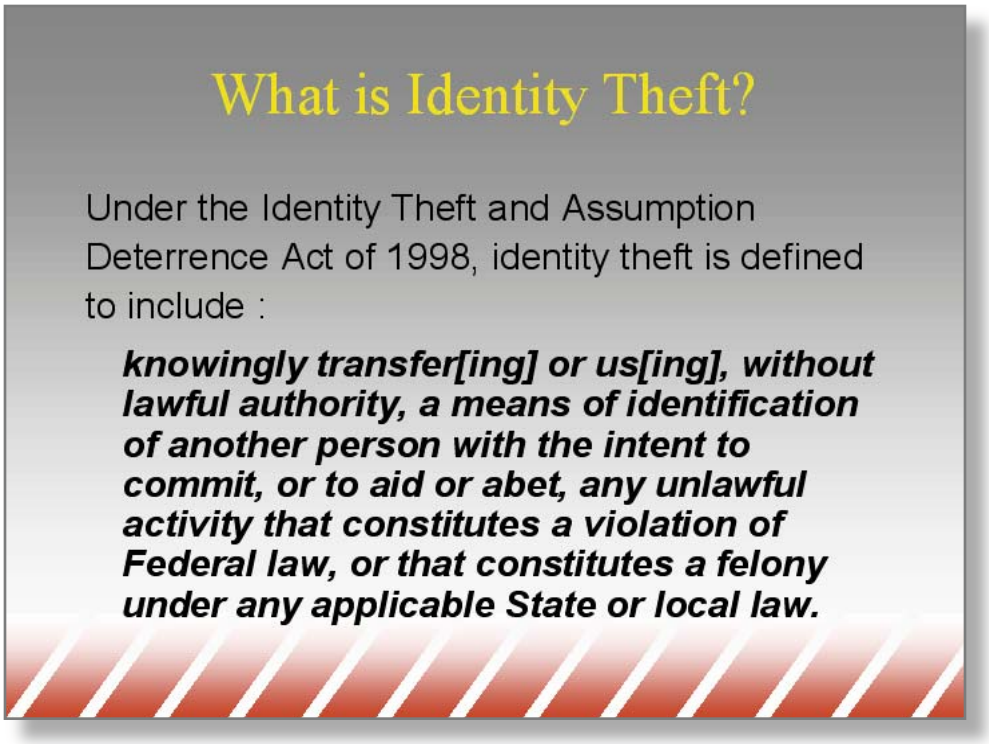
- Protecting the Confidentiality of Social Security Numbers (2002; rev. 2003): These recommendations could be applied to protecting any sensitive personal information.
- Security Breach Notification (2003): These recommendations cover prevention, preparation and notification and include sample notice letters.
- Info-Sharing Disclosures & Privacy Policy Statements (2004): These recommendations address providing information on how a company shares customer personal information for marketing purposes and also the larger issue of writing effective privacy policy statements.

We have also published a California Business Privacy Handbook, developed to help educate small and medium-sized businesses on how they can prevent identity theft. It presents basic privacy laws and good practices in a simple "Dos" and "Don'ts" format, with references to laws and additional information resources.

We conduct educational workshops for business and government and speak at organizational meetings. Last fiscal year, we made presentations at 52 business or government events, with an average attendance of 77. So far this year, we've spoken at 30 with an average attendance of 121.

In addition, we provide input to the State CIO and ISO on privacy and information security policies and practices for state agencies.

ID THEFT
The Federal Trade Commission's
Identity Theft Program


What is Identity Theft?
Under the Identity Theft and Assumption Deterrence Act of 1998, identity theft is defined to include :
knowingly transfer[ing] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

"Means of Identification"

Any name or number used to identify a specific individual, including:

- Name, SSN, DOB, driver's license number, credit card number, passport number, EIN
- Biometric data
- Telecommunication identifying information or access device

ID Theft Act directed FTC to:

- Log receipt of complaints
- Provide informational materials to victims of identity theft
- Refer complaints to appropriate entities

FTC's Identity Theft Program

- Toll-free phone number for complaints
  877-ID THEFT
- Consumer education materials
  - Web site: www.consumer.gov/idtheft
- Identity Theft Data Clearinghouse – the federal government's centralized database of ID Theft complaints

Identity Theft Data Clearinghouse

- Federal government's centralized database of identity theft victim complaints
- Sources: FTC Hotline, online complaint form, Social Security Administration
- Contents
  - victim contact information
  - suspect information: name address phone relation
  - description of crime, details
  - which financial institutions were involved
  - police report number, department name
  - what types of accounts were taken over & where

Consumer Sentinel Network

- Identity Theft Data Clearinghouse
  - available to law enforcement nationwide
  - through a secure website
  - helps investigators:
    - Spot & investigate identity theft problems
    - Coordinate with other law enforcement officers in multijurisdictional cases

What Should I do?!?

Our law enforcement database is only useful if it is comprehensive so:

REFER VICTIMS TO

877-ID-THEFT

Consumer Education and Victim Assistance

- Phone counselors staff our hotline from 9:00 A.M. – 8:00 P.M. Monday- Friday
  1-877-IDTHEFT
- Secure online complaint form available at: www.consumer.gov/idtheft
- By mail: Identity Theft Data Clearinghouse
  600 Pennsylvania Avenue, NW
  Washington, DC 20580

Gregory Campbell, Assistant Inspector in Charge, San Francisco Division, U.S. Postal Inspection Service

What is identity theft and how is the Postal Inspection Service involved?

Identity theft involves acquiring key pieces of someone's identifying information, such as name, address, birth date, Social Security number or mother's maiden name. in order to impersonate them. The information enables the thief to commit numerous forms of fraud, which may include taking over a victim's financial accounts, opening new bank accounts in a victim's name, purchasing automobiles, applying for loans, credit cards and Social Security benefits, renting apartments, and establishing utility or phone services. Most identity theft involves the use of an address. Postal Inspectors get involved when the criminal activity takes place through the mail, such as the fraudulent application for credit cards submitted through the mail or if the personal information is stolen from the mail.

How big of a problem is mail theft?

In fiscal year 2003, Postal Inspectors made 6,089 arrests for mail theft offenses and recorded 5,456 convictions. Common targets for theft are anything of negotiable value, including credit cards and other financial information, and government checks in the mail. Cash sent in greeting cards, parcels containing valuable items, and postal remittances are also attractive to mail thieves.

Volume mail thefts, or volume attacks, included as their targets postal vehicles, collection boxes, apartment mailbox panels, relay boxes, carrier cart-satchels, co-op box units (NDCBUs and CBUs) and carrier robberies.

	Arrests	Convictions	Volume Attacks
FY 2003	6,089	5,456	8,254
FY 2002	5,175	4,579	9,109
FY 2001	5,603	4,666	6,752
FY 2000	4,942	4,120	3,929
FY 1999	4,285	3,858	3,435

Who is stealing the mail?

We have seen an increase in gang-related mail theft. Gangs will steal from residential mailboxes, but prefer to hit postal delivery vehicles, collection boxes or apartment boxes, where larger volumes of mail tend to be concentrated. For the most part, the thefts are the work of organized groups. Certain gang members steal the mail, others create bogus identification and still others negotiate checks.

Many of the internal losses, which occur in the distribution chain before delivery, involve theft by airline ramp clerks, private delivery drivers, mailroom clerks working for the banks, and postal employees.

Is this a serious criminal offense? What are the penalties?

Theft or possession of stolen mail is a very serious offense (18 U>S>C> 1708), punishable by up to five years in prison and fines of up to $250,000.

What are these crooks looking for?

Thieves may be after Social Security checks, income tax refunds, public assistance checks, credit cards, credit card convenience checks or other valuables. Even the financial information on a bank statement, for example, could enable a thief to order blank checks on a checking account.

Outgoing mail also can be very attractive – especially checks. Stolen checks can be "washed" with chemicals, obliterating the original handwritten payee and amount, and then filled in by the crook for a larger amount, payable to an assumed name.

Consumers should check if their banks are using a check printer that takes advantage of new kinds of ink and paper that help prevent check washing. Stolen checks may also be counterfeited with the use of computer software programs, a personal computer, scanner, and printer.

Are there any new trends in mail theft?

Theft of financial account statements from the mail, both incoming and outgoing, contributes to the growing problem of identity theft or account takeover fraud.

Another trend in mail theft involves organized mail gangs who steal valuable items form the mail. Personal information, such as bank account numbers, Social Security numbers or dates of birth, is stolen from the mail and used by mail theft gangs to conduct fraud.

What security measures have been put into place?

The Postal Inspection Service helped develop a high-security, modified "arrow" lock to reduce the threat of counterfeit keys that can access letterboxes, and there has been increased emphasis on the use of security locking bars on collection boxes to prevent forced entry. The Inspection Service has also developed High Security Collection Box Units (HSCBUs) for use in high-risk areas.

High-risk cities are also "hardening" NDCBUs to deter prying. In other cities, collection boxes have been reinforced to defeat thieves. Neighborhood watch groups have been enlisted in some areas to help keep an eye on postal delivery trucks while carriers are walking their routes.

In April 1996 the Postal Service instituted a "Move Validation Letter." When a customer submits a change=of-address form, the Postal Service sends a letter to both the new and the old address, advising that a change of address has been received. If the change is invalid, the letter instructs the customer to contact a local post office immediately. Unfortunately, changes of address may be submitted to a bank or credit card issuer, bypassing the post office verification.

We have partnered with credit card and law enforcement groups in the Financial Industry Mail Security Initiative, a working group that in addition to analyzing crime trends and possible solutions and reviewing credit card mailing programs identifies and implements solutions to reduce the problem of identity takeover fraud. The group produced a fraud detection and reference guide. Also Inspectors use the information from credit card thefts to identify "hot spots" for attention and can notify the credit card issuers of ZIP Code areas that are suffering abnormal losses, so they can take extra precautions if they are mailing into those areas.

Credit card activation, which was first proposed by a Postal Inspector, has helped reduce losses tremendously by removing the value form the card until the account holder has received it and called in a pre-arranged code to activate it.

The Postal Inspection Service has been working with the airline industry to improve mail security by developing proactive prevention efforts at airport facilities. The Postal Service requires airmail transportation contractors and subcontractors to perform pre-employment screening of all employees hired after March 1996.

What are some of the things people should do to prevent mail theft?

1. Safeguard financial information, especially your Social Security number, account numbers and statements. Be careful when disposing of credit card receipts and pre-approved credit card solicitations.
2. Retrieve mail as soon as possible after delivery to the mail receptacle.
3. If a mail receptacle has a locking device, make sure it works. Apartment boxes should be maintained by the landlord.
4. If expecting a check or credit card but unable to be at home when it is delivered, have a trusted friend get the mail.
5. Report any suspicious activity to local police or Postal Inspector. Suspicious activity may be someone following the letter carrier, attempting to break into a postal vehicle or tampering with the mail.
6. Report non-receipt of valuable mail as soon as possible by calling banks, credit card issuers, and the Postal Inspection Service.
7. Use letter slots at the post office to mail letters or give them to your mail carrier.
8. Consider having blank checks mailed to a bank for pick-up.
9. Report mail theft by completing PS Form 1510, Mail Loss and Rifling Report, or PS From 2016, Mail Theft and Vandalism Complaint at any Post Office or by calling 1-800-ASKUSPS.
10. Obtain Label 33 from the Postal Inspection Service and affix it to your mailbox. The sticker warns that willful damage to mailboxes and theft of mail are crimes.
11. Keep your mailbox in good repair and make sure it's properly installed. This may help prevent theft of the box itself.

It is extremely important that individuals report the theft of any correspondence to the Postal Inspection Service, because the reports help Inspectors identify problem areas. Postal Inspectors have a standing reward offer of $10,000 for information leading to the arrest and conviction of anyone stealing mail or possessing stolen mail.

Consumer Perspectives

Tracey Thomas, Identity Theft Resource Center

My story began in 1999, when the company signed us up for health insurance. I told my company I didn't want to use my Social Security number for my healthcare identifier. They told me I had to talk to Aetna. I did, but was unable to get them to use another number. So reluctantly I allowed them to use my SSN. About six months later I found myself in an emergency room, where I gave my health plan card to the admitting nurse, who wrote down my information and stole my identity with it.

She opened credit card accounts, rented an apartment, got cell phones, you name it; she racked up about $50,000 in my name. I discovered it when I was trying to buy my first home, and my credit report came back showing my credit as destroyed.

You've heard of the experience of cleaning up identity theft described as a nightmare. That's only half the story – it's a recurring nightmare. Especially back in 1999-2000, when you had almost no tools to help clean this stuff up. The only tool available at that time was to put a fraud alert on my credit files. A fraud alert, I was told by the credit bureaus, would require banks or others requesting my credit file to call me before issuing credit. So I went about cleaning up my credit report and put on fraud alerts, then went on with my life. Three months later a brand new bunch of credit cards, utility bills started showing up on my credit history. So when I called the creditors and asked why they didn't see my fraud alerts, that's when I learned that while the fraud alerts are mandatory under federal law – that is credit bureaus are mandated to send them out – creditors aren't required by law to look at them. In the several years that I've had fraud alerts on my files, I've been contacted once. The thief got credit in my name and I got credit four or five times, with only once encountering a fraud alert. And that was the only tool to stop an identity thief five years ago.

So the cycle would just repeat. I would watch my imposter destroy my credit, then I'd clean it up again, and so it would go, on and on. And each time I'd take my new papers into my local sheriff's department, which was where my case was filed, and watch the stack of papers grow. There was one white-collar crime investigator in the county and he had about 250 cases at a time. So there was no hope in stopping my imposter and no hope of getting her arrested.

So I decided to do my own investigation and find my imposter. I ended up finding her and presented her profile to my law enforcement investigator, who found out that she had a prior conviction for identity theft and who did go out and arrested her. Now the judge in my case gave her the strongest sentence he could under California law, six months of work furlough, so she could pay off her debts to me and to the credit card companies, work as a receptionist in a doctor's office.

So after that fiasco I worked as a volunteer with ITRC to get some legislation passed to give ID theft victims better tools to fight this crime and to prevent it in the first place. We got the credit report freeze law passed, we curtailed the use of SSNs – Aetna would no longer be able to use my SSN as my medical ID number. We've gotten mandatory police reports. We've made a lot of progress, but we're still at the beginning and we need to do a whole lot more.

Robin Fifield, identity theft victim

In 2003 having just turned 20 years of age, my daughter was a full time college student, licensed cosmetologist, dedicated to her rigorous six-day-a-week gym workouts and had an active social calendar. She was bright, ambitious and outgoing with a wide, diverse group of friends. She was conscientious about her finances, her study habits, her appearance and her reputation to clients because she knew what she wanted in the future. Her plan at the time was to earn a degree in textile designs, eventually working within the fashion industry. She felt that somewhere down the road her diligence to fitness could be used to work with those physically challenged. This description is not to say that my daughter was perfect. But, as parents, my husband and I felt fortunate to have raised an independent thinker who had a great deal of common sense and realized that who she would be was in large degree up to her and the actions she took.

Then on March 20, 2003, two officers stood on the front porch of my house carrying what looked like several inches thick of case folios. They were looking for my daughter and stated that she was the victim of Identity Theft. I was told that for at least 18 months and perhaps longer than 2 years, one of my daughter's best friends had used her identity in the commission of felonies.

Identity theft was no strange term to me as I had been the victim of an individual who used my credit cards until they were at the maximum in 1995. The damage to my credit standing had taken years to recover. I have also been the victim of computer hackers who have retrieved my personal information to claim ownership of web domain names. These experiences alone had been unbelievably stressful, consuming huge amounts of time, energy and expense.

Questions from me were endless. Some could be answered specifically. Others could not.

The officers speculated that the accused had damaged her own record and perhaps thought that assuming my daughter's identity would be easy due to very similar appearance. They were both 6' – 6'1" tall, blonde hair, blue eyes, approximately 170 lbs. and similar body proportions. She also knew that my daughter had no criminal record. Outside of speculation, they only had the facts. The girl had used my daughter's full name, memorized address, license number, and other personal details.

The known felonies committed under my daughter's name initially were violations stemming from numerous DUI charges. There were others related to checks, banking, ATM use that were still under investigation. They could not provide me with any other specifics at that time other than to state that they required my daughter's cooperation in order to begin handling the charges appropriately.

Why had they never come to our house before if the accused had this alias for so long under such serious charges? They could only say that they were not certain of that answer entirely yet. Perhaps the girl had previously followed through on court appearances or paid fines. They also suspected that she had used other addresses perhaps to receive mail and no one ever made the connection until the last arrest. At that time, the individual had been pulled over for a traffic violation and was found to be intoxicated and in possession of an illegal substance. She had stated that her full name as my daughter's and her license number. However, during the booking process, the accused made an error in providing a correct birth date. She was then fingerprinted and was additionally charged with Identity Theft once confirmation was made through DMV records.

The really bad news was that the felony convictions that resulted left my daughter with an A.K.A. that associated her with this criminal. Just when I thought the officers were through telling me the "worst" that could happen

or had happened, they would add one more thing. What next? My daughter should not drive until everything had been "cleared up". To paraphrase their words, "Her friend is out on bail and it has come to our attention that additional warrants either already have or will be issued by other policing agencies. It is realistic to anticipate that she could even be arrested at home. Should your daughter be pulled over for a traffic violation, after running her license, the officer will consider her a dangerous felon and would draw their gun to arrest her."

These words were chilling and presented a very real threat to my daughter's safety. I wanted to know which courts had issued warrants and what could be done. They suggested that I start with L.A. County Sheriff's Department, the City of Compton, City of El Monte and City of Long Beach. If I found anything under my daughter's name outstanding, it would be best to address it immediately as well as any traffic or court related documents that came in the mail. The reason given for us to research this information was that we would know if an action had been brought was valid against my daughter or if it were caused by the perpetrator.

They continued by saying that if she gave her statement to the CHP in the Santa Fe Springs station and pressed charges, a letter could then be written stating that they had evidence of and had confirmed the identity theft. This letter would then go to a judge and have the court issue a Judicial Finding of Factual Innocence. This legal document, they explained, would then allow us to work our way through the situations arising from the perpetrator's use of my daughter's identity and would allow for such things as change of driver's license and social security numbers.

Painting a picture of my daughter and describing the events that initially took place in detail is necessary here in order to understand how the situations that followed affected those involved. Although the subsequent events will be condensed, having read the above, it is likely that the impact to our lives will be sensed. Suffice to say, this first day was only the beginning.

The very same day that we learned of the identity theft, several things took place:

Told my daughter the situation. Her reaction was:

- Disbelief, denial that her friend would do such a thing
- She wondered what she could have done to prevent this.
- Denial that situation required her to make a statement or press charges
- Feeling that since it wasn't really her that committed a crime the authorities would be able to clear things up for her.

Took the keys to my daughter's car away. One can imagine this initial scene and how it played out with a grown daughter, who had an independent life and busy schedule.

From this date, I began chauffeuring my daughter making every effort to maintain her schedule. This would eventually lead to stressful circumstances in trying to meet my own working commitments. It would be over 6 months before my daughter would drive herself again.

Using the Internet, went to the County of Los Angeles Sheriff's website www.la-sheriff.org. On Inmate Information Center page found reference to my daughter displayed publicly as an inmate. Record showed arrest for DUI Alcohol/drug w/priors noting 23152(A)VC. Potential for public humiliation and damage to reputation caused fear and depression.

- Record provided next court appearance in El Monte on June 24, 2003. Needed to investigate the charges there, any fines or associated warrants, etc.
- Pico Rivera was noted on the record and so investigated the same here. First checking with law enforcement and then checking courts for records.

Coincidentally on this day also received a notice to pay bail from the Compton Courthouse. Bail amount was $801.00 for violations 22343A 29 and 16028A 29.

- Called on Compton notice – advised that I needed to call Officer of Citation at this agency. Get name and I.D. and ask that officer to open an investigation for identity theft related to the citation.
- Getting them to tell me anything on this was impossible they said unless my daughter came down to get the information herself. If she did come, I was told outright that she would be arrested.

Using the internet and going to www.ca.gov searched and researched every code violation and read as much as I could through that first night on every law dealing with identity theft and/or the crimes committed using my daughter's identity. I used:

- The California Courts Section
- California Courts Self-help Center
- Court Administration
- Court Rules
- California Agencies, Departments and Commissions
- California Constitutions, Laws and Regulations

As days, weeks, months passed:

My daughter delivered her statement to the CHP Station in Santa Fe Springs 7 days after we were told. Three times, we drove over to this location for her to leave the statement but each time, she would not get out of the car until we finally talked through what the problem was.

- She revealed that the hesitation was fear of retribution from the perpetrator or those she associated with. Apparently the day before we had even learned of this, the "friend" had called the house. (Evening of March 19th). This was the day she was released. My daughter was surprised to hear from her because they had not been in contact much in the last year. This conversation was to "catch up" on what the other was doing. She told her that she was in Las Vegas and was not coming back to California. She said that she had met this "guy," he took care of her, and had a lot of money. Continued by saying she felt the man was into something "big" and she wondered if he were doing something illegal and then casually laughed it off.
- Although my daughter and I were very comfortable in conversations on any topic and she could freely speak of problems, she admitted that the news of identity theft made the telephone call seem ominous and far more threatening. This raised my level of fear but I did not let her know this. I just kept reinforcing the fact that she was doing the right thing and at this time was left with no other choice but to defend her own reputation.

- As parents our first concern was for our daughter's emotional well being in dealing with the betrayal of her friend. Many of her reactions were similar to those of a rape victim. In fact, we were eventually advised by Jay Foley of the Identity Theft Resource Center www.idtheftcenter.org that rape counseling seemed to be the most logically recommendation. No other organization offered such advice or direction throughout this ordeal.

With new information, began calling Las Vegas Law Enforcement Agencies to see if there were any records of a traffic or criminal nature for my daughter. Nevada had its own way of communicating and it would take months before we found that the perpetrator in California was using her identity in Nevada. The difference at this time was that she had received so far traffic citations that she actually was going to traffic school to clear!

- Used Nevada Department of Public Safety Records and Identification Bureau site located in the City of Carson City, Nevada
- Eventually spoke with the perpetrator's parents to find that they did not know their daughter's location or telephone number in Nevada, but knew she attended some traffic related class at a police station in Needles. This info was passed along to authorities to assist in apprehension.

Retrieved information from California Office of Privacy Protection Web site, www.privacy.ca.gov, regarding steps to be taken to guard against or handle various instances of identity theft. We seemed to be moving in the right direction.

Contacted all three major Credit Bureaus: Equifax, Experian, and TransUnion. Asked each agency to place a "fraud alert" on my daughter's credit report. One of the three had shown "unusual" activity. They all required the completion of affidavit packets.

Completed a form in accordance with the Federal Privacy Act '74 for the National Driver Registry (NDR)

Used the Los Angeles County District Attorney's Office Web site on Identity Theft. www.da.co.la.ca.us/cpd/idtheft.htm. Found a great deal of information and supporting documents to help me further the process.

- From there spoke to Los Angeles County Department of Consumer Affairs
- High Tech Crimes Unit, Los Angeles County District Attorney's Office
- Downloaded Identity Theft Pamphlet

Researched the very real possibility that we would have to change my daughter's name.

Utilized the www.anaheim.net site Identity Theft section – very helpful

- Contacted Anaheim Police Department's Fraud Unit

Utilized the Federal Trade Commission website www.ftc.gov

Utilized the U.S. Postal Inspection Service website www.usps.gov/postalinspectors

Researched how information available at the Social Security Administration www.ssa.gov

Contacted the Department of Motor Vehicles first by use of their website www.dmv.ca.gov and then by calling.

- Daughter's Driver's License is soon to be suspended.
- They were very helpful in advising various steps that should be taken in a case of identity theft
- Provided direction on where citations of concern had been issued against my daughter's record in the event that our address was not used and court documents were not received so that we could begin clearing record.

April 19, 2003 – Receive information regarding a premium due American Liberty Bail Bonds.

June 9, 2003 - Received a Failure to Appear notice from GC Services Limited Partnership, Collection Agency Division for failure to appear in Superior Court in California in the amount of $1,326.00.

- Hold was placed on driver's license.
- Civil Assessment $250 added pursuant to Penal Code Section 1214.1.
- Researched Penal Code using www.ca.gov site.

Met with the perpetrator's parents regarding information that they were holding on their daughter's vehicle and citations.

- Lien against impounded vehicle was jointly held in my daughter's name
- Vehicle had been sold through a lien process in accordance with DMV
- Parents had a copy of an additional citation signed by their daughter as my daughter on May 7, 2003 as well
- They also had original bail bond receipt with defendant's name noted AKA between the girls.
- We were provided these documents to assist with clearing my daughter.

July 7, 2003 – My daughter received Service Order for Suspension from the DMV

July 7, 2003 – Department of Consumer Affairs website – I read contents of a page titled 'California Identity Theft Law Goes Into Effect'. Within these pages is a link for consumers that ends up being our salvation www.idtheftcenter.org Identity Theft Resource Center

- Contacted by telephone Jay Foley of the Identity Theft Resource Center. Tell him our story and explain our feeling that we are getting nowhere in clearing this up because we have not received the promised letter from the CHP to even begin. Expressed that we were flailing in a sea of forms, legal structure and protocol over officiating bodies.
- Jay agrees to help and there are no words to describe how directed and confident this man and the organization made me feel. From this point on, we call him whenever we have any new information or whenever we are faced with a concern. The support was phenomenal.

July 8, 2003 – Received a letter with payment coupon from American Honda Finance Corporation regarding our insurance coverage for this car that my daughter had been driving.

- Had been notified by the insurance carrier that a driver with a revoked license was driving the vehicle and would soon be uninsured.

July 10, 2003 – Received notice of cancellation from 21st Century Insurance for the automobile insurance coverage for every driver in the household.

- Cancellation was due to the suspension of my daughter's license and the type of violations charged to her driving record. This affected four drivers in the house.
- We could have our insurance reinstated only if we signed an exclusion of Kellie from our insurance now, on future policies and with the understood amended clause that she would not ever be a driver of cars insured through them even if she obtained other coverage.
- According to the underwriting department, this exclusion would be very difficult to reverse once signed even with evidence. They took a rather harsh stance when we told them identity theft as though we likely conjured up a good part of what we were telling them.
- Informed them that we would not sign the exclusion and that we would use the two-week time frame that we were still insured to provide proof of innocence so that insurance could be retained.

July 14, 2003 – The Underwriter with 21st Century Insurance stated they cannot lift the exclusion of Kellie by simply referencing the tracking number provided by the Identity Theft Resource Center. They required a copy from the DMV upon completion of process.

DMV advises that the process for handling the information that comes to them and then providing the copy 21st Century requires will take a minimum of 3 months. Advised that it IS the process and there would just not be a way to handle this any sooner.

July 15, 2003 – Using the Internet went to the Office of the Attorney General for the State of California – Department of Justice – Identity Theft Resource Link. Reviewed Registry Application Process. Went through the six-step process, downloading all appropriate forms needed to follow through.

***July 17, 2003 – Finally* acquired a letter from Captain Jones, Commander of Santa Fe Springs CHP Station that was promised on statement delivery 3 months prior.**

- It took the intervention of Jay Foley to finally receive this letter.
- Gave a copy of this letter to my daughter to carry as a precaution.

July 21, 2003 – Completed the Identity Theft: Application for Registration as Victim for the Department of Justice in Sacramento.

July 21, 2003 – My Daughter received a letter postmarked this date from the Identity Thief. She had written to her from Santa Ana's Main Jail where she was being held for crimes unknown to us. In the letter she admitted to using my daughter's identity, expressing her regret for doing so and that fear of her own past drove her to do what she did. On the advice of Jay Foley with Identity Theft Resource Center, we scanned a copy of the letter then sealed it in a plastic bag. The original was then delivered

to the Los Angeles District Attorney's Office for Fingerprinting and verification of Identity Theft. Contacted DMV for an update providing them with this information as well. Provided a copy of this letter to all law enforcement agencies with pending investigations. Gave a copy of the letter to my daughter to carry as well as a precaution.

July 27, 2003 – Completed the Petition to Seal and Destroy Arrest Records

July 28, 2003 – Called the Department of Justice in Sacramento to get direction on Live Scan. Needed the local office information and directions for Kellie to be fingerprinted.

After being insured with 21st Century Insurance for our cars for over 20 years, they had made it so difficult for us to be believed with this ID theft situation that we shifted our coverage to Mercury Insurance Company.

***Jay Foley of Identity Theft Resource Center* met my daughter, my husband and I. (I'm sorry but I did not have a copy of this form here with me to tell you the date but it was approximately 6 months after we first found out) Together we went to court with all of the evidence that we had gathered. Mr. Foley stood by my daughter in the courtroom and made the request to sign the Factual Finding of Judicial Innocence. The Judge granted our request. Signing of this document allowed us to actually BEGIN clearing the damage.**

Over the next 6 months to follow, by use of this court document, we began to work our way back through the legal system, government system, financial system, and related information centers that store identity information releasing my daughter from the clutches of the identity thief. To this date, no one in our family has had any further contact with the perpetrator.

Beth Givens, Director, Privacy Rights Clearinghouse

Thank you for the opportunity to talk about criminal identity theft today. We at the Privacy Rights Clearinghouse call criminal identity theft the "worst case scenario" of identity theft for reasons that will become clear to you in my presentation.

I will over these four topics:

- *First, what criminal identity theft is.*
- *Second, some examples of individuals' experiences.*
- *Third, California's Identity Theft Registry, an attempt to ameliorate some of the harmful impacts of criminal identity theft.*
- *And fourth, I will close with recommendations involving, legislation, education, research, and state government responses.*

First, what is criminal identity theft?

Criminal identity theft occurs when an imposter gives another person's name and personal information, such as a Social Security number, driver's license number, and date of birth, to a law enforcement officer upon

arrest or during an investigation. Or the imposter may give to law enforcement a counterfeit driver's license or identification card containing another person's information.

In a typical situation, an individual stopped for a traffic violation, for shoplifting, or another misdemeanor, claims to not be carrying identification. He or she then gives the identifying information of another person to the officer. Often this information is of a family member, roommate, or friend.

In misdemeanor situations, the cited or arrested individual is usually released and told to appear in court when notified. The imposter does not appear in court, however, and at that date a warrant for the arrest of the innocent person is issued. The next time the innocent person – the criminal identity theft victim – is stopped for a broken tail light, the officer runs a search of the criminal records files and discovers the outstanding warrant. The victim is often brought to the police department and booked, even jailed.

Another typical scenario in which the victim discovers that he or she has a wrongful criminal record is when applying for a job – when a background check is conducted and the individual is denied employment. The inability to find work can go on for years.

Let me give you three such stories, from our files at the Privacy Rights Clearinghouse, and from the media.

- Mark is a 10-year Marine veteran with expertise in information technology. A decade ago when serving in Africa, his brother used his identifying information when arrested for traffic tickets and when convicted on felony charges in another state. Mark was recently laid off from a computer technology job and has applied for several positions for which he says he is eminently qualified. But none of the applications has resulted in an interview. One employer alerted him to two felonies and six misdemeanors uncovered in a background check. "Obviously," Mark told the PRC in an e-mail message, "no IT firm or professional organization would hire a felon to manage sensitive and confidential information." (From the PRC's files)

- The situation of Bay Area woman Stancy Nesby received considerable media attention in September 2004. Her purse was stolen in the late 1990s by someone who then used her identity when arrested for crimes. Nesby has since been detained six times, arrested four times, and jailed four times for five days on no-bail felony bench warrants naming her, even though a state judge determined that she was not the person arrested by law enforcement in 1999. In one arrest, her children were taken away and placed with Child Protective Services. She has had to hire an attorney to represent her and is suing the city of San Francisco for its failure to withdraw warrants. (Joyce Cutler, "Woman Sues City Over Arrests, Jailings Allegedly Spawned by ID Theft, Bad Warrants," BNA Privacy and Security Law, Sept. 20, 2004)

- The third case is that of Sacramento man Rodney Ware who received media attention in November 2004. His case involves both financial fraud and criminal identity theft. His wallet was stolen in 1989, and shortly after that he began to get notices in the mail that he owed the City for many light rail tickets. After that, he had to deal with fraudulently opened bank accounts, fake drivers licenses, fraudulent credit accounts, cell phone accounts, and fraudulent local phone service in several states. He has been arrested several times — in the airport, in front of his home, and at a new employment orientation session. There have been several warrants for his arrest in several states including Colorado and Kansas. He has had to go to court in these other states to clear his name. The crimes include hit and run, illegal drugs, bad checks, and traffic tickets, among others.

Mr. Ware considered changing his name and Social Security number before learning of the Identity Theft Registry. And in November 2004 he appeared in court here in Sacramento where a judge issued a court order declaring him innocent of the charges. With this order, he was able to add his name to the Registry. He said to reporters, "I don't feel haunted by law enforcement anymore. I have something that identifies me as a victim instead of a criminal." The news story concludes: "The next time Ware is stopped by law enforcement, one phone call to a special hotline staffed around the clock should clear up any confusion." (Sacramento News 10, Nov. 24, 2004)

California Identity Theft Registry

In the late 1990s, Tom Papageorge of the Los Angeles District Attorney's office hosted a series of meetings in which several of us attempted to search for legislative solutions to criminal identity theft. The voluntary ad hoc task force included local, state, and federal law enforcement, prosecutors, a criminal identity theft victim, myself as a consumer advocate, and Mari Frank who is an identity theft victim, an expert on ID theft, and attorney.

The work of our task force resulted in the Torlakson bill, AB 1862, signed into law in September 2000. It established Penal Code 530.7, the California Identity Theft Registry. (www.leginfo.ca.gov)

The Registry is a database, developed and maintained by the California Department of Justice (DOJ), in which information about individuals who are victims of criminal identity theft is recorded. Access to the database is provided to "criminal justice agencies, victims of identity theft, and individuals and agencies authorized by the victim." The bill also required the California DOJ to establish and maintain a toll-free number to enable these entities access to the Registry.

The Registry was developed in 2001 and has been in operation ever since. It is managed by Bud Wilford.

Here's how it works.

Let's say you have learned you are a victim or criminal identity theft – like the three individuals whose stories I told you a moment ago. You will need to obtain verification from the court in the California jurisdiction where the arrest and/or conviction occurred that you are indeed a victim of criminal identity theft. Then you have your fingerprints taken at one of the state's many Livescan sites. You complete the application to enter the Identity Theft Registry and send it along with the all-important court verification – known as the CR-150 form – to the California Department of Justice.

Once you've accomplished all this – which could take several months at minimum – let's say you are stopped for speeding, or for a broken taillight. When the law enforcement officer runs a check on your identity, you tell him or her that you are a victim of criminal identity theft and that an official record of your status is kept by the California DOJ. You give the officer the Registry's toll free number (888-880-0240) which is staffed every day of the year 24 hours a day. You must also give a PIN number, which you receive once you are successfully accepted into the Registry. If all goes well, the officer verifies your status as a criminal identity theft victim, and your only concern is to deal with the broken taillight or the speeding ticket.

For employment, Bud Wilford tells me that his office will send a letter to the employer verifying your status as a criminal identity theft victim. He says that letters are far more common than phone calls in this situation. http://caag.state.ca.us/idtheft/general.htm

Sounds simple enough, right? Unfortunately, the most difficult part of the whole process is obtaining court verification that you are a victim of criminal identity theft. The order that the individual is seeking from the court is known as a "Certificate of Identity Theft: Judicial Finding of Factual Innocence." It's also known by the form number, CR-150.

When the Registry was first developed, victims found it difficult to use the court system to obtain the necessary document that they are indeed innocent. In fact, in the early days, this process really required the assistance of an attorney. For the first couple of years, I'm told, there were only two registrants in the Registry. I'm told by Bud Wilford that there are now 30 registrants – four years after the Registry was developed.

What has made a difference for some victims is a guide developed by the California Office of Privacy Protection for victims of criminal identity theft, available on its web site, www.privacy.ca.gov. The OPP had the assistance of law students at Stanford Law School's Center for Internet and Society. Now, individuals can represent themselves much more easily than in the early days of the Registry, and are not as likely to have to hire an attorney.

- How to Use the California Identity Theft Registry, http://www.privacy.ca.gov/sheets/cis8englsih.pdf
- Court petition form, http://www.privacy.ca.gov/sheets/cis8petition.pdf
- Registry forms, http://www.privacy.ca.gov/sheets/cis8registry.pdf

The guide offers step-by-step instructions, and has all the necessary documents and forms. Further, it's written in plain English, at, I would guess, an 8th grade level at most. The packet is also available through the Web site of the California Attorney General, http://ag.ca.gov/idtyheft/general.htm.

Recommendations

This is a conference seeking solutions, so let me now discuss my recommendations. In preparing this presentation, I have relied on what we have learned from actual victims contacting the PRC. And I've talked at length with an individual who has assisted several individuals in the court process of obtaining the CR-150. That person is Mr. Jay Foley of the Identity Theft Resource Center in San Diego. He and his wife Linda, the founders and executive directors of the Center, assist victims through the entire life cycle of identity theft. They have in-depth understanding of the plight of victims of both credit and financial identity theft, as well as the worst-case scenario of criminal identity theft. Their Web site is www.idtheftcenter.org.

My recommendations are in the following categories: Legislation, education, and research.

First, possible legislation:

- There must be, if not already, enhanced penalties for those who use another person's identifying information when arrested, cited, and convicted. And those penalties must be sufficient to act, as much as possible, as a deterrent.
- Further, criminal identity thieves should be required to pay the court costs and other costs for their abuse of the system.
- For criminal identity thieves, there needs to be less probation and more real time.
- There must be more multi-jurisdiction cooperation in these cases.

- And there must be a victim-hand-holding function established, so a victim has the same individual to deal with as a "constant" throughout the whole process. Perhaps this could be done through the victim-witness assistance programs in most district attorneys' offices.
- And another recommendation on the victim's side of the equation, there should be the development of uniform court procedures across the state for the handling of the entire CR-150 process. More on this in a moment.

Second, education. This is key. Jay Foley of the Identity Theft Resource Center has walked several criminal identity theft victims through the court process in two different counties' Superior Courts. He and the victims he has assisted have found that there is almost no knowledge of the CR-150 process and the Registry.

There must be a broad-based education campaign to reach the following:

- judges
- court clerks
- court administrators
- LiveScan operators
- Prosecutors and staff in District Attorneys' and Attorneys' General offices
- law enforcement
- attorneys, especially criminal defense attorneys
- victim-witness assistance programs
- legal services for low-income individuals
- law school clinics
- consumer advocates
- community-based organizations, especially those serving low-income and non-English speaking individuals
- in short, anyone who might come in contact with a victim of criminal identity theft.

Educational materials should be in more languages than just English.

The California Office of Privacy Protection has done a vital service by preparing its guide, available on the OPP Web site, in a very readable form. This must be widely disseminated, and if it's not already in other languages, it needs to be. Perhaps a short version can be written, brochure-size, that could be handed out by court clerks, law enforcement, victim-witness programs and so on – in multiple languages.

A brochure is one educational tool, but there are more. The CR-150 process and the Identity Theft Registry must be included on the agendas of the many conferences that all those people I just listed attend. Not just for one year's conference, but on an ongoing basis.

The media can serve as a great educational vehicle. The people that I just listed as the targets of education all have their own professional and trade associations, with their own magazines and newsletters. Stories about the CR-150 process and the Registry should be submitted to them for publication. And they should not be limited to

just California publications. Californians who are victims of criminal identity theft are having to travel all over the country to work with law enforcement and participate in court hearings in states where there is no CR-150 process and no Registry. I feel for individuals who have to work within the criminal justice systems of states that do not have these systems in place.

Bud Wilford of the California DOJ tells me that there is a proposal in the works to develop a new ID Theft File by the NCIC so law enforcement agencies can flag "stolen identities" and "identify imposters." This can't come too soon.

My third recommendation is research – in two areas: criminal identity theft in general, as well as the effectiveness of the CR-150 process and the Registry.

How many criminal ID theft victims are there? How does it happen? How does it impact the victims' lives, both in the short-term and the long run? Is there disparate impact depending on race/ethnicity, income, education, and so on? The short answer is "yes." By the way, both the Identity Theft Resource Center and the Privacy Rights Clearinghouse can help with such research because we are contacted by many victims.

In terms of the CR-150 process and the Registry, we need to know how effective they are. Why are there only 30 people in the Registry right now? How can the court verification process be made even simpler than it is now? How much time does it take to finally get into the Registry? Remember, for all those months that the victim is attempting to get the CR-150 form and listed in the Registry, they are vulnerable to being arrested and detained. In addition, they are virtually un-hirable. What sorts of uses are made of the Registry? For those unable to obtain the CR-150 form, what happened that makes it difficult or impossible for them to get court clearance?

Another aspect of research is to find out what is happening in other states. For example, Ohio and Virginia now have identity theft passport programs.

And finally, there must be an in-depth investigation conducted of the information broker industry. We know from talking with victims that getting a CR-150 document is not the end of the nightmare. Employers can still have access to the wrongful criminal records when they conduct employment background checks using the services of any one of the many commercial information brokers.

- See Beth Givens' 2000 speech on this topic, "Identity Theft: The Growing Problem of Wrongful Criminal Records, www.privacyrights.org/ar/wcr.htm.
- See also Beth Givens' 2002 speech, "Public Records on the Internet: The Privacy Dilemma, http://www.privacyrights.org/ar/onlinepubrecs.htm.

As we've all learned these past two weeks as the ChoicePoint data breach has unfolded, the information broker industry is not strongly regulated. A good research study could track the flow of records from law enforcement and the courts, to data compilers and beyond to the information brokers. The research would also examine what happens or does not happen when court records are sealed or expunged.

The largest information brokers are ChoicePoint, Lexis-Nexis, Acxiom, WestLaw, and Info USA. But there are many more who sell their wares for a fee – to virtually anyone – on the Internet, no questions asked. Intelius.com and US-Search.com are just a couple.

Thank you for listening.

In closing I want to acknowledge and thank Bud Wilford of the California DOJ's Identity Theft Registry, Jay Foley of the San Diego-based Identity Theft Resource Center, and Paul Satkowski of the DMV. All have helped me understand the complex crime of criminal identity theft.

Thank you again for the opportunity to speak here today.

Mari Frank, Attorney, Author of "Identity Theft Survival Kit"

The following consumer explanation of some of the new amendments to the Fair Credit Reporting Act (FCRA 15 U.S.C. 1681 et seq.) as amended by the Fair And Accurate Credit Transactions Act of 2003, are excerpted from Mari Frank' s new edition of *From Victim To Victor: A Step By Step Guide To Ending The Nightmare of Identity Theft.* (Second Edition with CD Rom including attorney composed letters, logs, forms, and resources- Porpoise Press, Inc. Copyright Mari Frank -2005.)

Your rights as a victim of identity theft with regard to The Fair Credit Reporting Act (FCRA) as of December 1, 2004:

- ***Initial phone fraud alert notification***

You have a legal right to add a Fraud Alert to your credit profile with each of the credit reporting agencies: Equifax, Experian and TransUnion. If you call the fraud number for one agency, that bureau must notify the other two agencies and place the alert in their files, as well. This alert shall notify all prospective users (potential creditors) that the victim or potential victim does not authorize any company to establish any new credit plan or extension of credit without calling the consumer to verify his identity and permission before extending credit. This means that a potential creditor shouldn't issue new credit, additional cards, or extend a higher limit unless the victim is called or other reasonable steps are taken to verify that the victim authorized it.

Once you place an Initial Fraud Alert by phone, you'll be able to request a free copy of your credit report, which must be sent to you within three (3) business days after your request. (We suggest you provide your cell phone number if you have one so you may apply for instant credit and can be reached when you are not home.) The Fraud Alert will be placed on your file and will stay active for not less than 90 days from your request, unless you write a letter asking for an extended fraud alert. You can only receive this by writing the letter and asking specifically for the Extended Fraud Alert for seven years.

Extended Fraud Alert - Additional Rights

To request an extended fraud alert to remain on your file for up to seven (7) years, you must include with your letter an "Identity Theft Report" which must include the following:

- Allegations of the Identity Theft Affidavit;
- An official valid report filed by you with a federal, state, or local law enforcement agency; and
- Your proof of identity. To avoid consumer fraud, you are subject to criminal penalties for providing any false information.

The credit reporting agencies must notify you of your right to receive two credit reports over the subsequent twelve months from when you first requested the fraud alert. You also have the right to be excluded from the pre-screening (it will stop "pre-approved offers" for up to five years.)

- ***Credit bureaus must block fraudulent information***

Once you, as the victim, identify in writing fraudulent information in your credit reports for the three credit reporting bureaus, each agency must block the fraudulent information from showing up on your credit report (not later than four days after they receive your letter — so make sure you send it return receipt requested). They must notify the furnisher of that information that you are claiming to be a victim of fraud. Then, the creditor must both investigate the information and take steps to prevent it from being re-submitted to any of the three credit reporting agencies. Under FCRA, those companies that report fraudulent information must establish reasonable procedures to respond to the notices by the credit reporting agencies that your information was blocked due to identity theft. Once the creditors receive an Identity Theft Report from the victim, and appropriate documentation, the creditor is required to stop furnishing that information to the credit bureaus. Once you send your letter to the credit grantor who has issued fraud accounts with your Identity Theft Report, they must re-investigate the underlying information and they may not transfer that debt to another company or to a collection company once they are notified that that debt is a result of fraud.

- ***Identity theft victims' access to fraudulent transaction information***

You, as the victim, are entitled to request from any business entity that instituted a fraud account by an identity thief, all documentation about the transactions by the thief. And, you may also request that copies of the documentation be sent to a law enforcement agency, as well.

You must make a written request for the information and include any relevant information that you know about the transactions. You must provide proof of your identification, the government-issued ID, personal identifying information, (more than the thief was required to give), or the same type of information that the business usually requests from new applicants. You must also send your Identity Theft Report from a law enforcement agency and your completed Federal Trade Commission Identity Theft Affidavit. Then, once you send this, return receipt requested, to the business, you should be provided copies of the application and all the business transactions within (30) days of receipt of your letter … at no cost to you. Now, here is the challenging part:

The business can refuse to give you access to such records even if you do all the things that you are supposed to do under the law. If the business determines "in the exercise of good faith" that any of the following exceptions exist:

- The business does not have a high degree of confidence in knowing the true identity of the victim who is requesting the information, even though the victim has satisfied the Identity Verification Requirements.
- The request is based on a misrepresentation of fact, or
- The information requested is "Internet navigational data or similar information."

Another problem with this provision is that you have no right to enforce this provision, meaning you have no right to sue the company if they fail to provide you the information, and your own state attorney general is precluded from suing on your behalf. Worse yet, the states are preempted from making stricter laws to protect you. The only agencies that have the right to sue are the Federal Trade Commission or other federal agencies. So, if a company refuses to provide you this information, you should make a complaint with the Federal Trade Commission, and also notify the U.S. Public Interest Research Group and the various consumer, nonprofit agencies to let them know that this is happening. We believe that if you let your state and federal legislators know, and let the media know, then perhaps some "teeth" will be put into this provision.

It is critical for you to get documentation of the crime, and for the law enforcement agency to get documentation of the crime, so that they can pursue the perpetrator. Many companies are reluctant to send you this information, since it will evidence their negligence. But you must explain to the company that in order for there to be prosecution and conviction, you need to find the thief, and you must have evidence to do so. And if the thief is prosecuted and convicted, then, of course, you are entitled to ask for restitution for your out-of-pocket expenses and your losses. So, it's critical for you to get fraud data, and you should demand it.

- ***Debt collectors must provide information to victims***

You have the right to notify any collection agency that the debt is fraudulent or resulted from identity theft. The debt collector must notify the original creditor and provide you with the information required under the debt validation of the Fair Debt Collection Practices Act. That allows you to demand written notice of the amount of the debt, the name of the creditor who's claiming that the debt is owed, a statement that you have the right to dispute the validity within 30 days, (otherwise the debt collector will assume that it's valid). You must dispute the fraud debt in writing. The collector must provide you documentation of the verification of that debt, and the name and address of the original creditor. Then you may follow through with requesting access to the thief's transaction information as above. A creditor who has been notified of a fraudulent debt must not sell it to a collection agency. So, be sure to write your letters and document any violation.

- ***Agency responsibilities to block all fraud***

You have the right to have all fraudulent information on your credit profile blocked (that means that it will be deleted from the view of any potential creditor and will not appear on your consumer reports unless they prove it is not fraud.) You must provide the credit bureaus with the following information:

  - Proof of your identity
  - Copy of your Identity Theft Report
  - Your identification of the fraudulent information
  - Your statement that the information does not relate to any transaction that you've made. (See all letters in *From Victim To Victor.*)

Once the credit bureau receives this information from you (return receipt requested to verify the date), they must block the items within four (4) business days; so the information in your file should be restored to what it was without the fraud. This is especially important if you're trying to buy a house or car, or get a job because the fraudulent information will be blocked immediately, and your score will be re-adjusted. But you must do this in writing!

- ***Credit bureau must notify furnisher***

When you write your letter to request a block of all the fraudulent information on your credit report, you should include not only fraudulent accounts, but also fraudulent bankruptcies, fraudulent tax liens, fraudulent addresses, fraudulent names, inquiries, etc. Once you notify the three major credit bureaus (in writing) that you're requesting that the information be blocked from your credit reports, each of the agencies has the duty to notify the entity or companies that furnished the information that was blocked due to your Identity Theft Report. They must notify the furnisher of the date of the block, and all other information pertaining to the fraud — so you must include all of the fraud information in your notification.

- ***Resellers of credit reports***

There are hundreds of resellers of consumer information that sell to mortgage companies, law offices, real estate brokers, car dealerships, etc. If you see a copy of your credit bureau report from a reseller, you have the right to inform the reseller of the fraud. The reseller must block the report and notify you of the name, address, and telephone number of the major consumer-reporting agency that provided the original information. Then you as the victim have the right to enforce the block with that major credit reporting agencies.

- ***Your rights with regard to the creditor or furnisher of information***

The creditor who furnished the information must institute procedures to prevent the re-reporting of that information to anyone, not just the credit bureaus. The creditor who issued the fraud account is required to purge their file of your fraud. You must submit your Identity Theft Report and letter directly to the furnisher or the creditor. Although this is extra work, take advantage of this right under the law. Once you submit your report and tell the creditor that the information was based on identity theft and the creditor stops reporting that information to the credit bureau, they can only re-report that information if they subsequently research and find out and "know" that that information is truly correct and not fraud.

- ***Creditors may not sell fraud accounts to collection companies.***

Once a creditor is notified that the information that they've reported to the credit reporting agencies was fraudulent as evidenced in an Identity Theft Report, the creditor may not sell, transfer, or place the debt for collection. This is a major improvement for victims who in the past would report the fraud to the original creditor, and then the creditor would sell the account to a collection agency that would then sell it to another collection agency. Some victims would clean up their credit reports, only to find new collection agencies would appear on their reports.

- ***Check verification companies and your rights under the Fair Credit Reporting Act***

Check services companies, which issue authorizations for the purpose of approving or processing checks, electronic fund transfers, or similar payments, are exempt from the blocking guidelines of fraud information to retailers and others who use their information. So, this is still a challenge for victims. However, once you notify a check services company that you are a victim of identity theft with regard to check fraud, that check services company must no longer report fraudulent information resulting from your identity theft.

- ***Unblocking of your fraud***

If a consumer credit bureau "reasonably believes that you misrepresented this fraudulent information or that, indeed, you received goods or that there was an error, then the agency has a right to rescind the block." Any genuine debts would not be blocked. If the agency decides to unblock your fraudulent information, they must notify you of the rescission and the specific reason for the rescission within five business days.

For more information please visit Identity Theft Prevention and Survival at www.identitytheft.org. Watch the 90-minute PBS Television Special with host Mari Frank: "Identity Theft: Protecting Yourself in the Information Age," which will air in March 2005 on your local PBS Television station. Read Mari Frank's new books Safeguard Your Identity: Protect Yourself with a Personal Privacy Audit (Porpoise Press 2005) and *From Victim To Victor: A Step by Step Guide For Ending the Nightmare of Identity Theft,* Second Edition, with CD of letters, forms, logs, affidavits, resources (Porpoise Press 2005), available at www.identitytheft.org, your local bookstore, or Amazon.com.

Tony Hadley, Vice President, Government Affairs, Experian

My wife and I have both been victims of identity theft too – even people who run credit bureaus are not immune. My purpose today is to bring the consumer perspective of Experian from talking to literally thousands of consumers every day. That's just a fraction of the tens of thousands who contact us in other ways, but these are personal contacts from people who are concerned about identity theft. These aren't all victims, many of them are just worried about identity theft. They want to know what they should do, how they can help themselves. We have programs and assistance for everyone who contacts us about identity theft.

Letting individuals know what to do and when to do it is really important. We have a special section on our Web site that tells just what to do. We have lots of other consumer education material, including a booklet I brought today. We also have our own version of "Dear Abby," called "Ask Max." It's a column in which she answers questions about identity theft and other consumer credit issues.

Experian also has experience assisting law enforcement at all levels investigate identity theft and financial fraud. We help financial services companies with tools and databases to help prevent identity theft. And of course we have programs to help victims restore their credit histories as fast as possible.

I'd like to provide a perspective on America's credit system, based on our experience here in America and in 36 countries on every continent in the world. Here a consumer can go to a car dealer and step off the lot in a new car quicker than he can pick out the interior colors. A consumer can apply for instant credit to finance furniture or clothing. He can apply for credit online and receive it in a matter of moments. These are examples of what FTC Commissioner Tim Muris called the miracle of instant credit, and it's a daily fact of life for Americans that exists no where else in the world. The American financial services industry has responded to consumer demand with a credit delivery system that provides them with access to credit immediately, when and where they want it and at a price relative to their own risk. And it's the envy of the world. As we know from working with the World Bank in developing countries, the establishment of a credit reporting system is the bedrock of economic development in those countries.

Americans expect that access to credit and at the lowest price and when they don't get it, they want it. We have a balancing job to do here. Instant credit cannot come at the expense of this ballooning identity theft. That's what FACTA was about: It's the first time that the U.S. Government took a comprehensive look at balancing these two factors. And I think it does a pretty good job of balancing these factors.

We're implementing it right now and there's still a lot of work to do. Many of its provisions became effective December 1, and we have some more new obligations under FACTA coming up later this year. I'm hoping that it will clear up some of the problems we've heard of today, and I'm sure that it will.

We've had a long history working on identity theft legislation in California, and I think Californians should be proud. Many of you who have worked on the law in California know that many of your laws are now codified as national law. In addition to that I count 14 new rights under FACTA that Californians have. There are lots of ideas that come out of California and we're always ready to listen.

We also have a long history of working with California law enforcement agencies to investigate identity theft and fraud. We have people who do nothing but work with law enforcement. We also have a history of working with consumer advocates in California. One example is our single-call system for identity theft victims. Organizations said that this is a problem that consumers are having: why make them call all three bureaus? We thought that was a good idea, so we adopted it and now it's been codified in FACTA.

We've also learned that there are other ways to help ease the situation for consumers. For example it was the direct advice of consumers that lead to our implementing the fraud alert system, back in 1992, when identity theft wasn't such a big problem. I'm hearing today that there are problems with the fraud alert, and I'm going to go back and look into that.

I want to talk about four new rights under FACTA. The first is the right to a free annual credit report. We're just rolling out the second phase of that, for the mid-tier of states. The ID theft report is, I agree, a problem, and we're working on ways to address it within the confines of the law. There are inconsistencies in ID theft reports and the process needs to be streamlined. Upcoming still – FACTA isn't finished – are Red Flag guidelines that credit issuers are going to have to use when extending credit, how to recognize potential identity theft in the making. We're going to have new address mismatch guidelines, new guidelines for data furnisher accuracy. And a new right that consumers have to directly dispute with data furnishers, which will help clear up some of these issues as well.

Law Enforcement Perspectives

Jonathan Fairtlough, Deputy District Attorney, County of Los Angeles

California has been innovative and proactive in addressing high tech crime and identity theft. The California High Technology Theft and Apprehension Act created five task forces. For each task force, at least two counties get together, prosecutors and major police agencies; they share resources and become the focal point for identity theft and high tech crimes in the area. The five task forces focus on particular issues, allowing a regional approach to problems.

In Southern California identity theft is huge problem. There is no way any one task force can handle all cases. We need specialized detectives and prosecutors to handle large rings, while providing expertise and training to other law enforcement agencies.

Over 20,000 cases were reported to the Los Angeles Sheriff, and 1,200 were filed by the Los Angeles District Attorney. Most were not handled by our Task Force, but the Task Force supplies expertise and training to other agencies to handle the smaller identity theft cases involving $3,000-$4,000 and one or two victims. This frees the Task Force to address large rings and organized efforts that really do damage to our credit and business structure.

The High Technology Crime Task Force program is funded to the tune of $14 million, but the resources must be carefully managed. Law enforcement has to perform triage and focus the resources where they can have the greatest impact. We also have to make sure that victims understand that California gives them a resource with a police report – the key to their future. First it allows them to retake control of their financial future; it provides a series of protections allowing them to regain their credit, and it protects them against suits and against the further use of the information in the future.

Given the level of identity theft, it's impossible for law enforcement to investigate and prosecute every case. Making the report gives a victim protection, notifies law enforcement of the problem and allows them to focus resources where they can make the most difference.

Lt. Robert Lozito, Sacramento Valley Hi-Tech Crime Task Force

There are some challenges that are unique to investigations of ID theft. First is the overwhelming volume of cases, each with host of different victims and different suspects. Also the crime doesn't stop at the boundaries of our jurisdiction. The Sacramento Valley Task Force encompasses eight counties, 32 jurisdictions participate, and also federal investigators. The sheer volume of evidence also presents problems to investigators and support staff. Criminals purchase products using stolen IDs. Our investigators collect whole housefuls of equipment and furniture, which poses problems of storage. It's good to have relationships with retailers, to help us get merchandise back into the proper hands, often the retailer's. Coordination between multiple agencies is critical, including prosecutorial agencies. Victims often don't know they're victims until some time after the crime has occurred. This puts law enforcement at a disadvantage. The trail is often cold by the time we get involved. Stiffer penalties would help with the recidivism we see so often. Communications with victims take a lot of law enforcement's time. The victim is the recipient of much of the evidence – bills, letters from collection agencies, etc. We rely on victims providing us with that information to help us move on the case.

Technology is our friend, but it's also becoming a problem. The ability to apply for credit online makes verification of identity difficult. Financial institutions are working on this and we're working closely with them.

Many cases our Task Force is working are large rings, because we're trying to get the biggest bang for the buck. Often there are hundreds of victims and dozens of suspects in a single case. Identities are traded as a commodity, often traded online. They are traded for drugs sometimes, especially for methamphetamine, which raises the danger level for investigators. Serving warrants, interviewing suspects when they're under the influence of meth, means that our officers must be highly trained in order to be safe. You'd think ID theft is soft, non-violent crime to investigate, but it isn't.

One of the problems we also experience – even though we have the luxury of vertical prosecutors on the Task Forces paid by State grant funds – is that the volume of cases doesn't allow a prosecutor for every case. Often only 30% can be handled by the vertical prosecutor, with 70% going to the intake DA. Vertical prosecutors can take the time to really get into the nuts and bolts of the case and get the biggest prosecutorial bang, so they can put the criminal away for as long as possible. Unfortunately, on the intake side, knowing that the cases have to be moved as quickly as possible because the bucket is full and more are coming in the morning, we tend to see lesser sentences, more probation, and misdemeanor charges. That puts the people back on the street, perpetrating the crime again almost immediately.

Not all police agencies in the state are equipped to take the initial police report – either because they don't have the personnel or because they don't recognize the crime. That leaves the victim searching for someone, anyone, to take the report. That's the way it stands today. So we put part of our Office of Emergency Services money to training other law enforcement agencies to respond to this problem, to make sure they're taking good, comprehensive reports on the front end, which helps investigators follow up.

Some of the things we're looking to for help in the future include some of the biometric uses, to make sure that we only issue one ID card to one person, preventing people from assuming the same identity. I know some financial institutions are putting a lot of money into that.

Our partnership with private business is somewhat unique in law enforcement. We work hand in hand with fraud investigators in financial institutions and retail stores. It's working very well.

Edward S. Berberian, Jr., District Attorney, Marin County

We must all work together to get to a solution for this crime – banks, credit card companies, law enforcement and prosecutors, all working together – government alone can't do it, no matter how much support we have. Our state government has been very supportive of the task forces and we hope that support will continue, but that alone will not solve the problem.

California has been a leader on this issue. But we can do things better. One of the challenges I see – is what I will call "the priority challenge" – it must be a priority in our legislature, in our executive branch – they have to come up with the money and the resources to make it work. They've done this in the past and it has to continue to happen to get results.

The next challenge is called "breaking the cycle." People who commit this crime do it repeatedly. The regional task force approach we use in California gives us an opportunity to use different approaches. LA's approach has obviously got to be different from the approach we take in our large, more rural region in Northern California. Our approach is different because we have over 60 police jurisdictions and 13 counties that our task force covers

– they're very small jurisdictions, with few officers. We can't become the identity theft police for the whole area. What we've done, following CATCH's [San Diego task force] example, is to train the officers to "break the cycle" by following up with probationers who've already committed identity theft. We get together teams and do probation sweeps – and we do find violations: About one third of the violations we find on these sweeps are identity theft related. We also pick up the large cases along with this probation approach, as a means of impressing on those individuals that we're serious about this.

Another challenge, I will call the "lip-service challenge:" I asked my staff what they find the most frustrating thing in dealing with prosecutions of identity theft. One issue that came up often is the jurisdictional issue -- while I'm sure my federal brother over here on my right can cure all jurisdictional problems, we need state legislative changes to give us broader ability to deal with this issue. Here we get into the area of cross-designation, putting aside turf issues on all levels, allowing us to use our resources more efficiently – you can have local prosecutors designated as Deputy Attorneys General and Assistant U.S. Attorneys. Both agencies are willing to get into this [allow cross-designation], which was not always the case in the past.

And finally, I want to talk about industry. Normally the ones we work with are ex-cops, who became the security personnel in the businesses used by our victims, and they work with us quite well and are very willing to assist. I do think, however, that industry needs to look at itself, and decide to handle this issue as more than just a cost of doing business. You have to re-educate yourself to move away from that concept [ID theft loss is a cost of doing business] and be willing to support us. My attorneys tell me that when they go to get the bank or credit card records, or the bank witness who can lay the business record foundation to get the material in and prove the case, they repeatedly run into roadblocks. I know industry only has so many resources, but given the exposure they have because of the marketing that they do, they have to look at the other side of the equation and be ready to back it up when we need documents and witnesses. There's a need for improvement – for all of us.

Lawrence Brown, First Assistant U.S. Attorney, Eastern District of California

The crime of identity theft is widespread and easy to commit. Unfortunately, one cannot look to law enforcement alone to "solve" the problem. Consumers and financial institutions must continue to take steps to prevent identity theft and allow for victims to clear their good names as quickly as possible. However, to make a real impact on the problem of identity theft, law enforcement must have a vigorous, visible effort in the overall effort.

Law enforcement's response must be coordinated, at all levels, such as taken place with the advent of task forces across the state. We also must maximize publicity when we successfully prosecute identity thieves. While debate will long rage about whether a violent criminal's behavior can be deterred, there is no dispute that with these sorts of crimes, which are calculated and financially-driven, offenders will pay attention if there is a high likelihood of being apprehended and there are severe consequences. Our laws have come a long ways in recent years, but it is doubtful they are sufficiently punitive to deter large numbers of would-be identity thieves at present.

There are a number of federal agencies involved in the fight against identity theft, including the United States Secret Service and the Federal Bureau of Investigation. Another key agency is the United States Postal Inspection Service. Theft of mail is a common precursor to committing identity theft. Recently, I indicted someone who had been breaking into multi-unit mail boxes. In his car he had over 1,000 pieces of stolen mail, and a search of his house revealed computers, a printer, a laminating machine, and acid to "wash" checks. He was on probation

for possessing fictitious checks in Sacramento County, after having been sentenced to 60 days county jail. Under federal law, for simply possessing stolen mail, his sentencing range is between three and four years in a federal penitentiary. Can all cases be taken federally? Of course not. I highlight this case as an example of a cooperative effort between local and federal law enforcement. The deputy district attorney believed that given the offender's history and his ongoing conduct, he warranted federal prosecution; the U.S. Postal Service and the U.S. Attorney's Office were only too happy to oblige.

The federal identity theft statute, 18 U.S.C. § 1028, has been on the books since 1998. So long as there is an interstate nexus, we have jurisdiction. The sentencing range is five to 15 years. The federal sentencing guidelines determine more precisely what sentence an offender will receive. Given recent United States Supreme Court decisions, the guidelines are now advisory only. While it is too early to tell the precise impact, it is safe to say sentencing is less predictable as a result.

Last July, President Bush signed into law the Identity Theft Penalty Enhancement Act. This law, codified at 18 U.S.C. §1028A, provides a two-year mandatory enhancement for someone who commits identity theft during such crimes as bank fraud, mail fraud, and wire fraud. Another important aspect of federal law is that an offender must serve 85% of his sentence, and restitution orders are imposed for 20 years and cannot be discharged in bankruptcy nor reduced due to inability to pay.

By necessity, federal law enforcement and prosecutors must be selective about the kinds of cases we pursue. It is a question of resources, not commitment to the problem. Prosecution thresholds are a necessary evil. However, whenever you can get the "feds" involved, it sends a strong message to the criminal community. They genuinely fear federal prosecution. It is incumbent on federal agencies to work closely with state and local authorities to ensure we are part of the equation.

Another challenge of identity theft is that it is being committed internationally, in such far-away places as Nigeria and the former Soviet Union. These are problematic cases. However, if we can get custody of the offender, generally we have federal jurisdiction. The FBI often is able to investigate. They have legal attaches in many foreign countries, who build relations with local law enforcement to investigate crime. The Justice Department also has an Office of International Affairs to aid with extraditing criminals from abroad and working with foreign jurisdictions. Increasingly, investigators are working with foreign law enforcement and prosecuting the criminals overseas. While not perfect, it is certainly preferable to no prosecution whatsoever.

The problem of identity theft will not go away overnight. However, collaborative efforts among all rungs of government, including such forums as this summit, are critical to reigning in this growing problem.

Robert Morgester, Deputy Attorney General, Special Crimes

Identity Theft Jurisdiction

Did you know that New York, Georgia, Florida, Utah, Virginia, Wisconsin, and even Washington State now lead California in protecting the right of identity theft victims by allowing venue for prosecution of identity theft cases where the victim resides? California, once in the forefront of protecting its citizens, has fallen behind.

Under existing law, the jurisdiction of a criminal action for fraud or theft is in the county where the crime occurred, in the county in which the stolen property was brought into, or any contiguous jurisdictional territory

if the arrest is made within the contiguous territory and the prosecution secures the defendant's waiver of the right of vicinage, and the defendant is charged with one or more property crimes in the arresting territory. (Pen. Code, § 786.) As to Identity theft cases (Pen. Code, § 530.5), jurisdiction is limited to the county where the theft of the personal identifying information occurred, or the county where the information was used for an illegal purpose. (Pen. Code, § 786(b)(1))

This traditional definition creates unique issues in the area of intangible property such as identity. Often in identity theft crimes, a victims' identifying information is not stolen nor used within the county that they reside. The only aspect of the crime that can be shown to occur in the victim's county is the subsequent receipt of the bills. Many Superior Court judges are now stating that jurisdiction to prosecute identity theft crime only lies within the county where the theft of the personal identifying information occurred, in the county where the information was used for an illegal purpose. Thus jurisdiction does not reside within the victim's county.

Additionally, current law mandates that the local police that has jurisdiction over the victim's "actual residence" shall take a report and begin an investigation. (Pen. Code, § 530.6) However, the local jurisdiction does not have the ability to prosecute (information not stolen or used in the county).

To put this all in perspective, let us assume you are a Sacramento resident whose identity is stolen and used to have a computer delivered to an address in Los Angeles. You have no idea how your identity was compromised. A Sacramento detective is required to take a report and if a suspect is identified any subsequent prosecution must be in Los Angeles. Unfortunately, Los Angeles law enforcement handles hundreds of cases per investigator and cannot meet the needs of their own county residents, let alone the needs of an out-of-county victim.

Out-of-state cases pose even greater problems. Let's assume 3,000 California residents' identities were compromised by a suspect in Idaho and used to purchase goods that were delivered to Florida. Because jurisdiction is limited to the county where the theft of the personal identifying information occurred, or the county where the information was used for an illegal purpose California cannot even prosecute this case. It doesn't matter that 3,000 Californians were victimized - we have no jurisdiction that has been statutorily given to bring a prosecution.

The solution to this problem is simple: the jurisdiction for the identity theft related offenses should include the county in which the victim resides. This would expand the number of available jurisdictions to where identity theft could be prosecuted. This expansion will increase the legal tools available to the victim's local law enforcement agency enabling them to better investigate identity theft. Finally, the best jurisdiction to prosecute any crime is the place where the damage is done. In identity theft cases, this place is where the victim resides.

In Price v. Superior Court (2001) 25 Cal.4th 1046, the Supreme Court recognized the power of the Legislature to designate the place of trial of criminal offenses as long as there was a reasonable relationship or nexus between the place designated for trial and the commission of the offense. It is clear that with the taking of personal identifying information for purposes of committing identity theft that the suspect is targeting the emotional and financial well being of the victim at the location where they reside. All bills, debts, or any other illegal activity that is set in motion by the suspect will end up on the victim's doorstep. It is the equivalent of pulling the trigger of a gun aimed at the victim. The negative impact, economic and otherwise, of identity theft on the victim, is directly connected to the commission of the offense, which is the theft or use of the information.

This one change will allow us to join States like New York, Georgia, Florida, Utah, Virginia, Wisconsin, and Washington State which have statutes that allow for the venue for prosecution of identity theft to include the jurisdiction where the victim lives.

Penal Code § 530.5: When is a person a person?

Identity theft perpetrators are constantly refining their craft to make more money and to avoid detection by law enforcement and the people that they victimize. One of the latest trends is for identity thieves to take over the identity of a business. They recognize that businesses have larger lines of credit and that volume purchases (100 notebook computers) don't raise suspicions. A well-done business take-over can easily net $50,000 to $100,000 in merchandise and cash advances compared to the $5,000 obtained from a identify theft take-over of an individual. This trend raises the question of whether a business is considered a person pursuant to Penal Code section 530.5.

Penal Code section 530.5 states in part that "[e]very person who willfully obtains personal identifying information . . . of another person and uses that information for any unlawful purpose . . . without the consent of that person is guilty of a public offense. So what is a person? Penal Code section 7 gives us guidance by stating that" the word "person" includes a corporation as well as a natural person." Therefore, an identity theft victim can be a natural person or a corporation.

Missing from Penal Code section 7 definition of "person" are firms, associations, organizations, partnerships, business trusts, limited liability companies, and public entities (government). (compare Pen. Code § 7 [defining person] with Evid. Code § 175 [defining person]; Govt. Code § 17 [defining person]; Vehicle Code § 470 [defining person]; Code Civ.Proc. § 17 [defining person].) At first blush, the expansive definitions of a "person" found in every other code except the Penal Code would seem to be ample justification for limiting the Penal Code definition to it's very words: "corporation as well as a natural person." However our inquiry doesn't end here.

Consistently the courts have held that "person" includes all forms of government. A general doctrine of statutory construction is that as long as the result would not infringe sovereign governmental powers, the legislature may properly be held to have intended that the statute apply to governmental bodies even though it used general statutory language only. Pursuant to this principle, governmental agencies have been held subject to legislation, which by its terms applies simply to any "person." (City of Los Angeles v. City of San Fernando (1975) 14 Cal.3d 199, 276-277; See Siegel v. City of Oakland (1978) 79 Cal.App.3d 351 [Governmental agencies fall within definition of "person" for purpose of weights and measure law]; People v. Strub (1975) 49 Cal.App.3d Supp 1 [county can be considered a "person" within the meaning of Penal Code § 7].) Thus the definition of a "person" is expanded to include governmental entities as well as corporations and natural persons.

The harder question is whether Penal Code section 7 is limited solely to corporations and excludes firms, associations, organizations, partnerships, business trusts, limited liability companies from being a "person." When written in 1872, Penal Code § 7 defined "person" as "the party whose property may be the subject of any offense" and included "this State" and "all public and private corporations or joint associations, as well as individuals." This definition was shortened to it present form by an amendment in 1873-1874. It is ordinarily presumed that the Legislature by deleting an express provision of a statute intended a substantial change in the law. (People v. Valentine (1946) 28 Cal.2d 121, 142.) The First District Court of Appeal supported this view when it found that a copartnership was not a "person" pursuant to Penal Code § 7. (People v. Schomig (1925) 74 Cal.App.109, 113; but see 34 Ops.Atty.Gen. 98 (1959) ["person" as used by Penal Code § 7 includes incorporated correspondence

schools as well as other business associations].) A conservative reading of Penal Code section 7 is that firms, associations, organizations, partnerships, business trusts, limited liability companies are excluded from being a "person."

Even if Penal Code section 7 excludes firms, associations, organizations, partnerships, business trusts, limited liability companies from being a "person," our inquiry is not ended. The Court noted in People v. Schomig, supra, 74 Cal.App. 109, that although a copartnership may not be punished as a separate entity for a criminal act, its members are responsible for its acts and may be individually prosecuted. Since a "natural person" is liable for the copartnership's actions an argument can be made that this same "natural person" is the "person" when information relating to the copartnership is used for purposes of identify theft. At a more practical level, many ID thieves will use information belonging to a natural person in committing an identity theft against a business. For example, a forged credit application will include the name of the business as well as the name of the company president. Thus, even if the business is excluded as a victim from a Penal Code section 530.5 prosecutions, the company president is not.

Finally, why should we care? After all, there are a plethora of statutes available to prosecute the use of a business name to commit fraud that can be used instead of Penal Code section 530.5. We should care because Penal Code section 530.5 is a "gateway" charge. Being a victim of Penal Code section 530.5 allows you to get a police report and use that report to obtain information from the credit grantor relating to the creation and use of the fraudulent account. (See Pen. Code § 530.6; 530.8.) No identify theft charges means that limited law enforcement resources must be tasked to write a search warrant for the production of the fraudulent account records. Local law enforcement may not even be able to assist, because without an identity theft charge, there may not be jurisdiction for the issuance of a search warrant from the jurisdiction [county] where the victim business resides. (See Pen. Code § 1524 (j) [warrant may issue from identity theft victims county even if information was used out-of-county].) It is in law enforcement's and the victim's best interest to correctly charge identity theft to allow the use of a Penal Code section 530.8 requests to compel the production of the fraudulent account records.

Until the Legislature conforms the Penal Code's definition of "person" to the definition that is found within the Evidence Code, Government Code, Vehicle Code, and Code of Civil Procedure, we need to take a close look at non-corporate identify theft business victims to ensure that in appropriate cases that they derive the benefits of being correctly labeled an identity theft victim.

Jerry Coleman, Assistant District Attorney, San Francisco

INTRODUCTION: I'm a 25 year prosecutor who has played an identity theft trifecta of sorts: I've prosecuted (and sent to prison) many of these perpetrators; I've published on the subject for years, and taught it to corporate and private groups and to all 3 branches of government (to prosecutors and police, to judges, and to the legislature), and I've even been an identify theft victim, personally…three times! (One way to learn the latest scams the perps are up to!)

METHODS OF PROSECUTION: Over the years, I've seen many methods of prosecuting this growing crime, and some are more effective than others. The petty paper passers at the low end of the criminal food chain – who go into check cashing stores with stolen or counterfeit checks and fake id's – are pretty frequently arrested. But they get equally low-end sentences from our courts, and you've only protected one or two victims at a time

(whose financial data was misused). Trying to arrange a police sting, such as a controlled delivery of merchandise ordered by a criminal individual or a ring to a safe house, takes exquisite timing and a wealth of law enforcement resources that make it usually impractical. Skimming cases (counterfeit credit cards made from the magnetic strips of legitimate cards swiped, for example at restaurants), rake in millions; yet by the time the victims get their bills, it's hard to trace the source of the counterfeit activity or the identities of the card users. So victim protection is virtually nil.

THE NEW PARADIGM: TRAFFICKING Prosecutors and cops from all over the West coast know that many identity thieves are intimately connected with methamphetamine abusers. Ringleaders hire meth addicts to dumpster dive in our private and corporate trash and meticulously piece together our financial information, often paying them in drugs. Before they create the false id's, such traffickers collect and produce financial profiles on their victims. Dope traded for stolen checks begets counterfeit checks, which, when cashed, provides the funds for more dope; or, for ubiquitous computer equipment used to produce more and better counterfeits. I've seen meth addicts living in cheap flophouse hotel rooms with no bathrooms and only a hot plate, yet owning $10,000 in laptop computers, scanners, digital cameras, and large screen plasma TV screens. And most significantly, they have stored in their hard drives the identity profiles of dozens of soon-to-be victims. If we can close these 'fraud factories' as I call them, we can get higher sentences and protect far more of our citizens from future crime.

That investigation & prosecution effort is two fold: police can utilize their drug informants to get information on who is buying stolen identities, or who is passing stolen/counterfeit checks and ids on the street. That information can be put in search warrants for the fraud factories themselves, and middle level perpetrators or above can be arrested and their hard drives seized, to put them out of business and locate all their potential victims. Teams of police and prosecutors have to become educated in the meth/id theft connection and learn to closely coordinate their efforts for maximum effect. But all of that falls short without the second major prong of attack: legislation.

Current identity theft law makes it a felony to obtain another's identity information and use it (or attempt to use it) to get goods or services. Unfortunately, simple possession of the information alone often can only be prosecuted as a misdemeanor. Yet possession of the completed checks, or false drivers' licenses, or multiple credit cards, can be treated as a felony. So we need to borrow legislative language from the drug trafficking laws and the credit card trafficking laws, to make possession of multiple people's identifying information, and trafficking in such profiles, a felony. New legislation can also be used to close other gaps in our current laws, so as to increase penalties for misusing the information of our most vulnerable victims, our young and our senior citizens. And new law is needed to increase the likelihood of local identity theft prosecution by allowing venue in the victim's county of residence, as well as where the paper is stolen or misused.

CONCLUSION: With the proper training of law enforcement, and utilizing new techniques to focus higher up on the criminal food chain, and armed with the tougher legislative remedies in the identity theft arena that we utilized in the past with drug and low tech fraud trafficking, we can stop more crime and protect more victims. And I can stop being a victim myself perhaps!

Summit Advisory Committee

Charlene Zettel
Department of Consumer Affairs
CHAIR

Joanne McNabb
Department of Consumer Affairs
Office of Privacy Protection
PROGRAM CHAIR

Sherry Mehl
Department of Consumer Affairs

David LaBahn
California District Attorneys Association

Mellonie Yang
California District Attorneys Association

Maurine Padden
California Bankers Association

Jeanne Caine
California Chamber of Commerce

Bill Dombrowski
California Retailers Association

Susan Shinneman
Government Technology Conference

Barbara Fulton
Government Technology Conference

J. Clark Kelso
State Chief Information Officer

Karen McGagin
Victim Compensation & Government Claims Board

PRESENTED BY

GOVERNOR ARNOLD SCHWARZENEGGER

CALIFORNIA STATE AND CONSUMER SERVICES AGENCY

CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS

CALIFORNIA OFFICE OF PRIVACY PROTECTION

HOSTED BY

CALIFORNIA DISTRICT ATTORNEYS ASSOCIATION