Still @ Risk

New Technology & Identity Theft Trends In California

CALPIRG Education Fund

Still @ Risk

New Technology & Identity Theft Trends In California

CALPIRG Education Fund

Jonathan Fox
Summer, 2012

Acknowledgments

The author wishes to thank Emily Rusch, State Director, CALPIRG Education Fund; Edmund Mierzwinski, Consumer Program Director, U.S. PIRG Education Fund; Jeff Bernstein, Policy Analyst, U.S. PIRG Education Fund; and Tony Dutzik, Senior Policy Analyst, Frontier Group, for their invaluable assistance in writing and editing this report.

The author bears responsibility for any factual errors. The recommendations are those of the CALPIRG Education Fund. The views expressed in this guide are those of the author and do not necessarily reflect those of the funders or those who provided review.

CALPIRG Education Fund offers an independent voice that works on behalf of the public interest. CALPIRG Education Fund, a 501 (c)(3) organization, works to protect consumers and promote good business practices. We examine problems, craft solutions, educate the public, and offer Californians meaningful opportunities for civic participation.

For more information about CALPIRG Education Fund or for additional copies of this report, please visit us at www.calpirgedfund.org

Cover photography: Bigstock
Design and layout: Alec Meltzer, meltzerdesign.net

Table of Contents

Executive Summary

Identity theft is the nation's leading method of fraud in the 21st century, with the highest number of complaints nationwide originating here in California.[1] While old practices such as mail theft and "dumpster diving" continue, consumers today face new threats as technology advances and new opportunities develop for criminals. These threats include the use of card-skimming devices, abuse of Bluetooth technology, key-logging malware, and attacks on unsecured WiFi networks.

California's consumers face an array of threats to their identity on multiple fronts. A Federal Trade Commission (FTC) report recently noted that for 12% of victims, criminals used more than one method to steal their identity. The FTC findings further reported that 63% of all identity theft victims were initially engaged online by a fraudulent email or Internet web site.[2]

A review of data provided by the California *High Technology Theft Apprehension and Prosecution* (HTTAP) program shows that in 2011 the average dollar loss per victim was $786, which was a significant increase from the previous year's average of $82.[3] FTC data also indicates that the average dollar loss per victim in California during 2011 was 4.8% higher than in 2010.[4] Combined, the data suggests that identity theft is costing consumers more today than in years past.

The increased consumer cost is mostly due to the rise in "new account fraud," where criminals use a victim's identity and good credit to create new accounts, which are then used to fraudulently obtain goods and services. This type of financial identity theft takes longer to detect and results in significant financial loss for both victims and businesses. Market estimates place the average cost for new account fraud at $3,197 per incident.[5] Our report highlights that costly new account fraud is on the rise throughout the United States, accounting for 46% of identity theft based fraud in 2010, up from 39% in 2009.[6]

Despite significant progress in recent years by both law enforcement agencies and the private sector there is still room for improvement in the effort to limit identity theft. California state law prohibits organizations, both private and public, from using a Social Security number as a personal identifier and from publicly posting or displaying that number.[7] Yet organizations continue to collect and store Social Security numbers, unnecessarily placing consumers at risk of identity theft. Authorities should investigate the present usage of Social Security numbers by government agencies and private business to determine if alternative means of identification can be used instead. This will reduce the amount of Social Security numbers collected and reduce risks for consumers.

Policy-makers should adopt statewide minimum standards for safeguarding personal data by business and other private entities. In addition, California should establish a statewide standardized identity theft reporting mechanism. Closing the existing information gap will provide more accurate insights into identity theft trends and levels of occurrence. Establishing a statewide identity theft database will empower law enforcement agencies and consumer groups with better data and enable them to craft better polices to counter identity theft.

Introduction

As technology advances and criminals discover new opportunities, consumers face new threats to their identity. This report looks at recent identity theft cases and examines numerical data provided by the California *High Technology Theft Apprehension and Prosecution* (HTTAP) Program to help consumers and policy makers better understand emergent risks of identity theft.[8] HTTAP data is compiled from actual complaints reported and cases investigated in California rather than surveys and statistical extrapolation, providing a more robust overview of statewide trends.

Protecting the public from identity theft has been at the top of the Californian Public Interest Research Group (CALPIRG) Education Fund's agenda for nearly two decades. Our work includes numerous reports that have helped document the problem of identity theft and highlight policy solutions.[9] Recently, CALPIRG Education Fund has focused special attention on privacy and identity theft issues arising from new technologies. This report continues our tradition of educating California's consumers about the risks of identity theft, empowering them with the knowledge necessary to protect their identity, and providing policy makers with the guidance needed to wage a more effective fight against identity theft.

Our report finds that criminals are utilizing new technologies and implementing new methods to steal consumer's identity and commit fraud. In addition, data indicates that identity theft today is costing consumers more than in recent years, due to the rise in "new account fraud" in which criminals use a victim's personal identifying information and good credit to create new accounts, which are then used to obtain products and services.

Identity Theft 101

Identity theft is a term used to describe a range of criminal acts that use an unsuspecting consumer's "personally identifiable information" (PII) to obtain goods or services or conduct business. The Federal Trade Commission (FTC) defines identity theft as "a fraud that is committed or attempted, using a person's identifying information without authority."[10]

Most identity theft crimes are committed in two steps:

Step #1, Identity theft:
Stealing someone's identity by illegally obtaining personal information such as a Social Security number, date of birth, or bank account information.

Step #2, Identity fraud:
The fraudulent act or financial theft that criminals engage in using the victim's personal information.

Once criminals gain access to a victim's personal information, there are various types of crimes they can commit. For example, criminals can steal money by making purchases with the victim's credit card or removing funds from the victim's bank account. These types of crimes are the most costly form of identity theft.[11] Alternately, criminals will use a victim's stolen identity in order to defraud others, for example, by illegally receiving Social Security benefits or IRS tax reimbursements. In California, this type of identity fraud, relating to government documents and benefits, was the single most common, accounting for 20% of all identity theft complaints.[12] While there are many types of identity theft, all share the common characteristics of illegally obtaining an individual's personal information and then engaging in criminal activity to derive gain using that information.

On March 22, 2012, IRS agents arrested Damon Charles Dubose, an H&R Block office manager in southern California, and charged him with using clients' personal information in an identity theft scheme. Dubose allegedly used personal identifying information of H&R Block customers to prepare bogus tax returns and obtain tax refunds and credits in their names. According to prosecutors, he then used H&R Block Emerald Cards to withdraw the fraudulently obtained refunds from ATM machines. Dubose was caught wearing a disguise near the ATMs of three banks. IRS agents later found $9,860 in cash and H&R Block Emerald Cards, client records with dates of birth, names, and Social Security numbers in his car and at the home of Dubose's girlfriend.

There are various ways identity theft harms consumers. It can lead to monetary loss, harm to reputation, or damage to credit scores and subsequent credit services. Cost to consumers includes out-of-pocket monetary loss and costs relating to the time spent – on average 4 weeks – to resolve problems caused by identity theft.[13]

Identity Theft Techniques

Identifying information exists in many places, over which we often have limited or no control. Consumers can limit and safely store sensitive information in their possession. However, consumers have less control over loan agencies, banks, medical centers, and other business that hold significant amounts of personal information in both print and digital records. From simple techniques – such as stealing letters from a mail box – to more sophisticated data breaches, criminals seek out sensitive personal information wherever it exists, and use different methods to steal people's identities.

What is Data Loss?

In February 2012, St. Joseph's Medical Center in Stockton, California discovered a storeroom break-in at the HealthCare Clinical Laboratory (HCCL) Patient Service Center. Three storage boxes containing HCCL lab requisition forms went missing from the center. The lab forms taken from the center included at least 700 patients' records containing names, insurance information, addresses, phone numbers, and Social Security numbers.

A recent FTC report found that in 12% of identity theft cases, criminals used more than one method of identity theft. The following section describes some of the newer methods criminals use, alone and in combination, to gain access to victims' personal information.

Phishing: Criminals contact consumers pretending to be a trusted service provider (banks, IRS, U.S. Postal Service), and trick victims into sharing with them sensitive information. Often they will ask for account information, login details or other information that will allow them to gain control over a victim's account.

In November 2011, *101Domain.com* - a website that offers domain registration services - suffered a data breach resulting from a phishing attack. Criminals first sent out emails appearing to be official correspondence that directed recipients to phishing sites. Once on the phishing sites, customers were prompted to enter their sensitive information. The attack exposed the names, addresses, email addresses, and in some cases, credit card, PayPal, and bank account information of up to 10,000 customers.

Skimming: This occurs when criminals covertly record credit or debit card information at point-of-sale locations and steal account information and passwords using a small electronic device called a "skimmer." Common scenarios for skimming include restaurants or bars where the person using a skimmer has possession of the victim's credit card out of his/her immediate view or at merchants where criminals install "skimming" devices inside unsupervised card-swiping terminals (such as gas stations).

In March 2012, Gervork Aroutiounyan and Gnel Snapyan were sentenced by a San Luis Obispo County Superior Court for "skimming" debit card information of Chase Bank customers and stealing $320,728. The two operated the scheme across seven counties, including Santa Clara, Marin, Fresno, San Bernardino, San Diego and Los Angeles. Between July 2010 and February 2011, the two men replaced the card readers at Chase Bank ATM machines with "skimmers" which allowed them to retrieve customers' card information. The two also installed micro-cameras to capture the card holders' PIN number.

With the card and PIN information, the two were able to create fake ATM cards that were then used to withdraw money from victim's accounts. The two defendants pleaded guilty to conspiracy to commit grand theft, computer access fraud, identity theft, second-degree burglary, and forgery of access cards.

Social Media: In order to gain access to victim's accounts, criminals often need identifying information such as date of birth, e-mail address, mother's maiden name, or which high school they attended. This information can often be found by searching through publicly available social media web sites. In fact, while the average rates of fraud experienced by consumers nationally in 2011 was 4.9%, according to research 10.1% of LinkedIn users, 7% of Google+ users, 6.3% of Twitter users, and 5.7% of Facebook users had their identities stolen and used for fraud.[14]

Bluetooth Technology: Using various methods, criminals can access devices such as smart phones, laptops, and tablets with active Bluetooth connections and extract personal information. Depending on the device, criminals can access calendars, address books, login information, and even saved documents.

Key-logging: Criminals infect a victim's computer with a malicious software (malware) program that secretly records the letters typed on a computer. By using key-logging malware, criminals see commonly typed phrases and words, which are often a victim's usernames and passwords. A key-logger program does not usually cause any other harm to a computer system, and can therefore go undetected by the victim.

In January 2012, three high-school students were caught selling quiz answers to fellow students. The three had discovered the network passwords of four teachers using a key-logging program installed onto their computers. With the passwords, the three were then able to access the central files on the school network, download tests, and then sell answers other students.

Unsecured WiFi: Criminals can utilize the vulnerabilities of unsecured WiFi hotspots, and access unsuspecting users' devices. Criminals can "pull" information from victims' web-browsers and access account details, credit card numbers, and login information.

Large Scale Data Breach: A security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. The information obtained by either physical loss of data or through a computer intrusion may include financial information (credit card or bank details), personal medical records, personally identifiable information, business trade secrets or intellectual property. Incidents range from concerted attacks by criminal hacker groups, to physical theft of sensitive records (in either print or digital formats), to careless disposal of used computer equipment and lost data storage units.

In January 2012, City College of San Francisco reported that since 1999 their computer systems had been infected by a series of malicious viruses. The data breach was noticed when the College's data security monitoring service detected unusual patterns in computer traffic. An investigation revealed that the college's servers and desktop computers had been infected by viruses that searched and transmitted data to sites in Russia, China, and at least eight other countries.

At the time it was still unclear how much and what type of information was illicitly transferred. Financial information and other personal information belonging to thousands of students, faculty, and visitors using campus computers between 1999 and January of 2012 may have been stolen.

High Technology Crime Task Force In California

The *California High Technology Crimes Task Force* was created in 1998 through Senate Bill *1734 (Johnston)*, to help combat computer-related crimes such as network intrusions, computer hacking, counterfeiting and piracy, theft of trade secrets, and telecommunications fraud. Legislation established the *High Technology Theft Apprehension and Prosecution* (HTTAP) Program, which includes the following five regional Task Forces covering 29 counties encompassing a population of over 31 million people in California:

1. Northern California Computer Crimes Task Force (NC3TF)

2. Sacramento Valley Hi-Tech Crimes Task Force (SVHTCTF)

3. Silicon Valley Rapid Enforcement Allied Computer Team (REACT)

4. Southern California High Tech Task Force (SCHTTF)

5. San Diego – Riverside Computer and Technology Crime High-Tech Response Team (CATCH)

The HTTAP program was expanded in 2001 to include identity theft. The current mission of the HTTAP Program is to investigate, apprehend, and prosecute high technology crimes and to combat identity theft. The Task Force's personnel are highly trained professionals who draw upon the expertise of private industry, academia, and government IT specialists to serve the corporate and individual citizens of California.[15]

Our report is based primarily on numerical data provided by the HTTAP. The strength of this data is that it is compiled from actual complaints reported and cases investigated in California rather than surveys and statistical extrapolation. That said, HTTAP data is collected from only 29 out of California's 55 counties, and relates mostly to identity theft committed using high technology. While not accounting for each and every case of identity theft in California, HTTAP provides the best overview of identity theft cases and trends throughout the state.

What is the law?

In California, identity theft is typically prosecuted under the following Penal Code sections: § 529 – False Impersonation; § 530.5 – Unauthorized Use of Personal Identifying Information; and § 532a – False Financial Statements. Increasingly, criminals are using the Internet to perpetrate identify theft. This provides prosecutors further legal tools to prosecute *Internet Fraud* as defined in California Penal Code § 535 - Internet Auction Fraud and § 487 – Grand Theft.

Recent Trends in California

The data regarding identity theft cases investigated by the five HTTAP task forces in the period between 2007 and 2011 fluctuated due to changes in budgets and resources allocated to their investigations. Nonetheless, in 2011 nearly one

thousand identity theft cases were investigated by the task forces, leading to the arrest of 367 individuals and the prosecution of 344 cases. These investigations examined the loss of nearly $8 million and involved over ten thousand victims of identity theft.[16]

A review of HTTAP data indicates that while fewer people fell victim to identity theft, the dollar loss per victim of identity theft increased substantially.[17] In 2011 HTTAP data showed that the average dollar loss per identity theft victim in California was $786, which was a significant increase from the year before. FTC data also indicates that the average dollar loss per victim in California during 2011 was 4.8% higher than in 2010.[18] Combined, the data indicates that identity theft is costing consumers more today than in recent years past.

This trend can be explained by the rise in "new account fraud", in which criminals use a victim's personal identifying information and good credit to create new accounts, which are then used to obtain products and services. Since the criminal typically submits a different mailing address when applying for new accounts, the victim never receives the bills and remains unaware of their existence until creditors come seeking payment for debts the thief left in the victim's name. This type of financial identity theft takes longer to detect and often results in significant financial loss. New account fraud is on the rise across the U.S., accounting for 46% of identity theft based fraud in 2010, up from 39% in 2009.[19]

How To Prevent Identity Theft

Identity theft is increasing in scope and variety, forcing consumers to learn how to keep private information safe. CALPIRG Education Fund recommends these simple 12 steps to help consumers keep their private information private:

1. Do not disclose your full nine-digit Social Security number unless you have to. Never use it as an identifier or password, and question institutions who ask for it.

2. Avoid paper billing by requesting secure electronic statements instead. If you still require hard copies, you can print them and store them safely rather than risk mail theft.

3. Lock your mailbox.

4. Keep your information safe, both online and offline. Shred documents containing personal information before throwing them away. Password protect sensitive computer files.

5. Use unique hard-to-guess passwords that include a combination of letters, numbers, and symbols.

6. Avoid using the same password across multiple accounts, and change your passwords once or twice per year.

7. Install and update antivirus, anti-malware, and security programs on all computers, tablets, and smart-phones.

8. Don't disclose information commonly used to verify your identity on social network sites. This includes date of birth, city of birth, mother's maiden name, and name of high school.

9. Avoid making purchases, paying bills, or sending sensitive information over unsecured WiFi networks (at airports, coffee shops, or hotels).

10. Disable Bluetooth connections on devices when not in use.

11. Watch out for "phishing" scams. If you receive un-solicited requests for personal information in email or over the phone, ignore them. Instead, use official methods of contact online or by calling the institution's customer service numbers available on statements, back of cards, or on official websites.

12. Fight "skimmers" by not handing your debit card to a server or anyone who could have a hand-held skimming device out of sight. When using ATM machines, touch to see if the all the parts are solid and not add-ons; always cover the hand typing the password; look for suspicious holes or cameras; and avoid using ATM machines in unsupervised locations.

Protecting your Smart-phone and Tablet:

- Set a personal password and protect your smart phone to prevent un-authorized access.
- Use only authorized apps provided by your bank or reputable publishers to access financial information.
- Look for popular apps that have been accessed and downloaded by many consumers. "Wisdom of crowds" is a good indicator if the apps are legitimate and safe to use.
- Keep track of your monthly bills, in case unknown phone calls or service charges are made on your account.

Detecting Identity Theft

Since individuals are likely to be the first to notice when something is wrong, it is no surprise that 45% of identity theft is discovered first by consumers.[20] Heightened consumer vigilance is key to limiting identity theft. To stay on top of account activity, consumers can sign up for email and mobile alerts offered by their bank and credit card servicers. This will enable them to see fraudulent charges or account changes as soon as they happen, limiting the time criminals have to do damage.

Automatic email alerts inform consumers about unusual credit activity and address changes in their accounts. FTC research found that 35% of identity theft victims reported that their bank or credit card provider first alerted them to fraud on their accounts.[21] In 2010, 22% of identity fraud was detected by consumers monitoring their financial accounts for unauthorized address changes, a common method criminals use to take over a victim's identity.[22]

Consumers should review their free annual credit report to ensure that all the accounts and employers listed are accurate. Doing so will alert consumers to fraudulent accounts, loans, and employment criminals may have engaged in using their identity. Free credit reports are available online at AnnualCreditReport.com or by calling 1-877-322-8228. At least 8% of identity fraud was detected by consumers monitoring their annual credit reports.[23]

What to do when you detect identity theft

In addition to financial loss, victims of identity theft spend time and effort undoing the damage left behind by criminals. In order to safeguard themselves from future claims and debt collectors, consumers must establish that they were victims of identity theft, collect supporting documentation, and keep track of the agencies and businesses they have contacted.[24]

Step 1: Notify your financial institutions.

When consumers discover that their wallet, checkbook, credit card or other sensitive information has been lost or stolen, they should immediately notify the issuing bank, credit

Getting Your Free Credit Report

Consumers should avoid the following common mistakes when getting their free credit reports:

1. Mistyping annualcreditreport.com and instead reaching fraudulent or misleading websites offering bogus services.

2. Mistaking "annual" for once a calendar year. Everyone is entitled to a free credit report from each of the three main credit reporting agencies once every 12 months, regardless of the calendar year cycle. Consumers often request a credit report from all three credit services at the same time. Instead, consumers should know that they can request a credit report from one of the credit report servicers every four months.

Avoiding these mistakes will allow consumers to safely monitor their credit activity throughout the year for free.

card or relevant institution to close all existing accounts. Consumers should also immediately report any suspicious activity on their accounts to the relevant institutions. Early reporting is crucial to limiting the time criminals have to damage to their victims' finances or credit.

Step 2: Notify the FTC.

If consumers notice fraudulent activity and suspect identity theft, they should report the suspected cases to the FTC using the online complaint form.[25] In addition to providing further insights into identity theft, reporting to the FTC will help victims develop documentation establishing that they were victims of identity theft. Such documentation will prove helpful later on as victims work to undo damage caused by identity thieves.

How to contact the FTC?

Call the FTC's Identity Theft Hotline toll-free: 1-877-ID-THEFT (438-4338), or write to Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Step 3: File a police report.

Consumers who believe they have fallen victim to identity theft should then file a report with their local police department and retain copies of the police report for future use. In California, local police are required to file an identity theft report documenting a victim's complaint. A comprehensive identity theft police report includes enough information to detail damage caused by identity theft. Consumers should bring a printed copy of the *FTC ID Theft Complaint form*, a prepared cover letter, and supporting documentation when filing a report.[26]

Step 4: Contact one of the three major credit reporting companies and place a fraud alert and security freeze on your account.

An important next step is to place a fraud alert on your credit reports, and review credit reports regularly. Placing a fraud alert will frustrate criminals' efforts to open new accounts in your name in order to commit fraud and minimize future damage. Alerts can be placed by contacting the toll-free fraud number of any of the three consumer reporting companies noted below. Consumers do not need to contact all three, as notifying one will suffice.

- **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
- **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9554, Allen, TX 75013

Consumers should also place a security freeze on their credit reports. This will restrict access to their credit report and reduce the likelihood that criminals will be able to open a new account in their name. Initiating a credit freeze does not impact credit scores nor does it prevent consumers from getting free annual credit reports or from buying their credit reports or scores later on. In California, a security freeze is free for victims who have a police report of identity theft.[27] To place a freeze, victims must contact each of the three credit bureaus noted earlier and provide them with their personal information and a copy of their police report of identity theft.

The difference between a *Fraud Alert* and *Security Freeze*

A fraud alert is a notation on a credit report that a business receives when checking a consumer's credit rating. It tells the business that there may be fraud involved in the account. A security freeze means that a consumer's credit file cannot be seen unless the consumer gives prior consent. Most businesses will not open credit accounts without first checking a consumer's credit history.

Policy Recommendations

Identity theft is the nation's leading method of fraud in the 21st century, with the highest number of complaints nationwide originating here in California.[28] Although there has been significant progress in recent years by both law enforcement agencies and the private sector to combat identity theft there is still room for improvement.

The CALPIRG Education Fund recommends the following actions to wage a more effective fight against identity theft and reduce its incidence and damage.

1. California state law prohibits organizations, both private and public, from using a Social Security number as a personal identifier and from publicly posting or displaying that number.[29] Yet while organizations continue to collect Social Security numbers, authorities should investigate the present usage of Social Security numbers by government agencies and private business to determine if alternative means of identification can be used. This will reduce the amount of Social Security numbers collected and reduce risks for consumers.

2. Establish statewide laws requiring minimum standards for safeguarding personal data by business and other private entities.

3. Ensure sufficient resources and funding are provided to HTTAP and other law enforcement efforts combating identity theft.

4. Establish a statewide standardized reporting mechanism for law enforcement agencies regarding identity theft investigations.

Closing the existing information gap will provide more accurate insights into identity theft trends and levels of occurrence. Establishing a statewide identity theft database will empower law enforcement agencies and consumer groups with better data and enable them to craft better polices to counter identity theft.

Appendix

HTTAP High Technology Crime in California - FY 10/11 Report

Group	# Cases Investigated	# Of Victims	$ Loss To Victims	$ Cost Per Victim	# Of Arrests	# Of Criminal Cases Filed	# Of Convictions
Northern California (NC3TF)	79	553	$77,479	$140	38	49	17
Sacramento Valley (SVHTCTF)	602	2,178	$2,030,778	$932	197	178	130
Silicon Valley (REACT)	59	5,918	$47,318	$8	35	64	15
Southern California (SCHTTF)	225	1,409	$5,763,635	$4,091	85	42	52
San Diego (CATCH)	32	117	$80,026	$684	12	11	15
2011 TOTAL	**997**	**10,175**	**$7,999,236**	**$786**	**367**	**344**	**229**

HTTAP High Technology Crime in California - FY 09/10 Report

Group	# Cases Investigated	# Of Victims	$ Loss To Victims	$ Cost Per Victim	# Of Arrests	# Of Criminal Cases Filed	# Of Convictions
Northern California (NC3TF)	35	181	$1,153,580	$6,373	8	0	8
Sacramento Valley (SVHTCTF)	180	29,946	$1,344,820	$45	151	365	115
Silicon Valley (REACT)	114	380	$2,038,742	$5,365	41	21	19
Southern California (SCHTTF)	90	111,690	$6,595,173	$59	234	130	68
San Diego (CATCH)	49	77	$500,828	$6,504	15	13	9
2011 TOTAL	**468**	**142,274**	**$11,633,143**	**$82**	**449**	**529**	**219**

Notes

1. *High Technology Crime in California FY 2010-2011*, High Technology Crime Advisory Committee, January 2012. p.5.

2. *Sentinel Network Data Book, January-December 2011,* Federal Trade Commission, February 2012, p.9.

3. *High Technology Crime in California FY 2010-2011*, High Technology Crime Advisory Committee, January 2012.

4. A comparison of FTC data show that the dollar loss from identity theft in 2011 was $210,644,569 compared to $200,997,812 in 2010. *Sentinel Network Data Book, January-December 2011,* Federal Trade Commission, February 2012, p.87.

5. *2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier,* Javelin Strategy & Research, February 2012.

6. *2011 Identity Fraud Survey Report: Consumer Version*, Javelin Strategy & Research, February, 2011, p. 5.

7. See Cal. Civ. Code § 1798.85 (2001).

8. Learn more online at : http://oag.ca.gov/ecrime/httap

9. Some examples of our work include the 1996 ground breaking report "Theft of Identity: The Consumer X-Files," which offered a comprehensive overview of the then-nascent but growing problem of identity theft; our 2000 "Nowhere to Turn: Victims Speak Out on Identity Theft" report surveying the cost of identity theft to victims; and our 2003 report "Policing Privacy: Law Enforcement's Response to Identity Theft" for which we interviewed and surveyed police officers investigating identity theft.

10. The rule also states that "identifying information" should have the same meaning as "means of identification" in the federal criminal statute defining identity theft. See *FTC Issues Final Rules on FACTA Identity Theft Definitions, Active Duty Alert Duration, and Appropriate Proof of Identity,* FTC, October 29, 2004.

11. *High Technology Crime in California FY 2010-2011*, High Technology Crime Advisory Committee, January 2012, p.5.

12. *Consumer Sentential Network Data book: January – December 2011*, Federal Trade Commission, February 2012, p.27.

13. *High Technology Crime in California – FY 09/10*, High Technology Crime Advisory Committee, December 2010, p.3.

14. *2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier,* Javelin Strategy & Research, February 2012.

15. High Technology Theft Apprehension and Prosecution (HTTAP) Program description, available online at: https://oag.ca.gov/ecrime/httap

16. *High Technology Crime in California FY 2010-2011*, High Technology Crime Advisory Committee, January 2012.

17. See appendix for a full comparison of 2011 and 2010 HTTAP data.

18. A comparison of FTC data show that the dollar loss per victim in 2011 was $2,839 was compared to$2,769 in 2010. *Sentinel Network Data Book, January-December 2011,* Federal Trade Commission, February 2012, p.87

19. *2011 Identity Fraud Survey Report: Consumer Version*, Javelin Strategy & Research, February, 2011, p.5.

20. *2011 Identity Fraud Survey Report: Consumer Version*, Javelin Strategy & Research, February, 2011, p.14.

21. *2011 Identity Fraud Survey Report: Consumer Version*, Javelin Strategy & Research, February, 2011, p.14.

22. *2011 Identity Fraud Survey Report: Consumer Version*, Javelin Strategy & Research, February, 2011, p.14.

23. *2011 Identity Fraud Survey Report: Consumer Version*, Javelin Strategy & Research, February, 2011, p.14.

24. The FTC provides a simple tracking form available for download at: http://www.ftc.gov/bcp/edu/resources/forms/chart-course-action.pdf

25. Available online at : https://www.ftccomplaintassistant.gov/

26. More information is available online at: http://www.ftc.gov/bcp/edu/microsites/idtheft//instructions1.htm

27. For more information on the process and costs associated with setting up an security freeze in California, see: http://www.privacy.ca.gov/consumers/cis10english.pdf

28. *High Technology Crime in California FY 2010-2011*, High Technology Crime Advisory Committee, January 2012, p.5.

29. See Cal. Civ. Code § 1798.85 (2001).