

---

# 2009 Identity Fraud Survey Report: Consumer Version

## Prevent – Detect – Resolve

February 2009



© 2009 Javelin Strategy & Research

## Table of Contents

---

|   |    |
|---|----|
| Getting a Full Copy of the Identity Fraud Survey Report .....               | 3  |
| Overview .....  | 5  |
| Prevent, Detect, and Resolve .....  | 5  |
| What Does Javelin Mean by .....   | 6  |
| How Does Identity Theft Happen? .....                                       | 6  |
| How Do Identity Thieves Steal Information?.....                             | 7  |
| Consumer Security Alert: Credit and Debit Card Fraud.....                   | 8  |
| Javelin’s Top Six Identity Safety Tips: How YOU can Fight Fraud .....       | 9  |
| Additional Recommendations: A Comprehensive Approach to Fighting Fraud..... | 10 |
| Prevention .....  | 10 |
| How Can I Prevent Identity Fraud?.....                                      | 10 |
| Detection .....   | 11 |
| How Can I Detect Identity Fraud?.....                                       | 11 |
| Resolution .....  | 12 |
| What Should I Do if I Become a Victim of Identity Theft or Fraud? .....     | 12 |
| Consumer Fraud Protection Solutions: What’s Out There?.....                 | 13 |
| Where Can I Go to Get More Information? .....                               | 14 |
| 2008 Identity Fraud Report: Preview .....                                   | 14 |
| Common Fraud Scams and Terms.....   | 15 |
| Methodology.....  | 18 |

## Table of Figures

---

|  |    |
|--|----|
| <b>Figure 1:</b> Javelin’s Prevention, Detection and Resolution Model .....                            | 5  |
| <b>Figure 2:</b> Preventing Identity Fraud: Basic Precautions Can Go a Long Way.....                   | 7  |
| <b>Figure 3:</b> Detecting Identity Fraud: Earlier Detection Equals Faster and Easier Resolution ..... | 10 |
| <b>Figure 4:</b> Identity Fraud Protection Services.....   | 11 |
| <b>Figure 5:</b> How to Contact the Three Credit Bureaus.....  | 13 |
| <b>Figure 6:</b> Numbers of Victims before Weighting by Year.....                                      | 18 |
| <b>Figure 7:</b> Mean Dollar Value of Misappropriated Funds .....                                      | 20 |
| <b>Figure 8:</b> Three-Year Averaging of Fraud Amounts.....  | 21 |

***Where Can I Get the Industry Version of the 2009 Identity Fraud Survey Report?***

If you are a business or industry professional looking for more detailed statistics, incidence rates and fraud figures from our 2009 Identity Fraud Survey please reference the full report, entitled:

***2009 Identity Fraud Survey Report:  
Identity Fraud on the Rise But Consumer Costs Plummet As Protections Increase***

The full report consists of **96** pages with 56 graphs and tables and can be accessed for purchase on the research page of our Web site at [www.javelinstrategy.com/research](http://www.javelinstrategy.com/research), or by calling a sales representative at (925) 225-9100 ext.35. This Consumer Version was intended for the sole purpose of consumer education and awareness. Javelin recommends purchasing the full report for a complete overview of the key findings, analysis, new trends, and overall benchmarking of identity fraud in the U.S.

|                          |   |
|--------------------------|---|
| <b>Authors:</b>          | Rachel Kim, Analyst   |
| <b>Contributors:</b>     | Mary T. Monahan, Partner and Research Director<br>Tom Wills, Senior Analyst, Risk and Fraud<br>Alan Ruperto, Associate Analyst<br>James Van Dyke, President and Founder |
| <b>Research:</b>         | Stephen Knighten, Research Analyst  |
| <b>Publication date:</b> | February 2009   |

The Javelin *2009 Identity Fraud Survey Report: Consumer Version* provides guidelines for consumers to help prevent, detect and resolve identity fraud. Over the past five years, Javelin has surveyed nearly 25,000 adults to find out the actual ways consumers are being affected by identity fraud in the United States. The results of the study are used to help educate consumers to lower their risk of identity fraud. This year's phone survey of almost 4,800 adults is the largest, most up-to-date study of identity fraud in the U.S.

For commercial institutions desiring to view the complete version of this research study, the *2009 Identity Fraud Survey Report* (96 pages) is available for purchase.



This survey is co-sponsored by organizations committed to educating and helping consumers and businesses reduce their risk of identity fraud including Intersections, Inc., and Wells Fargo & Company, and is supported by the Better Business Bureau. Sponsors partially underwrite Javelin's cost of data collection, analysis and reporting in return for having their organization cited in the release of the study. Javelin retains complete independence of data analysis and reporting, and the report has been created solely by Javelin employees.

#### About Javelin

Javelin is the leading provider of independent, industry-specific, quantitative research and strategic direction for payments and financial services initiatives. Javelin conducts rigorous research and analysis to create successful strategies related to financial institutions, payments firms, technology vendors, merchants and billers, regulators and other policy-makers, associations, and consumer or business end-users.

## OVERVIEW

For the very first time since Javelin began this study five years ago, identity fraud rose this past year. Almost 10 million Americans learned they were victims of identity fraud in 2008, up from 8.1 million victims in 2007. More consumers are becoming victimized by this serious crime, reversing a previous trend in which identity fraud had been gradually decreasing. This makes sense because overall criminal activity tends to increase when there is a recession.

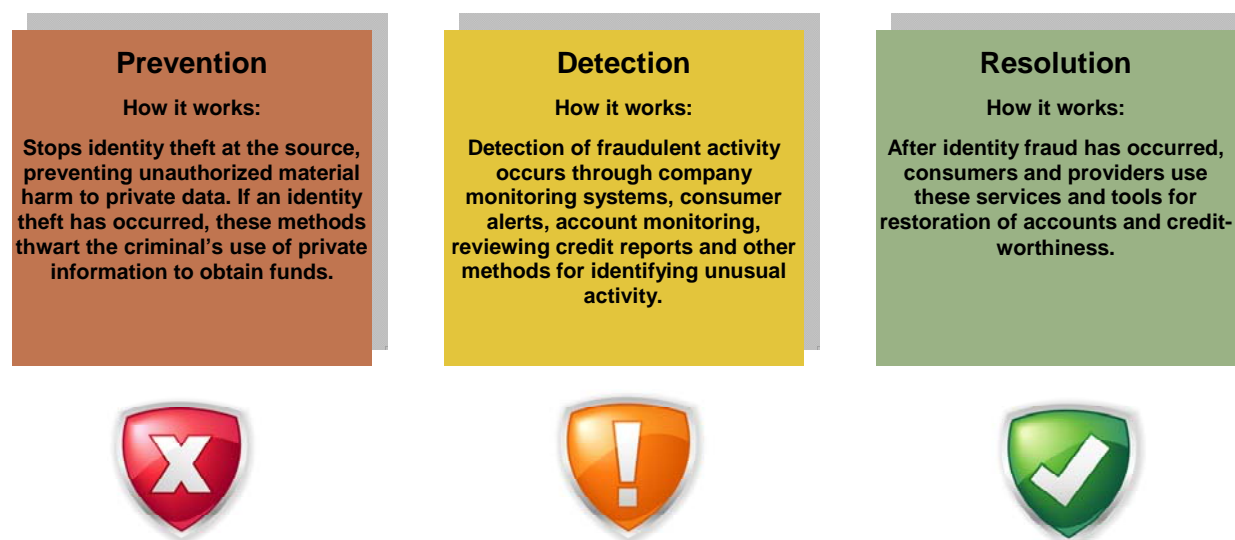
The good news is that the average consumer cost has dropped to almost \$500, which is much lower than in years past. Consumer cost is the out-of-pocket cost suffered by victims in order to resolve the fraud. Because of zero-liability fraud protection offered by many banks and credit card companies, most victims will pay nothing out-of-pocket.

Over the past five years, Javelin has collected data on nearly 25,000 adults to measure the overall impact of identity fraud on consumers. In 2008, almost 4,800 adults were asked about their day-to-day financial behaviors to help determine the potential causes of such fraud.

In this report, Javelin provides basic, easy-to-follow guidelines that consumers can use to protect themselves against this serious crime. The 2009 Identity Fraud Survey Report: Consumer Version equips consumers with proven methods that show how to prevent, detect and resolve identity fraud. Our recommendations to consumers are solidly based upon the results of thorough research and are backed by accurate and careful analysis of the most up-to-date data on identity fraud.

## PREVENT, DETECT AND RESOLVE

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



© 2009 Javelin Strategy & Research

## **WHAT DOES JAVELIN MEAN BY “IDENTITY FRAUD?” ISN’T IT SUPPOSED TO BE “IDENTITY THEFT?”**

While the term “identity theft” is an all-encompassing term that is widely referenced by most media, government and non-profit consumer groups on this topic, it is important to distinguish between the exposure of personal information versus the actual misuse of information for financial gain.

*Identity theft* happens when your personal information is accessed by someone else without your explicit permission. *Identity fraud* occurs when criminals take that illegally obtained personal information and misuse it for their financial gain, by making fraudulent purchases or withdrawals, creating false accounts, or attempting to obtain services such as employment or healthcare. Personally identifying information such as your Social Security number, bank or credit card account numbers, passwords, telephone calling card number, birth date, name, address and so on can be used by criminals to profit at your expense.

With even the most basic information, a criminal can either take over your existing financial accounts or use your personal identifying information to create new ones. Examples of fraud may include the unauthorized withdrawal of funds from your accounts, fraudulent purchases to your credit cards, or the creation of new accounts (telephone, utility, loans) in your name, all of which can have a damaging effect on your credit. In fact you may not even know that a fraud has been committed until you see an account that you did not open on your credit report, or until a debt collector contacts you for payment.

### **How Does Identity Theft Happen?**

Although many people believe that most identity theft only occurs over the Internet and that hackers are responsible for all identity theft and fraud, Javelin research has found that many thefts occur through more traditional methods, such as a stolen wallet or “friendly fraud,” in which the criminal may be someone close to you. In fact, among the victims who knew how their data was taken, lost or stolen wallets, checkbooks or credit cards accounted for nearly four times as many instances of theft as all online attack methods put together.

Your personal or financial information can be stolen in a number of different ways. The most common methods:

- Through a lost or stolen wallet, checkbook or credit card
- Through a transaction, such as a purchase you’ve made in-store, over the phone, or online
- Through information stolen in your own home, including by friends, relatives, and in-home employees
- Through spying by a criminal while you enter a PIN and use your payment card at the ATM or a store (this is known as “shoulder surfing”)
- By a data breach, whereby an organization or business that uses your personal information (this could be a hospital, school, or another business) has experienced widespread exposure of customer and/or employee records, including your own
- By someone who e-mails, calls, or text messages you, pretending to be a bank or other trusted source to trick you into providing private information
- By hacking, viruses, and malware/spyware on a computer
- Through mail theft from an unlocked mailbox
- By retrieving your unshredded information from a trash can, a method known as “dumpster diving”
- Through new and different methods that criminals are continually developing

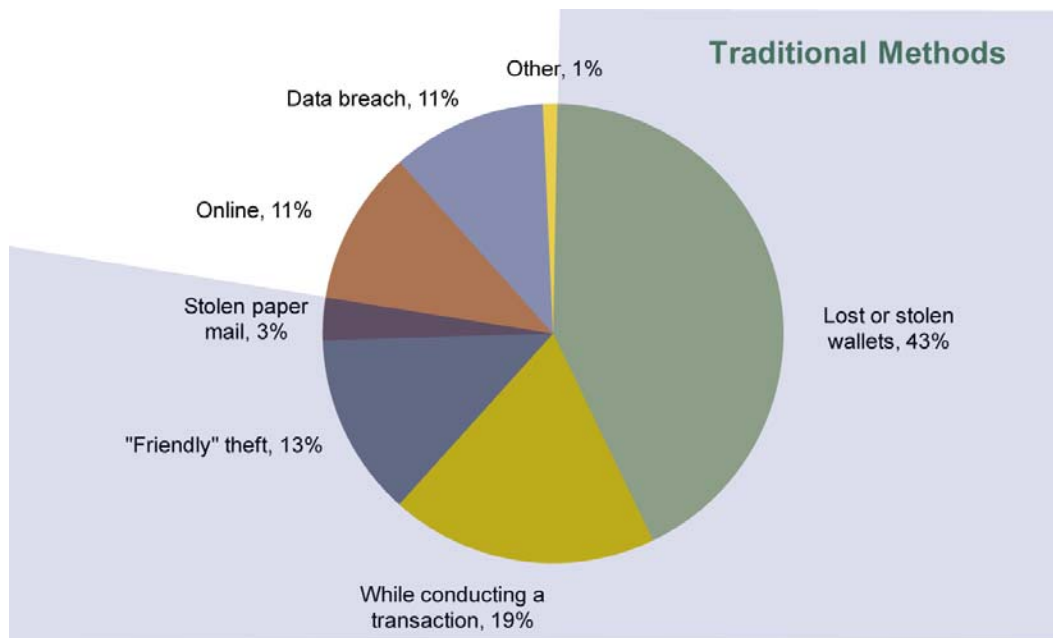
Because theft can be committed through so many methods, consumers are advised to put into practice a variety of the most effective measures to protect themselves. These measures are discussed in further detail in the “Top Five Tips” and “Additional Recommendations” sections.

## How Do Identity Thieves Steal Information?

The pie chart above shows the methods most commonly used by criminals to commit identity theft. Despite the hefty blame – largely perpetuated by the media – placed on the Internet and cyber-crime, online identity theft methods (phishing, hacking and malware) only accounted for 11% of fraud cases in 2008. The truth is, most known cases of fraud occur through traditional methods, when a criminal has direct, physical access to the victim’s information. These instances include stolen and lost wallets, checkbooks, or credit cards, or even through the simple act of a criminal surreptitiously eavesdropping into your conversation as you make a purchase. “Friendly theft,” reported by 13% of victims, occurs when friends, family or in-home employees take your private data and use it without your permission for their personal gain. While it is hard to believe that those who are close to us would engage in such an act, it is these individuals that have the closest access to sensitive documents that may contain your financial account numbers, Social Security numbers, and any other valuable personal identifying information needed to commit fraud. They also know your habits so it is easier for them to avoid detection for longer periods of time.

Preventing theft of your information doesn’t require spending money on security products or even a whole lot of effort. Practicing safe habits in your day-to-day activities can go far in reducing your risk of becoming a victim. Covering the keypad as you enter your PIN at the ATM, keeping sensitive documents in a locked drawer at home, or shredding old financial statements -- these are all considered basic precautionary measures that are easy and work to your benefit.

**Figure 2: What Are the Most Common Methods of Access?**



Q28: How was your information obtained? Keep in mind "other" is an option. Was it obtained...

October 2008, n = 157/4784  
(Based on the 35% of Victims Who Know How Their Information Was Obtained)  
Base: Victims Who Know How Their Information Was Accessed.  
© 2009 Javelin Strategy & Research

## **Consumer Security Alert: Credit and Debit Card Fraud**

This year Javelin is seeing increased attempts at card fraud, whereby identity thieves steal consumers' credit and debit card numbers and make fraudulent purchases or run up charges on stolen credit cards. This type of fraud is happening with existing credit cards and debit cards.

Card fraud is one of the easier frauds for criminals to perpetrate because, in certain cases, all it requires is an account number. With difficult economic times over the past year and overall crime rising in tandem, it is hardly surprising that there would be an increase in the theft and misuse of credit and debit cards.

### **Protect Your Debit and Credit Cards**

It is crucial for consumers to monitor credit card and checking accounts regularly online through their bank and credit card company's Web sites, by ATMs or by phone. Consumers who monitor their accounts more frequently are most likely to uncover suspicious or unauthorized activity earlier, rather than later. Those who use slower methods such as reviewing paper statements or being contacted by a debt collector are more likely to detect fraud much later after it has occurred.

If obtaining a credit or debit card, make sure the bank or credit card company provides you with zero liability if your card is ever lost, stolen or used without authorization. Nearly all financial institutions automatically protect you against any unauthorized transactions made at merchants, over the phone, on the Internet or at the ATM.

Banks can also notify you of certain types of account activity, through account alerts. You can sign up for alerts through online banking, or by contacting your bank or credit card company. Many financial institutions offer alerts for different types of activity, such as a purchase that is over a specified amount or when a transaction is international. You can generally receive alerts via e-mail, but some banks offer a mobile option, whereby alerts are sent to your mobile phone via text message.

For greater protection when shopping online, consider signing up for Verified by Visa or MasterCard SecureCode. Both provide a simple-to-use service that confirms your identity with an extra password when you make an online purchase. You can enroll at either the Visa or MasterCard Web sites, through your bank or credit card company, or when prompted during the checkout process at one of the participating online merchants.

If you lose your credit or debit card, or it is stolen, report it to your bank or credit card company *immediately*. That way, you can limit the chances of the card being misused or reduce potential losses.



## Javelin's Top Six Identity Safety Tips: How YOU can Fight Fraud

While it may be impossible to completely prevent identity fraud, consumers can still take basic measures to reduce their chances of being victimized. Those who are aware of the potential threats and take steps to protect themselves are significantly less likely to have their personal information stolen and misused.

Javelin has summarized the top six tips to highlight the easiest and most effective ways to combat fraud:

1. **Be Vigilant** – Monitor your accounts regularly online at bank and credit card websites, ATMs or by phone and set up alerts that can be sent both online and to a mobile device. Americans who monitor their accounts frequently are most likely to uncover suspicious or unauthorized activity. The survey found that those victims who took more than six months to detect the fraud saw four times higher average costs. Meanwhile, too many cases of fraud are detected via slower methods, such as when consumers review credit histories, paper statements or are contacted by a debt collector.
2. **Keep Personal Data Private** – Do not provide sensitive financial information over the Internet or phone, including Social Security numbers, passwords, personal identification numbers (PINs) or account numbers, unless you initiated the interaction to a verified and trusted location, such as the number or web address on the back of a credit card, debit card or statement.
3. **Online is Safer Than Offline When Consumers Use Available Security Controls** – Consumers should install and regularly update anti-virus and anti-spyware software, and keep operating systems and browsers updated. Once online access is secure consumers should move financial transactions online to eliminate many of the most common avenues fraudsters use to obtain personal information and gain more control compared to traditional channels. Moving online includes turning off paper invoices, statements and checks, including paychecks, and replacing them with electronic versions. Avoid mailing checks to pay bills or deposit funds in your banking account. Instead, pay bills online and use remote deposit check imaging services.
4. **Be Aware of Those Around You** - Be mindful of your environment and others who may be in proximity of overhearing sensitive financial or personal information or watching you text. This includes purchases over the phone or use of your Social Security Number for identification.
5. **Ensure Credit and Debit Cards are Protected** – Obtain credit and debit cards from financial institutions that provide zero liability if a card is ever lost, stolen or used without authorization. Nearly all financial institutions automatically protect you against any unauthorized transactions made at merchants, over the phone, on the Internet or at the ATM.
6. **Learn About Identity Protection Services** – There are additional services for those consumers who want extra protection and peace of mind. These include credit monitoring, fraud alerts, credit freezes and database scanning, some of which can be obtained for a fee and others at no cost. At a minimum, consumers should review their credit report no less than once per year, either for free at AnnualCreditReport.com or through many financial institutions' websites



## **ADDITIONAL RECOMMENDATIONS: A COMPREHENSIVE APPROACH TO FIGHTING FRAUD**

Aside from Javelin's top six tips, there are many other actions that consumers can take to protect themselves. When it comes to comprehensively battling identity fraud, Javelin recommends a three-part approach to addressing this problem: prevention, detection and resolution. This guide includes steps to take in order to prevent fraud from happening in the first place; actions to detect fraud earlier in the event that it happens; and what to do to resolve fraud if you become a victim.



### **Prevention**

#### **How Can I Prevent Identity Fraud?**

Consumers can best prevent identity fraud by preventing the exposure and theft of their most sensitive information, such as PINs, financial account numbers, and Social Security numbers. They can also prevent fraud from happening through awareness and education of common fraudster techniques, such as phishing and other scams.

**Figure 3: Preventing Identity Fraud: Basic Precautions Can Go a Long Way**



1. **Install and regularly update firewall, browser, anti-spyware and anti-virus security software on your personal computer**, and where available on your personal mobile device, and keep operating systems updated. Maintain your browser settings up-to-date.
2. **Do not reveal any sensitive personal information on your Facebook, MySpace, Twitter, or any other social networking site.** Social networking sites are quickly becoming a potential hazard for theft of information.
3. **Do not provide your card information to any Web site that is not a secure site.** To determine if it is a secure Web site, look at the URL for the "s" after the "http" in the address bar ("https") and look for the padlock symbol. Double click on the padlock symbol with your browser, and the SSL certificate will appear. If the firm offers an even better level of security, its name in the URL address box will turn bright green.
4. **Reduce unnecessary access to your financial cards and documents wherever possible.** For example, don't carry Social Security cards or unused credit cards or checks. Shred documents with any sensitive information prior to disposal, and do not leave your personal information lying about, especially statements with account numbers, your Social Security number, or any type of personal identification. To opt out of pre-approved credit offers, call 1-888-5-OPTOUT (1-888-567-8688) or visit [www.optoutprescreen.com](http://www.optoutprescreen.com) for more information.



## Detection

**Figure 4: Detecting Identity Fraud: Earlier Detection Equals Faster and Easier Resolution**



Usually, the longer a fraud goes on undetected, the greater the amount the criminal is able to steal. Therefore, it is essential for consumers to detect fraud as soon as possible to minimize potential losses. Faster detection results in lower losses, especially when it comes to any out-of-pocket expenses victims may incur as a result of being defrauded. (Out-of-pocket expenses are unreimbursed losses, legal fees and lost wages.) Earlier detection also makes the fraud easier to resolve in the long run.

### How Can I Detect Identity Fraud?

Javelin research has consistently shown that consumers are the best detectors of identity fraud. A proactive approach to fraud detection affords consumers the best protection against fraud. However, it is important to remember that the most effective crime fighting is achieved when consumers and their financial institutions partner together to stop fraud.

5. **Sign up for e-mail or mobile alerts through your primary bank or credit card company** to constantly monitor activity on your financial accounts and as well as any changes to your personal information which could indicate fraud. For example, address changes are the most common method fraudsters use to takeover an account; so setting up an address change alert is an excellent idea.
6. **Monitor your credit report on a regular basis** (free reports are available at AnnualCreditReport.com or by calling 1-877-322-8228). By staggering receipt of reports for each of the three bureaus, it is possible to review a report every four months. Review and confirm that all accounts listed are yours and that no unauthorized changes have been made. (Note: To help block access to your credit report, refer to Resolution section numbers 3 or 4 below.)
7. **Review your financial statements promptly.** Check your account balances weekly through online banking, by phone or ATM. Confirm that all transactions are authorized. (This is also one of the best ways to prevent identity fraud.)



## Resolution

### What Should I Do if I Become a Victim of Identity Theft or Fraud?

First of all, do not panic. Financial institutions are well-prepared to deal with instances of identity theft. In most cases, these institutions have already established internal processes to help you resolve your situation. There are a few simple steps to follow so that your fraud issues can be handled quickly and efficiently. You may even consider writing down the follow items to create a “To Do” checklist in the event that you yourself become a victim.

8. **Immediately contact your bank or credit card company** if your physical documents (checkbook, wallet, debit/credit cards) are lost or stolen or if you notice any unauthorized account activity (suspicious transactions) or changes to personal information (e.g., physical address change, e-mail address change, paper statement turn-off, etc.). Depending on the situation, the bank or company will close your account, issue you a new card, etc.



9. **Contact the Federal Trade Commission (FTC) to report any incidents of suspected fraud or identity theft.** This can be done through their online complaint form, at [www.ftc.gov/bcp/edu/microsites/idtheft](http://www.ftc.gov/bcp/edu/microsites/idtheft), or by telephone at 1-877-IDTHEFT (1-877-438-4338). Alternatively, you can write to the Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
10. **If your personal information has been compromised or you’ve become a victim of fraud, place a fraud alert on your credit report by contacting (online or by phone) the three principal credit reporting agencies.** (Refer to Figure 6 on page 18, for contact information for Equifax, Experian and TransUnion). All three of these firms provide products such as credit monitoring services. *Fraud alerts* notify potential creditors that a potential fraud has occurred and that they should verify the identity of the applicant before extending any credit. An initial alert stays on for 90 days, or an extended alert for identity fraud victims lasts seven years.
11. **If you have been a victim of new accounts fraud more than once and are not actively applying for credit, considering placing a security freeze on your credit report at each of the three reporting agencies.** A *security freeze* blocks access to your credit report. This service helps to stop new account fraud from occurring, but does not stop existing account fraud. You should also obtain a copy of your free credit reports to see if fraud has already occurred.
12. **File a police report if fraud has occurred.** Be sure to obtain a copy of the police report for your personal records.

## Consumer Fraud Protection Solutions: What's Out There?

In addition to the guidelines listed above and on the previous pages, there are additional services for those consumers who want extra protection and peace of mind. These include credit monitoring, fraud alerts, credit freezes and data scanning, some of which can be obtained for a fee and others at no cost.

- **Credit monitoring** services are generally a paid service that regularly monitors for suspicious activity or changes to your credit file.

E-mail alerts are sent when abnormal activity is found, and you have unlimited access to your credit report from all three credit bureaus. Credit monitoring is designed to *detect* potential fraud earlier, and may require some follow-up action on your part. You can purchase credit monitoring through your bank or credit card company, or through any of the three major credit bureaus.

- You can set up a **fraud alert** at no cost by contacting the fraud departments of all three major credit bureaus and asking them to mark your credit file. Each bureau is required by law to notify the other two agencies; however, to ensure safety, consumer privacy advocates consulted by Javelin currently recommend placing alerts at all three bureaus. Fraud alerts are meant to prevent someone from opening a fraudulent new account (such as a new credit card or loan) in your name.

The fraud alert will remain in place for only 90 days, after which you'll need to renew the alert. Fraud victims qualify (with proof) for the seven-year victim statement, which will keep the alert in place for seven years. Non-victims who don't want to bother with reactivating the alert can also pay for a fraud alert service that takes care of the renewal process (these typically cost about \$10 per month).

**Figure 5: Identity Fraud Protection Services**

| Service                               | What is it?  |
|---------------------------------------|--|
| <b>Credit Monitoring</b>              | <ul style="list-style-type: none"> <li>• A paid subscription service that monitors for suspicious activity or changes to your credit file (e.g., credit inquiries, employment changes, new accounts and address changes)</li> <li>• <b>Detects potential fraud</b></li> </ul>  |
| <b>Fraud Alert</b>                    | <ul style="list-style-type: none"> <li>• A message that is placed on your credit report, requiring lenders and creditors to confirm your identity before issuing a new line of credit</li> <li>• <b>Intended to prevent fraud</b></li> </ul>   |
| <b>Credit Freeze</b>                  | <ul style="list-style-type: none"> <li>• Locks down your credit file at the credit reporting agencies, which are prohibited from issuing your credit history to any lender, creditor, etc.</li> <li>• <b>Prevents fraudulent new accounts</b> from being opened in your name</li> </ul>  |
| <b>Public Records/Database Mining</b> | <ul style="list-style-type: none"> <li>• Scans public records and Internet sites to detect if your personal information is out there (credit card numbers, Social Security numbers, etc.)</li> <li>• <b>Detects potential identity theft</b> (your information has been found, and may or may not have been misused for financial gain)</li> </ul> |

© 2009 Javelin Strategy & Research

- A **credit freeze** locks down your credit file, and basically prevents any lender or creditor from accessing your credit history. This service is designed to block new credit from being issued in your name. If you are a victim of identity fraud, you may qualify for free coverage (depending in which state you live). Otherwise, it may cost you up to \$30 to place a freeze and \$30 to remove it through the credit bureaus. Remember, if you place a credit freeze you cannot apply for new credit unless you remove or temporarily lift the freeze, which could take up to a few days. Credit freezes are recommended for people who are not actively applying for credit.
- **Public data scanning** is a service that scans public sources of information, including Internet sites and public records, to detect whether your personal or financial information has been compromised.

Data scanning is available for a monthly fee (usually around \$12 per month) from independent companies that specialize in this offering. If your information is found, you will be alerted of potential identity theft. It is important to recognize that these alerts do not necessarily mean that you have been defrauded. From then on, you can place a fraud alert to help prevent fraud or continue monitoring your information.

## ***WHERE CAN I GO TO GET 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](http://www.IDSafety.net)

The 2009 Identity Fraud Report's co-sponsors (Intersections, Wells Fargo and Better Business Bureau) also offer safety recommendations:

- **Intersections Inc.**  
<http://www.identityguard.com/aboutidentitytheft/landing.aspx>
- **Wells Fargo**  
[www.wellsfargo.com/privacy\\_security/fraud\\_prevention/](http://www.wellsfargo.com/privacy_security/fraud_prevention/)
- **Better Business Bureau**  
[www.us.bbb.org](http://www.us.bbb.org)

## ***THE 2009 IDENTITY FRAUD REPORT: PREVIEW***

The complete Javelin *2009 Identity Fraud Survey Report: Identity Fraud on the Rise but Consumer Costs Plummet as Protections Increase* (over **96** pages long with 56 graphs and tables) is available for purchase at our Web site at [www.javelinstrategy.com/research/](http://www.javelinstrategy.com/research/). The full report provides a detailed, comprehensive analysis of identity fraud in the United States, in order to help consumers and businesses better understand the effectiveness of methods used for its prevention, detection and resolution. This report is issued as the fourth annual longitudinal update to the original Javelin *Identity Fraud Survey Report*.

## COMMON FRAUD SCAMS AND TERMS

To clarify common fraud scams and terminology, definitions are provided below.

Javelin uses identity fraud as the term to describe the crime discussed in this report. Because this report's underlying survey was based on interviews with individuals who were the victims of fraud committed with at least some portion of their personal information, it does not include other categories of crime such as synthetic identity fraud, which is based upon a wholly fictitious identity. However, Javelin believes that most types of identity fraud do contain a mixture of true and synthetic components. These are included in this report.

To clarify the usage of common terms by Javelin, definitions are provided below.

|   |  |
|---|--|
| <b>Account Takeover Fraud</b>           | method of identity fraud in which a fraud operator attempts to gain access to a consumer account by fraudulently adding his/her information to the account; for example, changing account mailing address or making other alterations  |
| <b>Advanced Fee Fraud</b>               | 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.  |
| <b>Cloning</b>                          | every cell phone has a unique electronic serial number (ESN) and telephone number (MIN); a cloned cell 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   |
| <b>Card-Not-Present (CNP)</b>           | transaction where the card is not present at the time of transaction; card data is manually inputted   |
| <b>Consumer Cost</b>                    | out-of-pocket costs incurred by the victim in order to resolve a fraud case including postage, copying, notarizing documents, legal fees; may also include payment of any fraudulent debts in order to avoid further problems  |
| <b>Credit Freeze</b>                    | 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   |
| <b>Cross-Site Scripting</b>             | an attack that exploits existing Web site vulnerabilities to download malware onto the computers of viewers who visit the infected Web site, e.g., Sinowal Trojan  |
| <b>Data Breach</b>                      | unauthorized disclosure of information that compromises the security, privacy or integrity of personally identifiable data   |
| <b>Existing Accounts Fraud</b>          | identity fraud perpetrated against either or both existing card and existing non-card accounts   |
| <b>Existing Card Accounts Fraud</b>     | identity fraud perpetrated using existing credit or debit cards and/or their account numbers   |
| <b>Existing Non-Card Accounts Fraud</b> | identity fraud perpetrated using existing checking and savings accounts, and existing loans, insurance, telephone and utilities accounts   |
| <b>Fraud Amount</b>                     | total amount of funds that 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; the funds may be recovered or the loss avoided due to preventive measures adopted by the businesses |
| <b>Identity Fraud</b>                   | 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                 |

|  |  |
|--|--|
| <b>Identity Theft</b>                    | unauthorized access to personal information; identity theft can occur without identity fraud, for example, through large-scale data breaches   |
| <b>Interactive Financial Messaging</b>   | two-way messaging between FIs and their customers, including alerts for consumer-directed prohibitions   |
| <b>Keylogger</b>                         | spyware that captures and records user keystrokes on a computer, used by fraudsters to obtain passwords, PINs, logins, and other sensitive information   |
| <b>Mail Order/Telephone Order (MOTO)</b> | orders placed through mail or telephone channels (a type of card-not-present transaction)  |
| <b>Man-in-the-Middle (MITM)</b>          | attack in which a perpetrator is able to read, insert and modify, at will, messages between two parties without either party knowing that the link between them has been compromised   |
| <b>Mutual Authentication</b>             | method by which both the FI and the customer identify each other, for example, by providing and identifying shared secrets   |
| <b>New Accounts and Other Fraud</b>      | identity fraud perpetrated by using the victim's personal information to open fraudulent new accounts  |
| <b>Non-Identity Fraud</b>                | direct misrepresentation by a fraudulent merchant, investment firm, charity or other organization that results in financial loss to the consumer   |
| <b>Packet Sniffer</b>                    | programs that record all data ("network packets") traveling past a certain computer on a network   |
| <b>Phishing</b>                          | method of "fishing" for Internet users' passwords, financial or personal information by luring them to a fake Web site through an authentic-looking e-mail that impersonates the victim's financial institution  |
| <b>Pretexting</b>                        | 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   |
| <b>Smishing</b>                          | version of phishing sent by SMS (text message) that sends a text message directing victims to a Web site that downloads malicious spyware (Trojan horse) onto the victim's cell phone or computer  |
| <b>SQL Injection Attack</b>              | manipulation of poorly written code using a Web form input box to gain access to a corporation's database, to locate key data, to compromise the server, etc.  |
| <b>Synthetic Identity Fraud</b>          | fictitious identity created in order to defraud an organization; typically generated using a real Social Security number and multiple different names. These frauds are covered under this survey because a consumer victim is involved. To be considered "true synthetic identity fraud," <i>all</i> consumer information must be fictitious, which is very rare. In the unlikely event that all components of the identity are fictitious this would not be covered under this survey. |
| <b>Trojan Horse</b>                      | 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   |
| <b>True Name Fraud</b>                   | see identity fraud   |
| <b>Vishing</b>                           | version of phishing that uses a combination of e-mail and telephone, or just telephone; the victim is urged to resolve an account issue by a criminal posing as a financial institution, and is thereby prompted to provide personal information   |

**VoIP**

Voice over Internet Protocol: 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

## METHODOLOGY

The following section explains the methodology (how the data was collected, composed and analyzed) behind this study. This section is more suitable for those individuals who may already be familiar with market research methods.

The Javelin *Identity Fraud Survey Report* provides consumers and businesses an in-depth and comprehensive examination of identity fraud in the United States. Its purpose is to help readers understand the causes and incidence rates of identity fraud and the success rates of methods used for its prevention, detection and resolution.

This report builds on the Javelin's annually published *Identity Fraud Survey Report* and the Federal Trade Commission's *2003 Identity Theft Survey Report*.

### Survey Questionnaire

The set of questions and underlying methodology used for this report were identical to or highly similar to the 2007, 2006, 2005, 2004 and 2003 surveys. This allows the ability to provide longitudinal trends on various subjects, such as incidence rates and detection methods.

In addition, to more deeply explore the significance of past responses, a discrete number of new questions were added. These expanded on the behaviors of consumers after personal information was compromised and/or misused in order to identify the lasting impact of identity fraud on victims.

Some questions from the previous surveys were modified to improve the accuracy of estimates. Questions used to measure the fraud amounts, consumer cost and resolution hours previously provided ranges of responses. In the 2008, 2007 and 2006 reports, these questions were changed to collect exact amounts.

### Survey Respondents

In all, 4,784 consumers, representative of the U.S. population, were interviewed via a standardized 50-question telephone survey to develop accurate and actionable insight into this pervasive and costly crime.

The polling yielded interviews with 482 fraud victims. After weighting the responses to standardize them to national demographics,<sup>1</sup> the 2008 survey's computed number of victims interviewed was 487. For comparison, the numbers of victims in previous years are provided below, before and after weighting:

**Figure 6: Numbers of Victims before Weighting by Year**

|   | 2008       | 2007 | 2006 | 2005 | 2004 | 2003 |
|---|------------|------|------|------|------|------|
| <b>Number of victims before weighting</b> | <b>482</b> | 442  | 469  | 529  | 507  | 433  |
| <b>Number of victims after weighting</b>  | <b>487</b> | 445  | 458  | 505  | 509  | 514  |

© 2009 Javelin Strategy & Research

<sup>1</sup> Responses were adjusted to be nationally representative based on respondents' age, gender, income level, and race/ethnicity as reported by US Census on 12/11/2006 [http://www.census.gov/prod/www/statistical-abstract-2001\\_2005.html](http://www.census.gov/prod/www/statistical-abstract-2001_2005.html) accessed 12/11/2007.

## Survey Data Collection

Javelin employed the Discovery Research Group for this survey's data collection. Discovery, one of the nation's largest data collection providers, is recognized as a reputable data collection service firm with over 20 years of experience in the industry. Previous studies employed Synovate for all phases of data collection using Computer Assisted Telephone Interviewing (CATI) via Random-Digit-Dialing (RDD). Synovate has since changed its sampling method from RDD to a remunerated opt-in panel. In order to maintain consistency in methodology by continuing to sample respondents through RDD, Javelin engaged the services of the Discovery Research Group for the 2008 study.

The study was conducted using interviews administered by telephone with 4,784 U.S. adults over age 18 and a sample that is representative of the U.S. census demographics distribution. Data collection began September 19, 2008 and ended November 7, 2008.

## Margin of Error

For questions answered by all 4,784 respondents, the maximum margin of sampling error is +/- 1.4% at the 95% confidence level.

For questions answered by all 487 identity fraud victims, the maximum margin of sampling error is +/- 4.4% at the 95% confidence level.

For questions answered by a proportion of all identity fraud victims, the maximum margin of sampling error varies and is greater than +/- 4.4% at the 95% confidence level.

## Categorizing Fraud

With one exception, this report continues to classify fraud within the three categories originally defined by the FTC. For 2005 and beyond, debit card fraud has been re-categorized as existing card accounts fraud<sup>2</sup> instead of existing non-card accounts fraud.<sup>3</sup> Javelin believes that this change reflects a more accurate representation of debit card fraud since much of its means of compromise, fraudulent use and detection methods parallel those of credit cards.

The categories of fraud are listed below from least to most serious:

- Existing card accounts: This category includes both the account numbers and/or the actual cards for existing credit and card-linked debit accounts. Prepaid cards were added for 2007 and subsequently removed due to extremely low incidence.
- Existing non-card accounts: This category includes existing checking and savings accounts, and existing loans, insurance, telephone and utilities accounts.
- New accounts and other frauds: This category includes new accounts or loans for committing theft, fraud or other crimes using the victim's personal information.

Many victims experience identity fraud within more than one of these categories. In reporting the *overall incidence rates* of the three categories or types of accounts, the victims of crimes to more than one type of account are categorized based on the most serious (as designated by the FTC) problem reported. Thus, victims who reported that new accounts had been opened using their

<sup>2</sup> Formerly titled "Existing Credit Card Accounts" in the 2003 and 2005 reports

<sup>3</sup> Formerly titled "Existing Non-Credit Card Accounts" in the 2003 and 2005 reports

information and also that their existing credit cards had been misused would be placed in the new accounts and other frauds classification, not in the existing card accounts classification. This categorization is applicable only for reporting the rates of the three types of fraud.

### Reporting Years of Findings

This report labels longitudinal findings according to the year the data was collected, in contrast to previous years when longitudinal findings were labeled according to the year the report was published. Most notably, the current year of the data in this report is labeled as 2008 as the data collection was finished in November 2008.

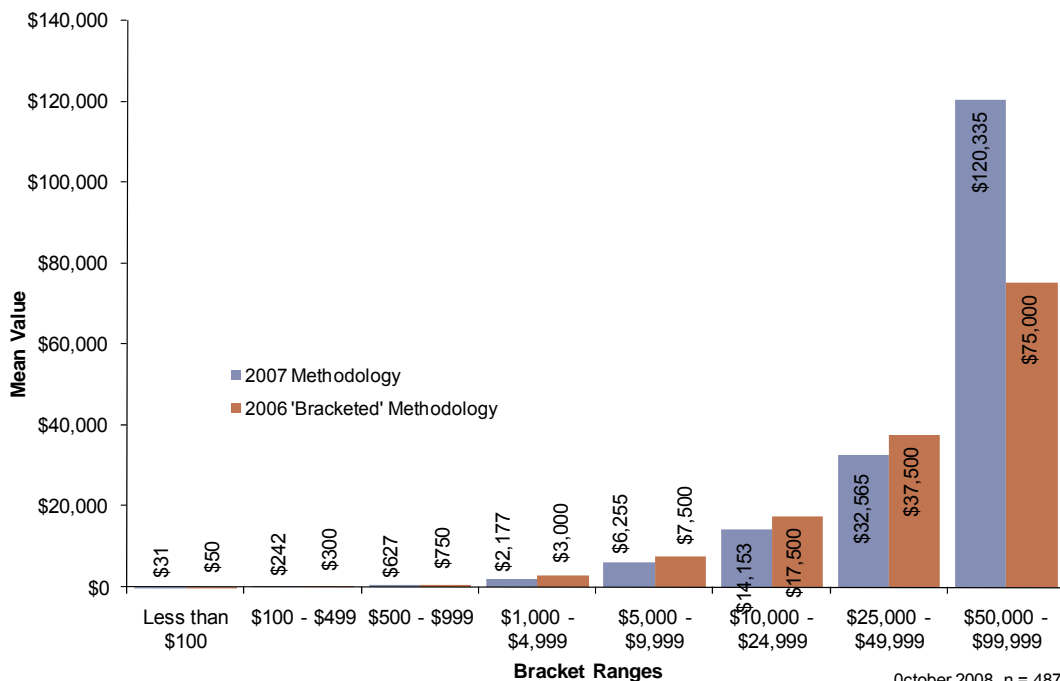
### Calculations

#### Comparing Annual Numbers

To create a more accurate understanding of the costs of identity fraud, Javelin has departed from using ranged brackets (e.g., \$0 to \$50) to measure the fraud amount, consumer cost and hours spent resolving fraud. This change in methodology leads to a lower estimate of the average fraud amount.

By converting the data collected into the 2005 “bracketed” year’s methodology, Javelin has found that the means derived from the former bracketed methodology overstate the average losses by over 20% (with the exception of the final category, where the bracketed fraud amount decreased the average fraud amount of the victims by 60%). By adopting this change, Javelin has created a more accurate picture of the impact of identity fraud in the U.S.

**Figure 7: Mean Dollar Value of Misappropriated Funds  
Comparing 2008 and 2006 Methodologies**



Q32. What is the approximate total dollar value of what the person obtained while misusing your information?

October 2008, n = 487  
Base: All fraud victims  
© 2009 Javelin Strategy & Research

To allow for comparisons to previous years, it is necessary to re-bracket the actual amounts and this is what has been done. In the future, access to these actual (versus bracketed) numbers will allow for comparisons of like figures using the more accurate actual numbers.

Due to rounding errors, the percentages on graphs add up to 100% plus or minus one percent.

To assure consistency in comparing year-to-year changes, historical figures for average fraud amounts were adjusted for inflation by using the Consumer Price Index (CPI). 2007 survey numbers were adjusted by 3.9%, 2006 survey numbers were adjusted by 7.5%, 2005 survey numbers were adjusted by 9.8%, 2004 survey numbers were adjusted by 13.3% and 2003 numbers were adjusted by 17.1% to normalize the value of currency to 2008 dollars.<sup>4</sup>

### **Data Smoothing Techniques**

2005, 2006, 2007 and 2008 total dollar cost estimates have been smoothed by taking a moving three-year average of the victim's fraud amount. Time series data smoothing techniques are

**Figure 8: Three-Year Averaging of Fraud Amounts**

|                                  | 2008        | 2007 | 2006 | 2005 | 2004 | 2003 |
|----------------------------------|-------------|------|------|------|------|------|
| <b>Original Amount</b>           | <b>\$50</b> | \$42 | \$36 | \$62 | \$60 | \$58 |
| <b>Three-year moving average</b> | <b>\$48</b> | \$45 | \$50 | \$57 | N/A  | N/A  |

© 2009 Javelin Strategy & Research

### **Calculating Mean and Median Values**

Where responses pertained to a range in value, e.g., "one day to less than one week," the midpoint of the range, rounded up to the nearest whole unit, was used to calculate the median or mean value.

- Example: If the response selected for fraud amount was one day to less than one week, the assigned value would be the median of one day and seven days, inclusive, or 4.5 days.

### **Deviation From FTC and 2003 Methodology and Reporting**

When reporting victims' average financial damages or resolution times in *dollars or hours*, the entire amount of damages or losses are placed into every type of fraud that the victims suffered. For example, for a victim who reports that a total of \$100 is obtained for both new accounts and other frauds category and existing card accounts, the \$100 is counted in both categories. This method of reporting costs by types of fraud will not change the *overall* total costs of fraud across all three categories, but the average amount of dollars or time associated within the three types of fraud should not be summed because there will be overlapping amounts.

In the 2003 report, responses to the new accounts and other frauds question (Q13) were modified based on respondents' subsequent answers to question 18. 2008's question 18 is slightly modified from 2003's, thus avoiding the possibility of needing to adjust responses to question 13 in order to maintain the longitudinal integrity. 2008's responses to question 13 are reported as they were reported by the victims.

<sup>2</sup> Dollars costs were adjusted using the Consumer Price Index (CPI-U, Base 1982-84=100) issued by the Bureau of Labor Statistics, <ftp://ftp.bls.gov/pub/special.requests/cpi/cpi.txt> accessed 11/10/2008.

Secondly, 2008's detection time question (Q24) is categorized differently from the 2003 study. While the 2003 study provided 13 answers from which victims could choose, the 2006 study contained only 9 such responses. Javelin merged similar response categories that contained few replies in 2003 into single categories, allowing the data to be cross tabbed with larger numbers and fewer categories for a more robust calculation.

On several other questions, longitudinal comparisons are performed with numbers that Javelin calculated using 2003 raw data instead of 2003 reported figures. This was done in order to avoid inserting rounding errors or methodology differences.

### ***Contributing Organizations***

The survey was in part made possible by Intersections, Inc., and Wells Fargo & Company. To preserve the project's independence and objectivity, the sponsors of this project were not involved in the tabulation, analysis or reporting of final results.