



Media Contact:
 Matt Pennacchio
Javelin@ruderfinn.com
 212-715-1613
 Twitter: @IDFraudReport

All Additional Inquiries:
 Elizabeth Travers
etravers@javelinstrategy.com
 925-225-9100 ext. 31

Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back

Identity Fraud Affected 11 Million Americans in 2009; Proactive Measures by Financial Institutions, Businesses and Consumers Helped Decrease Costs; Increase in Prosecutions and Convictions

SAN FRANCISCO, February 10, 2010 – The 2010 Identity Fraud Survey Report – released today by [Javelin Strategy & Research](http://www.javelinstrategy.com) – found that the number of identity fraud victims in the United States increased 12 percent to 11.1 million adults in 2009, while the total annual fraud amount increased by 12.5 percent to \$54 billion¹. The report found that protection of data by consumers and businesses and enlisting assistance in resolution are helping consumers and businesses resolve fraud more quickly, and are also reducing or eliminating costs for the consumer. Average fraud resolution time dropped 30 percent to 21 hours, and nearly half of new victims file police reports, resulting in double the reported arrests, triple the prosecutions, and double the percentage of convictions in 2009.

More Consumers Experience Fraud, but Mean Consumer Costs and Resolution Hours Drop

Overall Measures of Impact

	Survey Report							
	Trend	2009	2008	2007	2006	2005	2004	2003
US adult victims of identity fraud **	▲	11.1 M	9.9 M	8.1 M	8.4 M	8.9 M	9.3 M	10.1 M
Fraud victims as % of US population	▲	4.8%	4.3%	3.6%	3.7%	4.0%	4.3%	4.7%
Total one year fraud amount *	▲	\$54 B	\$48 B	\$45 B	\$50 B	\$57 B	\$60 B	\$58 B
Mean fraud amount per fraud victim ***	▬	\$4,841	\$4,858	\$5,509	\$5,955	\$6,436	\$6,507	\$5,736
Median fraud amount per fraud victim	▬	\$750	\$750	\$750	\$750	\$750	\$750	\$750
Mean consumer cost	▲	\$373	\$498	\$720	\$574	\$467	\$746	\$606
Median consumer cost	▬	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Mean resolution time (hours)	▲	21	30	26	25	40	28	33
Median resolution time (hours)	▬	5	5	5	5	5	5	5

© 2010 Javelin Strategy & Research
*Past years dollars figures have been adjusted for inflation using the Consumer Price Index (CPI-U) issued by the Bureau of Labor Statistics. <http://ftp.bls.gov/pub/special.requests/cpi/cpiat.txt> accessed 12/14/2009.
 **Based on US population estimates (age 18 and over). <http://www.census.gov/popest/estimates.php> accessed January 01/11/10
 ***2006, 2007, 2008, and 2009 dollar cost estimates have been smoothed using three-year averaging—refer to Methodology Section for details.

¹ Past years dollars figures have been adjusted for inflation using the Consumer Price Index (CPI-U) issued by the Bureau of Labor Statistics <http://www.bls.gov/cpi/cpid0912.pdf>

Now in its seventh consecutive year, the comprehensive identity fraud survey report is independently produced by Javelin Strategy & Research and co-sponsored by leading companies in financial services and identity fraud prevention technology and resolution. Co-sponsors in 2009 include Fiserv, Inc., Intersections Inc., Wells Fargo & Company and ITAC, the Identity Theft Assistance Center. The survey is the nation's longest-running study of identity fraud, with more than 29,000 U.S. respondents over the past seven years. Identity fraud is defined as the unauthorized use of another person's personal information to achieve illicit financial gain. In November 2009, Javelin conducted telephone interviews with 5,000 U.S. adults to identify and track the methods fraudsters used, the impact of fraud on Americans and how these findings can help consumers most effectively avoid becoming victims of fraud.

"The 2010 Identity Fraud Survey Report shows that fraud increased for the second straight year and is at the highest rate since Javelin began this report in 2003²," said James Van Dyke, president and founder, Javelin Strategy & Research. "The good news is consumers are getting more aggressive in monitoring, detecting and preventing fraud with the help of technology and partnerships with financial institutions, government agencies and resolution services. Through IDSafety.net and our free consumer report, Javelin and our co-sponsor partners are working to educate consumers and provide guidelines and tips to help them safeguard their personal information."

Other findings in this year's report reinforce the trend that fraudsters are becoming increasingly savvy with technology and are using personal information stolen in data breaches to open new accounts or to make changes to existing non-card accounts. Financial institutions and businesses are countering this by minimizing the use of Social Security numbers in account information and more proactively monitoring and notifying customers of possible fraudulent activity. While consumers are monitoring their accounts more frequently using technologies such as online banking and mobile alerts, consumer education on protection and prevention measures such as keeping anti-virus software up to date will continue to be important.

Key Survey Findings:

- **Fraud is Up, but Consumer Costs and Resolution Hours Drop** – The number of identity fraud victims increased by 12 percent over 2008, reaching the highest level since the survey started in 2003. Javelin believes this may be due to the economic downturn, when historically, higher rates of fraud occur. However, during 2009 there was a drop in fraud costs per victim and a decrease in time to resolution, thanks to increased consumer awareness, assistance provided by financial institutions consumer support organizations, and law enforcement.
- **Increase in New Account Fraud** – Identity fraud that resulted from fraudsters opening new accounts with stolen information increased in 2009. The number of fraudulent new credit card accounts increased to 39 percent of all identity fraud victims, up from 33 percent in 2008. New online accounts opened fraudulently more than doubled over the previous year, and the number of new e-mail payment accounts increased 12 percent. This year for the first time, the survey asked about new mobile phone account fraud and

² Based on U.S. population estimates (age 18 and over), <http://www.census.gov/popest/estimates.php>

29 percent of new accounts fraud victims reported new mobile phone accounts were fraudulently opened.

- **Data Breaches Across Various Industries Continue to Compromise Personal Information** – Identification most likely to be compromised in a data breach continues to be Full Name (63 percent) and Physical Address (37 percent). With a year-over-year increase of 4 percent, Health Insurance Information is increasingly targeted. The percentage of Social Security numbers compromised decreased to 32 percent from 38 percent in 2008.
- **Fraudsters Target Existing Credit Cards** – 75 percent of existing card fraud incidents came from credit cards, an increase of 12 percent over 2008. In contrast, existing debit card fraud incidents decreased two percent and represented 33 percent of total existing card fraud in 2009.
- **Proactive Consumers are Catching Thieves** – Half of all victims filed a police report, resulting in more arrests and convictions. Victims became more vigilant in reporting identity fraud, and reported this resulted in an arrest rate twice last year's rate, and a prosecution rate that tripled compared to 2008. These findings indicate greater success using information provided by consumers, banks and credit card providers to detect, catch and convict criminals.
- **18 to 24 Year Olds are Slowest to Detect Fraud** – Millennials (consumers aged 18 to 24 years old) take nearly twice as many days to detect fraud, compared to other age groups, and thus are fraud victims for longer periods of time. Millennials were found to be the less likely to monitor accounts regularly and the least likely group to take advantage of monitoring programs offered by financial institutions. However, Millennials were the most likely group to take action such as switching primary banks or switching forms of payment.
- **Small Business Should Exercise Caution** – Small business owners suffered identity fraud at one-and-a-half times the rate of other adults. This appears to be due to the fact that small office / home office business owners use personal accounts when making business transactions and make more transactions than typical adults.

Criminals are conducting more identity fraud, but consumer costs and resolution times are down and online and mobile tools are helping

Identity fraud increased in 2009 and the number of fraud victims in the U.S. grew to 4.8³ percent of the population, adding up to a projected total of \$54 billion in crime.

Financial institutions, businesses and government agencies are helping prevent fraud, protect consumer identities and respond to fraud incidents. As a result, consumers are benefitting. Banks are continually providing more behind-the-scenes customer and analytic tools for safer electronic and traditional banking. They are investing in identity fraud monitoring, intelligent fraud engines to detect account access and payment anomalies, and resolution and education services, typically offering these services free to customers. Banks are also increasingly offering mobile banking solutions, which allow monitoring and alerts in near-real-time that proactively notify customers when account activity and possible fraud occurs. These partnerships and increased activism on

³ Based on U.S. population estimates (age 18 and over), <http://www.census.gov/popest/estimates.php>

the behalf of consumers resulted in consumer out of pocket costs being at an all-time low of \$373 in 2009. Consumer out of pocket costs refer to unreimbursed loses, legal fees and actual lost wages. The typical out of pocket cost for a consumer fraud victim is zero, due to guarantees provided by financial institutions.

Technology is empowering consumers against fraudsters, but consumers need to take precautions

Electronic account monitoring and services provided by financial institutions through partnerships are allowing consumers to become increasingly vigilant when it comes to detecting and resolving identity fraud. Consumers are adopting best practices in safeguarding their personal and private information by reviewing electronic statements and fraud alerts sent to e-mail accounts and mobile devices, and not responding to e-mail requests for personal information such as “phishing.” Monitoring for fraudulent activities with a mobile device allows consumers to review and report identity fraud in near-real-time, which can result in lower victim costs and faster detection times.

Millennials lead all age groups in using technology to resolve identity fraud, but only after a fraudulent incident has occurred. They are most likely to switch primary banks or switch forms of payment *after* fraud has been committed. They widely use online banking and bill pay and are quick to adopt mobile banking.

While technology is helping consumers to monitor, detect and resolve identity fraud, consumers should be vigilant about safeguarding their personal information online and offline. Consumers can leverage technologies that are available through their financial institutions to help protect their information. Consumers should follow best practices and change passwords regularly, refrain from sharing passwords or other account information, lock computers and safeguard personal information, use a paper shredder to destroy paper account documents, keep anti-virus software up to date on their personal computers, and use discretion when sharing information on e-commerce sites. Mobile banking and mobile commerce are not as yet widely susceptible to fraud, however consumers should apply the same practices to those channels as well.

Consumers can play a key role in preventing, detecting and resolving identity fraud committed against them

This year’s Identity Fraud Report found that more consumers are pursuing legal action following identity fraud, with nearly 50 percent of all victims filing police reports. Empowered consumers are leading to more arrests, prosecutions and convictions. Most consumers are actively monitoring accounts for suspicious activity and fraud and are acting faster when fraud is detected.

All consumers need to better secure their private information. Perpetrators who are known to victims committed more non-card and new accounts fraud in 2009. Reasons for this include theft of physical documents from places such as desks and mailboxes, sharing computers with friends and family, storing online account passwords and using auto-login, and using simple, guessable passwords.

Consumer Recommendations for Prevention, Detection and Resolution™ of Identity Fraud

1. Prevent Criminal Access by Protecting your Paper Documents

- Keep sensitive information from prying eyes. Request electronic statements, use direct deposit, and don't put checks in an unlocked mailbox. When your Social Security number is requested as an identifier in paper documents, ask if you can provide alternate information. At home or work, secure your personal and financial records in a locked storage device—last year, at least 13% of all identity crimes were committed by someone previously known to the victim. Shred any sensitive paper documents.

2. Prevent High-Tech Criminal Access

- Install anti-virus software on your computer and keep it updated along with your applications and operating system.
- Secure your electronic personal and financial records on your computer behind a password.
- Never respond to requests for personal or account information online (or over the phone). Watch out for convincing imitations of banks, card companies, charities and government agencies in the mail, on the Web, over the phone, or on your mobile device. Use legitimate sources to contact financial institutions, such as an official website or the telephone number listed on statements and the back of bank or credit cards.
- Don't publish your birth date, mother's maiden name, pet's name or other identifying and personal information on social media websites.
- Use unique and hard-to-guess passwords, including for your wireless Internet connection, and don't access secure Web sites using public Wi-Fi.
- Install security patches and software updates as soon as they are released by verified sources. For phones, turn off Bluetooth and Wi-Fi if they are not being used.

3. Detect Unauthorized Activity in Existing Accounts

- Monitor current available bank and credit card account balances at least weekly, via online, mobile, ATM, or touch-tone banking. Sign up for alerts to be sent to your mobile phone or e-mail account. Javelin's study of 5,000 adults finds 43 percent of all reported identity fraud cases are spotted by consumers self-monitoring their accounts and those who use more timely electronic methods to detect fraud experience lower average out-of-pocket costs.

4. Detect Fraudulent Establishment of New Accounts.

- Monitor your credit reports and non credit account information to spot unauthorized activity. Free credit reports from each of the three major credit bureaus are available each year 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 offer timely and thorough protection.
- If you receive a letter notifying you that your private records were involved in a data breach, 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. One in four letters are followed by actual fraud, yet many who are alerted fail to take action.

5. Resolve Identity Fraud Completely

- Work through your bank, credit union or protection services provider to report problems immediately and take advantage of your financial provider's offers of loss protections (all large financial institutions offer zero-liability for debit and credit cards and many provide the same protection for online banking and bill-pay).

For Additional Educational Tips, Consumers Should Visit:

- Fiserv
www.ebillplace.com/staysafe
- Intersections Inc.
<http://www.identityguard.com/consumer-tools>
- Wells Fargo Fraud Information Center
https://www.wellsfargo.com/privacy_security/fraud/
- ITAC, Identity Theft Assistance Center
<http://www.identitytheftassistance.org>

For the consumer report, please visit: www.IDSafety.net

To register for an interactive webinar detailing the report's findings, please visit:

<https://www1.gotomeeting.com/register/115681009>

About Javelin Strategy & Research

Javelin is the leading independent provider of quantitative and qualitative research focused exclusively on financial services topics. Based on the most rigorous statistical methodologies, Javelin conducts in-depth primary research studies to pinpoint dynamic risks and opportunities. Javelin helps its clients achieve their initiatives through three service offerings, including

syndicated research subscriptions, custom research projects and strategic consulting. Javelin's client list includes some of the largest financial institutions, technology enterprises and security firms.

#