JAVELIN STRATEGY & RESEARCH

SYNDICATED RESEARCH
CUSTOM RESEARCH
STRATEGIC CONSULTING

2011 Identity Fraud Survey Report: Consumer Version

Prevention – Detection – Resolution ™

February 2011

4301 Hacienda Drive, Pleasanton, CA 94588 USA ● +1 925.225.9100 t ● +1 925.225.9101 f ● www.javelinstrategy.com

Table of Contents

Table of Figures

Where Can I Get the Industry Version of the 2011 Identity Fraud Survey Report?

If you represent a business or are a professional looking for a more detailed analysis of identity fraud from our 2010 Identity Fraud Survey, please reference the full report, entitled:

2011 Identity Fraud Survey Report:
Identity Fraud Decreases – but Remaining Frauds
Cost Consumers More Time & Money

The full report consists of **96** pages with **73** graphs and tables. You can purchase it on the research page of our website at www.javelinstrategy.com/research or by contacting Paul Zegar at 925-218-4724. The sole purpose of the consumer version is consumer education and awareness. Javelin recommends purchasing the full report for a complete analysis, including an overview of the key findings, trends, quantitative cross tabulations and longitudinal U.S. identity fraud data from 2003 to 2010.

Authors: Danielle Miceli, Associate Analyst
Robert Vamosi, Analyst, Security, Risk and Fraud

Contributors: Mary Monahan, Managing Partner and Research Director
James Van Dyke, President and Founder

Research: Mark Ayoub, Associate Analyst
Shailaja Dixit, Analyst
Rachel Townsend, Analyst

Publication date: February 2011

Javelin's 2011 Identity Fraud Survey Report: Consumer Version provides tips and recommendations to help consumers prevent, detect and resolve identity theft and fraud. This study will assist consumers in lowering their risk of identity fraud by equipping them with the tools and resources necessary to detect and resolve this crime. Over the past eight years, Javelin has surveyed approximately 35,000 adults to determine how consumers are being affected by identity fraud in the United States. The 2010 phone survey of 5,004 adults is the largest, most accurate identity fraud study in the United States. Javelin's identity fraud study reaches an audience of 63 million and is a factual resource for the Federal Trade Commission (FTC) and Better Business Bureau (BBB).

For commercial institutions wanting to view the complete version of this research study, the *2011 Identity Fraud Survey Report*: (96 pages) is available for purchase.

This research study is made possible by Fiserv, Inc., Intersections Inc. and Wells Fargo & Company, companies committed to helping consumers reduce their risk of identity fraud. Through their sponsorships, they have contributed to combating identity fraud and educating consumers. The Better Business Bureau also supports this study.

Javelin maintains complete independence in its data collection, findings and analysis; the report is a product of Javelin employees only. The sponsors' contributions to the study include partially underwriting the costs for data collection, analysis and reporting.

About Javelin

Javelin Strategy & Research provides superior direction on key facts and forces that materially determine the success of customer-facing financial services, payments and security initiatives. Our advantages are rigorous process, independent position and expert people.

OVERVIEW

The good news is that identity fraud decreased sharply in 2010, after increasing for two years. Approximately 8.1 million Americans, or 3.5% of the total U.S. population, learned that they were victims of identity fraud in 2010. This crime affected 3 million fewer people than in 2009. At $37 billion, the annual overall fraud amount was at its lowest point since the survey began in 2003.

Although the number of incidents of identity fraud has dropped and there are fewer victims, the remaining frauds are more difficult to detect and resolve, resulting in higher consumer costs. Average (mean) consumer costs in 2010 were at $631, their highest level since 2007, although the median consumer cost remained at $0. Consumer costs are any out-of-pocket expenses suffered by the fraud victim, including unreimbursed monetary losses, and lost wages as a result of time spent to resolve the fraud as well as any related legal costs and credit monitoring costs. Because of the zero-liability fraud protection offered by the majority of banks and card issuers, most victims will have to pay out-of-pocket expenses only to cover their time in resolving fraud, not to reimburse fraudulent charges. The average time to resolve identity fraud in 2010 rose to 33 hours, up 12 hours from 2009. Resolution times are now at their highest point since 2005 when they were at 40 hours.

A major reason for the rise in consumer costs and resolution times is explained by the relative rise in new account fraud. New account fraud is now responsible for almost half of the total dollar amount lost to identity fraud (46% in 2010 vs. only 38% in 2009). New account fraud on average takes longer to detect and results in higher mean consumer costs than other types of fraud, such as existing account fraud and non-card fraud. This is partly because new account fraud typically requires a credit report or use of a credit monitoring service to detect; thus, stopping the fraud requires teamwork between consumers and businesses.

The longer identity fraud goes undetected, the more expensive and difficult to resolve it tends to be for the consumer. Therefore, it is vital for consumers to monitor their accounts frequently and to partner with their financial institutions to help prevent, detect and resolve fraud. About half of identity frauds are detected by consumers, and half are detected by third parties (45% vs. 55%). Banks, credit unions and credit card issuers detect more identity fraud but often need the cooperation of their customers to stop incidents quickly.

Since 2003, Javelin has collected data from approximately 35,000 adults to measure the overall impact of identity fraud on consumers. In 2010, 5,004 adults, including 470 actual fraud victims, answered questions regarding their daily financial practices and behaviors to help determine the potential causes of such fraud as well as to provide detailed information regarding their fraud.

This report provides easy-to-follow guidelines and recommendations for consumers to protect themselves against this $37 billion crime. Javelin's goal is to equip consumers with proven methods to prevent, detect and resolve identity fraud. The recommendations in this report are based on the results of our 2011 report and are backed by the most up-to-date identity fraud findings available.

A deeper analysis of economic indicators and identity fraud trends is available in the full version of the 2011 Identity Fraud Survey Report, along with a detailed breakdown of how different economic factors, payment purchasing trends and security dynamics correlate with the change in identity fraud.

Figure 1: Javelin's Prevention, Detection and Resolution Identity Fraud Model

Figure 1: Javelin's Prevention, Detection and Resolution Identity Fraud Model

Identity Fraud vs. Identity Theft

Most individuals are familiar with the term "identity theft," which is widely used by media, government and consumer groups and by nonprofit organizations. However, it is important to distinguish between identity theft and identity fraud because the terms have different meanings, although Javelin uses identity fraud more commonly throughout the identity survey and corresponding reports.

True *identity theft* occurs after the exposure of personal information; typically someone's personal information is taken by another individual without explicit permission. *Identity fraud is the* actual misuse of information for financial gain and occurs when criminals use illegally obtained personal information to make purchases or withdrawals, create false accounts or modify existing ones and/or attempt to obtain services such as employment or health care. Personally identifiable information (PII) such as a Social Security number (SSN), bank or credit card account number, password, telephone calling card number, birth date, name and address can be used by criminals to profit at a victim's expense.

By accessing and using relatively basic information, a criminal can take over existing financial accounts (existing card fraud or existing non-card fraud) or use a victim's personal information to create new accounts (new account fraud). A criminal can commit identity fraud numerous ways, including making an unauthorized withdrawal of funds from an account or making fraudulent purchases with a credit card and creating new accounts (banking, telephone, utility, loans). All of which can have a damaging effect on an individual's credit. In fact, the first notification that fraud has been committed might be the appearance of an unfamiliar account on a credit report or contact from a debt collector.

Methods Criminals Use to Obtain Information

Many identity thefts occur through traditional methods such as stolen wallets and "friendly frauds," in which a person known to the victim has access to statements or other legal documents.

Identity theft occurrences are often the result of simple lost or stolen information and not necessarily through hacking or elaborate Internet schemes, although online and mobile threats are viable. Figure 2 shows some of the many ways that identity theft can occur.

Identity Theft Occurs Through Various Methods

Figure 2: How Theft of Personal Information Happens

At home:	**While you are out:**
Through information left out in the home (or at work) and stolen by family or friends	By means of a lost or stolen wallet or purse
Through "dumpster diving" by crooks looking for unshredded paperwork that contains personal or financial information	Through "shoulder surfing," in which someone obtains personal information by looking over an unsuspecting individual's shoulder
Through theft of your mail from your mailbox or diversion of your mail by a fraudster who changes the address to obtain your account statements	By card skimming, when someone illegally records an imprint of your credit or debit card information for later use
Through a business you use:	**By trickery or pretense:**
Through a security data breach, whereby a business or organization that accesses your personal information (hospital, school, department store, financial company, etc.) has been compromised	Through phishing or vishing, in which someone pretends to be a bank or trusted company and tricks you into providing confidential personal information via e-mails, calls or SMS/text messages
Through hacking incidences, such as Trojan horses, keylogger software, viruses or malware/spyware on a computer	Through social networking sites where personal information can be found and communication with fraudulent individuals can occur
Through these and other new and innovative ways that criminals are constantly developing	

What Should I Do If I Receive a Breach Notification Letter?

Currently, 46 states require companies to notify you if a breach of security occurs at their place of business and your personal information has been placed at risk. Each year, many consumers receive "breach notification" letters; in 2010, 7% of U.S. consumers received these notifications. Although this notification does not necessarily mean that you will suffer a fraud, Javelin data shows that consumers who received breach notifications in 2010 had more than four times higher risk of identity fraud than did those who didn't receive these types of notifications.

Take Action to Protect Yourself If You Receive a Security Breach Notification

Figure 3: Consumers Who Receive Breach Notifications Are at Significantly Higher Risk of Fraud

Consumers who receive security breach notifications therefore need to take action to protect themselves, and are strongly encouraged to take advantage of any free services offered in the notification letter, such as credit monitoring. They should also use the toll-free numbers or websites identified in the letter to gain information about the breach, to determine their level of risk, and to identify the actions needed to protect against further damage. Different breaches have different levels of risk and require different actions from consumers to protect against further harm.

These actions may include:

- Monitoring financial accounts
- Closing affected accounts
- Placing a fraud alert on a credit report with the three primary credit bureaus: Equifax, Experian and TransUnion (refer to Figure 4 for contact details)
- Placing a credit freeze on an account with the three primary credit bureaus

Credit Bureau Information

Figure 4: How to Contact the Three Credit Bureaus

Credit Bureau	Equifax	Experian	TransUnion
Order credit report	800-685-1111	888-397-3742	800-888-4213
Report fraud	888-766-0008	888-397-3742	800-680-7289
Web address	www.equifax.com	www.experian.com	www.transunion.com
Mailing address	Equifax Consumer Fraud Division P.O. Box 740241 Atlanta, GA 30374	Experian Consumer Assistance P.O. Box 9532 Allen, TX 75013	TransUnion Victim Assistance Dept. P.O. Box 6790 Fullerton, CA 92834
Note: To order a free annual credit report from any or all agencies, contact www.annualcreditreport.com or call toll free at 877-322-8228.			

Fraud alerts notify creditors that a potential fraud has occurred and that they should verify the identity of the applicant before extending credit. An initial alert stays active for 90 days, and an extended alert for identity fraud victims lasts seven years. A fraud alert will trigger a credit report, which the consumer needs to review carefully for any signs of fraud. A credit freeze is even stronger than a fraud alert because it locks down the consumer's credit report to prevent new credit from being extended. Consumers should continue to frequently monitor their existing accounts.

Because identity theft can occur via numerous methods, consumers should protect themselves through a variety of best practices and effective behaviors. Javelin recommends a comprehensive, three-part approach to address and combat identity fraud effectively: prevention, detection and resolution. The next section provides steps to prevent fraud from happening, actions to detect fraud if it does occur and ways to resolve fraud if you become a victim.

CONSUMER RECOMMENDATIONS

Prevention

- Keep sensitive information from prying eyes. At home or work, secure your personal and financial records in a locked storage device or in a password- protected file— in 2010, 14% of all identity fraud crimes were committed by someone known to the victim.
- Avoid providing your full 9-digit SSN whenever possible. When your Social Security number is requested as an identifier, ask if you can provide alternate information. In 2010, Javelin surveyed 5,004 adults and found that among the 470 fraud victims, 29% reported having their SSN stolen.
- Request electronic statements and use online bill pay whenever possible. Enroll in direct deposit, shred sensitive paper documents, and don't put checks in an unlocked mailbox.
- Watch out for convincing imitations of banks, card companies, charities and government agencies. Never respond directly to requests for personal or account information online, over the phone, on email, or through the mobile device -- including SMS text messages. Instead, use legitimate sources of contact information to verify requests for information such as your financial institution's official website or the telephone number listed on statements and the back of bank or credit cards.
- Be aware of the dangers of online threats and install anti-virus and anti-malware software on your computer, and keep it updated along with applications, browsers, and operating systems. Install security patches and software updates as soon as they are released by verified sources.
- Don't publish your birth date, email address, mother's maiden name, pet's name or other identifying or personal information on social networking sites. Use privacy settings on social networking sites to control who is able to access personal profile information.
- Use unique and hard-to-guess passwords that combine letters, numbers, and symbols, and change passwords regularly. Use strong passwords for wireless Internet connections, and don't access unsecure websites or type in personally-identifiable information using public Wi-Fi on mobile devices, laptops, or computers. Turn off Bluetooth and Wi-Fi when they are not being used.

Detection

- Monitor bank and credit card accounts at least weekly via online, mobile, ATM, or touch-tone banking.
- Monitor your credit and public information to spot unauthorized activity. Free credit reports from each of the three major credit bureaus (staggered quarterly for year-round monitoring) are available yearly through annualcreditreport.com or 877-322-8228. Optional fee-based services, such as more extensive monitoring of credit information, personal identity records, and Social Security numbers provide extra security and convenience for those who don't want to personally monitor their information. When choosing an identity protection service, select a provider that encompasses both personal information and credit monitoring.
- Sign up for security alerts to be sent to your mobile phone or email account so that you are notified of changes to your account or personal information. The most common method for fraudsters to take over a victim's account is by changing the physical address.
- If you receive a letter notifying you that your private records were involved in a data breach, take the following steps: 1) confirm the letter is legitimate, 2) take advantage of any free protection services that are offered, and 3) place a fraud alert on your credit report. A fraud alert requires lenders to make sure it is actually you applying for credit. Consumers who receive a data breach notification letter are more than four times as likely to become identity fraud victims versus those who don't, yet many who are alerted fail to take action.

Resolution

- Report problems immediately and work with your bank, credit union or identity protection services provider to take advantage of resolution services and reimbursement policies.
- Educate yourself regarding your financial institution's and issuer's zero-liability protections of debit cards and ATM withdrawals as they vary among providers. Report all lost or stolen cards and/or fraudulent transactions immediately as the timing of your report of the loss or unauthorized transactions may impact the amount that you are liable for under the law.

PREVENTION

Consumers can best prevent identity fraud by carefully protecting their sensitive information, such as PINs, banking and account numbers and Social Security numbers as well as by limiting the exposure of personally identifiable information. Consumers also should be aware of common fraudster techniques, such as phishing, vishing, smishing and other scams.

How Can I Prevent Identity Fraud?

Javelin recommends taking the following steps to prevent identity fraud:

Regularly install and update firewall, antivirus and antispyware software on your computer (and mobile device when possible). Also, make sure all operating systems and browser settings are the latest versions.

Do not reveal sensitive or personal information on social networking sites. This includes Facebook, Flickr, Friendster, LinkedIn, MySpace and Twitter. These sites can provide fraudsters with personal information to access accounts. Also, take advantage of privacy settings so that you can control who sees your profile information.

Recognize secure websites. Do not provide card or personal information at unsecured sites. Extended-validation Secure Sockets Layer (EV SSL) and SSL sites are the most secure and use encryption and other security methods to protect consumer information. To recognize these sites, look for a padlock symbol and an "s" after the "http" in the address bar (https). If you double-click on the padlock symbol, the SSL certificate will appear. If the website has an additional layer of security (EV SSL), green highlighting will appear in the address bar when you access the site using a high-security browser. High-security browsers are safer for consumers to use (i.e., Microsoft Internet Explorer 8, Firefox 4, Opera 11, Safari 5, and Google Chrome 10).

Reduce unnecessary access to financial cards and documents. Do not carry around Social Security cards or unnecessary credit cards or checks. Shred documents with sensitive information prior to disposal, and keep your documents and all personal information in a safe place, inaccessible to those around you.

Opt out of preapproved credit offers. Call 1-888-5-OPTOUT (1-888-567-8688) or visit www.optoutprescreen.com to be removed from credit card applications and other mail that contains personal information.

Follow safe password practices. Make your passwords at least eight characters long and change them frequently. They should contain at least one combination of upper/lowercase letters, numbers or symbols. Store them in a safe, protected place, not near a computer. Do not use easily guessed passwords, such as your birth date, the name of a close relative or your pet's name. Do not use dictionary words, the name of the website or the word ''password.'' Capitalized letters shouldn't be the first character (capitalize a random letter) and numbers should be integrated throughout the password.

Use secure Internet connections. Avoid accessing websites displaying personal or account information using unsecured Wi-Fi connections, such as those at coffee shops, libraries or airports. Also ensure that the Internet connections you use at home and at work are through a secure network protected by firewalls.

Be aware of your surroundings. Be mindful of people in close proximity who could overhear or watch as you access sensitive financial or personal information when you are talking on the phone, logging into websites, purchasing goods at stores or reading sensitive documents.

DETECTION

It is critical that consumers detect fraud as early as possible to minimize potential losses and fraud resolution time. Faster detection results in lower out-of-pocket expenses, which include unreimbursed losses, legal fees and lost wages. The sooner fraud is detected, the easier it is to resolve and the less the criminal is able to steal.

How Can I Detect Identity Fraud?

Javelin research has consistently shown that consumers can be very successful at detecting identity fraud relating to their accounts. The most efficient way to combat fraud is for consumers and institutions (banks, government agencies such as the Federal Trade Commission and other organizations dedicated to fighting fraud) to work together. Consumers must be proactive in their approach to protect themselves against fraud and should work with institutions to safeguard their identity.

Javelin recommends doing the following to detect fraud early:

Monitor your credit report on a regular basis. Review and confirm that all the accounts listed belong to you and that no unauthorized charges have been made or unknown accounts or credit lines have been opened. Free reports are available at AnnualCreditReport.com or by calling 1-877-322-8228. By contacting a different one of the three credit bureaus every four months, you can stagger your free reports to review your credit report three times a year at no charge.

Sign up for e-mail and mobile alerts through your primary bank and credit card company. Set up e-mail and SMS/text alert notifications through financial institutions so that they will alert you of suspicious activities and changes to your accounts or personal information. From a wide array of alert offerings, you can choose the ones most relevant to your typical banking behaviors and practices, thereby increasing identity fraud protection. Change to a physical address is the most common method used by fraudsters to take over accounts, so set up an address-change alert whenever possible.

Review financial statements promptly. Check account balances at least weekly through online banking, mobile banking, the phone or ATM. Regularly monitor all financial accounts electronically, including banking, biller and credit card accounts. Consumers who discover fraud using electronic vs. paper-statement monitoring have shorter detection times. Confirm that all transactions are authorized and that no suspicious activity has occurred or unapproved changes have been made to your accounts.

Customers are able to effectively detect fraud by taking advantage of the tools offered by financial institutions such as e-mail, SMS/text alerts, mobile banking and online banking. These easy-to-use methods allow consumers to constantly monitor their financial accounts to quickly detect identity fraud. Credit monitoring or personal information monitoring services are fee-based identity protection solutions that can help to detect any fraudulent new accounts.

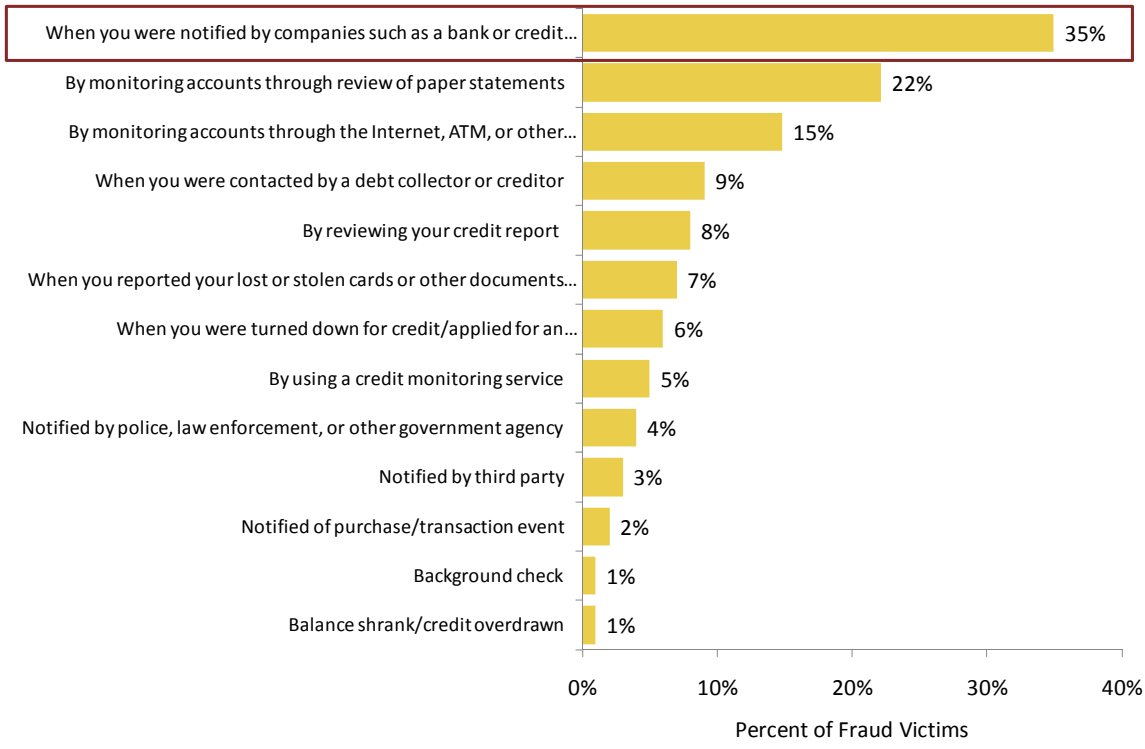
How Is Identity Fraud Detected?

Notification by financial institutions and credit card issuers was an especially prevalent and successful detection method in 2010; 35% of victims reported that their bank or card provider notified them of fraud on their accounts. Financial institutions continue to lead in detecting and informing fraud victims, effectively monitoring accounts on the back end and quickly alerting customers when they detect suspicious activity.

But it is equally important for consumers to recognize how important their own account monitoring is toward stopping fraud. The next two most frequent methods for victims to discover fraud were through their own review of either paper or electronic statements.

Notification by Financial Institutions and Credit Card Providers Leads Detection Methods

Figure 5: Detection Methods for Identity Fraud, 2010



November 2010, n = 439
Base: All fraud victims.
© 2011 Javelin Strategy & Research

Q22: How did you first discover you were a victim of identity theft?

Financial account protection is a shared responsibility of financial institutions (FIs) and customers:

45% of identity frauds are discovered by consumers and 55% are detected by third parties.

RESOLUTION

What Should I Do If I Become a Victim of Identity Fraud?

The first thing to remember if you become a victim or identity theft or fraud is not to panic. When it comes to your financial accounts, banks and credit card providers are prepared to deal with identity theft resolution. There is most likely a team dedicated to resolving identity fraud and guiding victims through the process. By following the few simple steps below, you can help ensure that your fraud case is handled as quickly and as painlessly as possible. These actions can serve as a checklist/ resource guide if you become a victim.

Immediately contact your bank and credit card companies. If physical documents such as a checkbook, wallet, debit card or credit card are lost or stolen, if unauthorized account activity (suspicious transactions) occurs, if changes are made to personal information (e.g. physical address, e-mail address, registered users, login or password) or if paper statements are turned off, notify the appropriate institutions as soon as possible. Depending on the individual case, a financial institution may close your account, cancel your debit or credit cards and take other necessary precautions. Banks and card issuers will also assist you in setting up new accounts and will issue new debit and credit cards.

Contact the Federal Trade Commission. To report incidents of suspected fraud or identity theft, contact the FTC online at www.ftc.gov/bcp/edu/microsites/idtheft to fill out a complaint form or call 1-877-IDTHEFT (1-877-438-4338). Alternately, the FTC can be reached at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Place a fraud alert on your credit report. If your personal information has been compromised or if you have been a victim of fraud, immediately contact the three primary credit reporting agencies: Equifax, Experian and TransUnion (refer back to Figure 4 for contact information). All of these companies provide credit monitoring services as well as additional products and services. Fraud alerts notify creditors that a potential fraud has occurred and that they should verify the identity of the applicant before extending credit. An initial alert stays active for 90 days, and an extended alert for identity fraud victims lasts seven years.

Consider placing a security freeze on your credit report. If you have been a victim of new account fraud more than once and are not actively applying for credit, you may want to place a security freeze on your credit report at each of the three reporting agencies. A security freeze will block access to your credit report, and will help stop new account fraud from occurring, but it will not stop existing account fraud. You should also obtain a copy of your free credit reports to see if the fraud has already occurred.

File a police report. If fraud has occurred, contact your local police agency to fill out an identity fraud report. Make sure to save a copy for your personal records.

Make sure that you review and are familiar with your banks' and card issuers' zero-liability policies. There are often limitations on your protections and coverage, depending on when the fraud is reported, as well as additional restrictions on debit cards and ATM withdrawals.

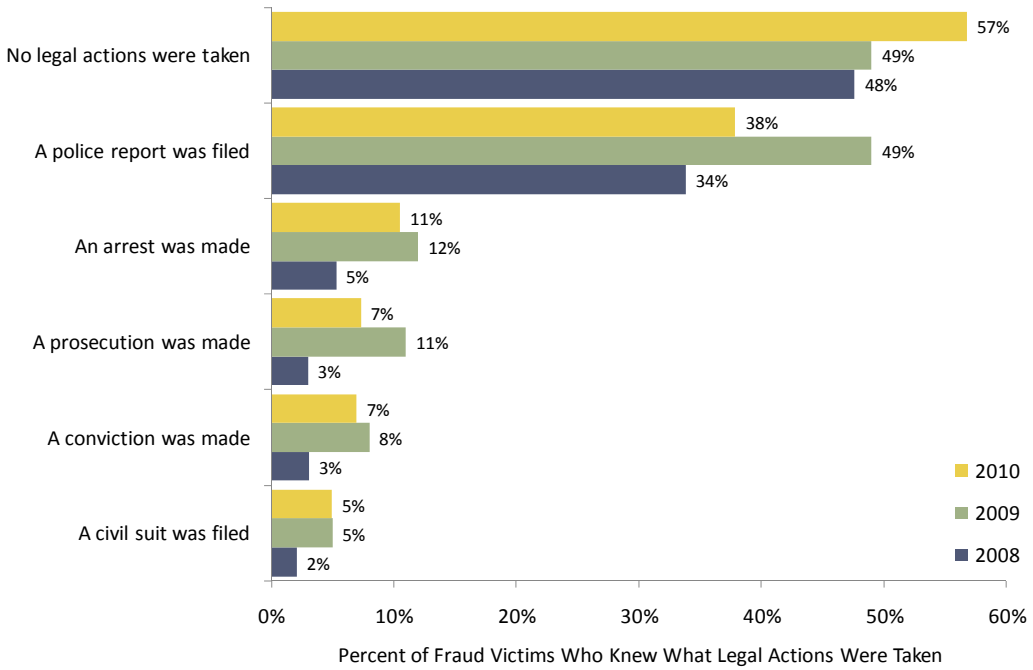
How Consumers React to Identity Fraud

The number of consumers who are taking legal action when they become fraud victims is decreasing. Many victims find they need a police report to prove their status, yet the number of victims filing a police report in 2010 dropped by 11 percentage points from 2009, and 57% took no legal action. Minor decreases also occurred in the number of arrests, prosecutions and convictions.

The Albert Gonzalez high-profile data breach case in 2009 may have contributed to the unusual jump in legal reporting that year.[1] Albert Gonzalez was the leader of a ring of computer hackers who was arrested in 2008, faced further indictments in 2009 and was convicted of fraud and sentenced to 20 years in prison in 2010 by the U.S. Department of Justice. His group was responsible for hacking into the customer databases of companies that included TJX and Heartland and affected over 100 million accounts. Law enforcement agencies worked diligently to shut down this multinational ring; the frequent media attention may have raised consumer awareness about this particular crime in 2009.

Fewer Consumers Are Taking Legal Action

Figure 6: Legal Actions Taken by Fraud Victims, 2008–2010



November 2010, 2009, 2008, n = 374, 551, 452
Base: All fraud victims excluding those who did not know or refused.

Q37: Which legal actions were taken since you became a fraud victim?

After becoming fraud victims, many respondents say they are taking preventive measures against identity fraud: More than half install antispyware or a firewall on their computer and use online banking, while almost half receive e-mail or mobile alerts regarding credit card or checking accounts at higher rates than in the previous year. Consumers are able to take further precautions by using sites that offer Verified by Visa and MasterSecure when shopping online.

[1] **2010 Identity Fraud Survey Report: Identity Fraud Continues to Rise – New Accounts Fraud Drives Increase; Consumer Costs at an All-Time Low**, Javelin Strategy & Research, February 2010.

Identity Fraud Protection Solutions

In addition to the guidelines and recommendations throughout the report, there are specific services for consumers who want extra protection against new account fraud – the type of fraud in which a criminal uses a victim's Social Security number and other pieces of personally identifying information to create a fraudulent account in the victim's name (e.g., a credit card account, a cell phone account or utility account) — and other types of fraud. As mentioned earlier, new account fraud now accounts for almost half of the total annual dollar amount of identity fraud (46%). Identity protection services such as credit monitoring and personal information monitoring services can be purchased for a fee. Javelin advises consumers purchasing fee-based services to look for the firm's BBB approval rating. These services can provide peace of mind and convenience for worried consumers who may want extra protection.

Credit Monitoring and Personal Information Monitoring Identity Protection Services Available

Figure 7: Identity Fraud Protection Services

Service	Description
Credit monitoring	• A paid subscription service that monitors your credit for suspicious activity or changes to your credit file (e.g., credit inquiries, employment changes, new accounts or address changes) • **Intended to detect potential identity fraud**
Personal information monitoring	• Scans public records, third-party databases and Internet sites to detect exposure of your personal information (credit card numbers, Social Security numbers, etc.) • **Intended to detect potential identity theft**
Fraud alert	• A message that is placed on your credit report, requiring lenders and creditors to confirm your identity before issuing a new line of credit • **Intended to prevent new account fraud**
Credit freeze	• Freezes your credit file at the credit reporting agencies, which are then prohibited from issuing your credit history to any lender, creditor or other individuals • **Intended to prevent new account fraud**

Credit monitoring services are generally fee based, although many consumers receive them free as part of a data breach settlement. These services regularly monitor your credit for suspicious activity and changes to your credit file. Changes include credit inquiries, public records, delinquencies, negative billing information, employment changes, new accounts and address changes. E-mail alerts are sent when abnormal activity is detected. Credit monitoring is designed to detect potential fraud as soon as possible after it has occurred and is one of Javelin's best customer safety preventive recommendations because it is extremely effective in early detection of fraud. Although many services offer monitoring for only a single credit bureau, single-bureau monitoring is not as effective as monitoring at all three credit bureaus because many lenders will contact one bureau and not the others.

Personal information monitoring is a paid service that scans public sources of information, including Internet sites, public records and even carding forums (underground sites where stolen cards are bought and sold) to detect if your personal information has been compromised. In using this service, you can determine if changes have been made to your accounts or information. The most complete identity protection services offer both personal information monitoring and credit monitoring.

Fraud alerts are a consumer's right under the Fair and Accurate Credit Transactions (FACT) Act. If you think you may have been a victim of fraud, you can set up a fraud alert by contacting the fraud departments of the three major credit bureaus and asking them to mark their credit files. Each bureau is required by law to notify the other two agencies, but Javelin and consumer privacy advocates recommend placing alerts at all three bureaus. Fraud alerts are an important feature in preventing someone from opening a fraudulent new account (such as a new credit card or loan) in your name. When an alert is in place, creditors are signaled that a possible fraud has occurred and that they should use additional measures to verify that consumers applying for credit are really who they say they are.

Because new accounts fraud is the most expensive and most difficult type of fraud to resolve, consumers should take advantage of fraud alerts as a critical, preventive service. Fraud alerts initially remain in place for 90 days, after which the consumer will need to renew the alert. The initial alert will generate a credit report, which the consumer should carefully review for signs of fraud. Victims who can document fraud according to set criteria can qualify for the seven-year fraud alert. A seven-year fraud alert requires creditors to contact the consumer by phone, in person or through the manner in which the consumer indicates before extending credit, raising limits or adding new users. An active-duty alert is available to active-duty military personnel. The active-duty alert lasts 12 months and includes name removal from prescreened credit or insurance offers for two years.

Credit freezes lock down your credit file and prevent any lender or creditor from accessing your credit history. This service is designed to block new credit from being issued in your name and is a stronger prevention method than a fraud alert. If you are a victim of identity fraud, depending on the state in which you live, you may qualify for free coverage. If you are not eligible for free coverage, it may cost up to $30 to place a freeze at the three bureaus and $30 to remove it (costs can vary by state law). Credit freezes are recommended only for people who will not be actively applying for credit. If you place a credit freeze, you cannot apply for new credit unless you remove or temporarily lift the freeze, which could take a few days. Many consumers are surprised at how often their credit reports are reviewed for such activities such as getting a new job, opening a new utility account or taking out a new insurance policy.

ADDITIONAL RESOURCES FOR MORE INFORMATION

There are a number of places to get more information. Javelin has used the results of its study to create an easy-to-use safety quiz and a list of recommended tips, which can be accessed at:

www.IDsafety.net

The 2011 Identity Fraud Report's sponsors, Fiserv, Intersections Inc. and Wells Fargo & Company, also make safety recommendations:

Fiserv, Inc.
www.ebillplace.com/staysafe

Intersections Inc.
www.identityguard.com/consumer-tools

Wells Fargo & Company
www.wellsfargo.com/privacy_security/fraud/

METHODOLOGY AND GLOSSARY

A detailed description of methodology for the Javelin *2011 Identity Fraud Survey Report* can be found at www.IDsafey.net.

Glossary for Common Fraud Scams and Terms

Explanations of common fraud scams and definitions of related terminology are provided below.

Account takeover fraud	Method of identity fraud in which a fraud operator attempts to gain access to a consumer's account by fraudulently adding his/her information to the account; for example, changing an account mailing address, adding himself/herself as a registered user or making other alterations.
Advanced fee fraud	Any scam that, during its course, requires advanced fees to be paid by the victim; usually these fees are posed as processing fees, bribes, finder's fees, etc.
Cloning-payment card	On the magnetic stripe of a payment card are two tracks that have recorded the card details: track 1 and track 2. Criminals use the details on the tracks to create duplicate payment cards.
Cloning-mobile phone	Every mobile phone has a unique electronic serial number (ESN) and telephone number (MIN); a cloned mobile phone has been reprogrammed to transmit the ESN and MIN of a legitimate cell phone and the legitimate phone is billed for the clone's calls.
Cloning-payment card	On the magnetic stripe of a payment card are two tracks that have recorded the card details, Track 1 and Track 2. Criminals copy and use the track data details to create duplicate payment cards.
Consumer cost	Out-of-pocket costs incurred by the victim to resolve a fraud case, including lost wages, postage, copying, notarizing of documents, legal fees; may also include payment of any fraudulent debts to avoid further problems.
Credit freeze	Security freeze placed on a consumer's credit file to prevent the file from being shared with creditors, thus forestalling new accounts from being opened in the consumer's name.
Credit monitoring	Service that scrutinizes a consumer's credit file for suspicious activity or changes on his/her credit report such as credit inquiries, delinquencies, negative billing information, employment changes and address changes. Monitoring is particularly helpful in detecting new account fraud after it occurs. The most effective credit monitoring companies will monitor all three credit bureaus because many lenders will contact only one.
Cross-site scripting	An attack that exploits existing website vulnerabilities to download malware onto the computers of viewers who visit the infected site (e.g., Sinowal Trojan).
Data breach	Unauthorized disclosure of information that compromises the security, privacy or integrity of personally identifiable data.
Drive-by download	Act of compromising a PC passively by downloading a malicious file while the victim views the content of a website.
Existing accounts fraud	Identity fraud perpetrated against either or both existing card and existing non-card accounts.
Existing card accounts fraud	Identity fraud perpetrated through use of existing credit or debit cards and/or account numbers.

Existing non-card account fraud	Identity fraud perpetrated through use of existing checking and savings accounts or existing loan, insurance, telephone and utilities accounts.
Fraud amount	Total amount of funds the fraud operator obtained or tried to obtain illegally; these may result in actual losses to various businesses and organizations and, in some cases, to the consumer.
Friendly fraud	Fraud committed by someone who knows the fraud victim personally, such as a family member, coworker or friend. Friendly frauds are more damaging (harder to detect and longer to resolve) because the perpetrators tend to be aware of the victim's habits and know how to hide the fraud. Also, victims tend not to report friendly fraud to authorities.
Identity fraud	Unauthorized use of some portion of another's personal information to achieve illicit financial gain. Identity fraud can occur without identity theft; for example, by relatives who are given access to personal information or by the use of randomly generated payment card numbers.
Identity theft	Unauthorized access to personal information; identity theft can occur without identity fraud, such as through large-scale data breaches.
Interactive financial messaging	Two-way messaging between financial institutions (FIs) and their customers, including alerts for consumer-directed prohibitions.
Keylogger	Spyware that captures and records user keystrokes on a computer and is used by fraudsters to obtain passwords, PINs, logins and other sensitive information.
Mail order/telephone order (MOTO)	Orders placed through mail or telephone channels (a type of card-not-present transaction).
Malware	Malicious software designed to access a computer or operating system without the knowledge or consent of the user. Some examples of malware are computer viruses, worms, Trojan horses, spyware, malicious adware and rootkits. Malware is damaging code or programming that gathers information without permission.
Man-in-the-middle (MITM) attack	Attack in which a perpetrator is able to read, insert into and modify, at will, messages between two parties without either party's knowing that the link between them has been compromised.
Mutual authentication	Method by which the FI and the customer identify each other by providing and identifying shared secrets.
New account and other fraud	Identity fraud perpetrated through use of the victim's personal information to open fraudulent new accounts.
Non-identity fraud	Direct misrepresentation by a fraudulent merchant, investment firm, charity or other organization that results in financial loss to the consumer.
Packet sniffer	Programs that record all data ("network packets") traveling past a certain computer on a network.
Personal information monitoring	Service that keeps an eye on a consumer's personally identifiable information by monitoring channels, including online surveillance, public records and databases, Internet sites and "carding" forums (underground sites where stolen credit cards are bought and sold). Third-party solutions that offer this service provide additional value because they can more holistically prevent and detect identity fraud, including medical and health insurance fraud.
Phishing	Method of "fishing" for Internet users' passwords and financial or personal information by luring them to a fake website through an authentic-looking e-mail that impersonates the victim's institution.

Pretexting	Collection of information about an individual under false pretenses (the "pretext"), usually done over the phone, such as calling a bank while posing as a customer to find out personal information.
Privacy settings	User-defined controls that allow users to manage the visibility of various parts of their social media profiles, including who has access to specific information. Privacy settings are important in preventing persons unknown to the consumer from accessing personal information.
Severely impacted	Victims who report that they have suffered a significantly negative effect because they have been fraud victims. Consumers rate the impact a 4 or 5 on a scale where 1 represents "little or no effect" and 5 represents a "severe effect."
Skimming	The theft of payment card information in what is otherwise a legitimate transaction. (For example, skimming devices are sometimes placed at unattended gas stations to record the card information of purchasers.)
Smishing	Version of phishing sent by SMS (text message) that directs victims to a website that downloads malicious spyware (Trojan horse) onto their cell phone or computer.
Social Networking	A medium for consumers to interact with each other online, utilizing accessible and publishing techniques and forums. Users are responsible for generating content and can post and edit conversations, pictures and media. Some of the most popular social media sites are Facebook, MySpace, LinkedIn, Twitter, FourSquare, Yelp and YouTube.
SQL injection attack	Manipulation of poorly written code using a web form input box to gain access to a corporation's database, to locate key data or to compromise the server.
Synthetic identity fraud	Fictitious identity created to defraud an organization, typically generated from use of a real Social Security number and multiple names. These frauds are covered under this survey because a consumer victim is involved. To be considered "true synthetic identity fraud," *all* consumer information must be fictitious, which is very rare. In the unlikely event that all components of the identity are fictitious, this category would not be covered under this survey.
Trojan horse	Program that appears to be a useful file (e.g., a music file or software upgrade) from a legitimate source, tricking the victim into opening it; once activated, the Trojan horse allows intruders to access private information.
Vishing	Version of phishing that uses a telephone or combination of e-mail and telephone in which the victim is urged to resolve an account issue by a criminal posing as a financial institution and is prompted to provide personal information.
VoIP	Voice over Internet Protocol is the protocol for transmitting voice over the Internet. Criminals use VoIP to place autodial phone calls to commit fraud because the calls are inexpensive and difficult to trace.
Wardriving	Act of searching for unprotected or improperly protected wireless networks in a moving vehicle using a portable computer of some type.