Contact:
Nancy Ozawa
nozawa@javelinstrategy.com
(925) 219-0116

Scott Love or Mark McClennan
javelin@schwartzmsl.com
781-684-0770

For Immediate Release

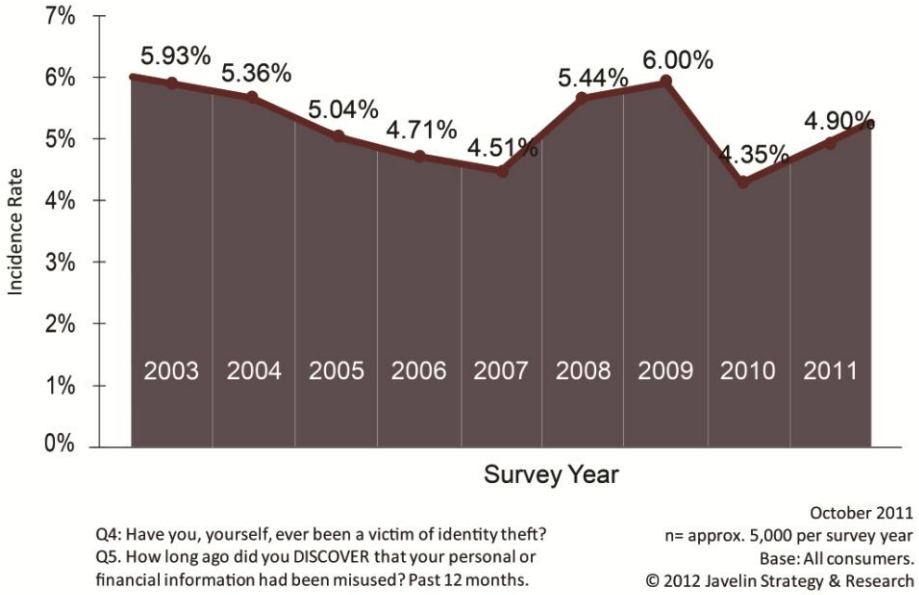
Identity Fraud Rose 13 Percent in 2011
According to New Javelin Strategy & Research Report

Consumers' Social and Mobile Behaviors May Be Putting Them at Greater Risk

Data Breach Victims 9.5 Times More Likely To Be Fraud Victims

SAN FRANCISCO, February 22, 2012 – The 2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier , released today by Javelin Strategy & Research (www.javelinstrategy.com), reports that in 2011 identity fraud increased by 13 percent. More than 11.6 million adults became a victim of identity fraud in the United States, while the dollar amount stolen held steady. The report also took the nation's most comprehensive quantitative look at consumer behavior and fraud and found consumers' social media and mobile behaviors may be putting them at greater risk.

Identity Fraud Rate Rose in 2011



Javelin Strategy & Research, Made Possible by Fiserv, Intersections Inc., Wells Fargo

Now in its ninth consecutive year, the comprehensive analysis of identity fraud trends is independently produced by Javelin Strategy & Research and made possible by Fiserv, Intersections Inc. and Wells Fargo & Company, companies dedicated to consumer fraud prevention and education. It is the nation's longest-running study of identity fraud, with 42,951 respondents surveyed over the past nine years.

Identity fraud is defined as the unauthorized use of another person's personal information to achieve illicit financial gain. In October 2011, Javelin Strategy & Research conducted an address-based survey of 5,022 U.S. consumers to identify important

findings about the impact of fraud, uncover areas of progress, and identify areas in which consumers must exercise continued vigilance.

"While identity fraud incidence increased last year, it is becoming less profitable for fraudsters. Consumers, the financial services industry, law enforcement and government agencies are stopping fraud earlier and making new account fraud more difficult to perpetrate," said James Van Dyke, president and founder of Javelin Strategy & Research. "The study found specific opportunities for improvement. Consumers must be vigilant and in control of their personal data as they adopt new mobile and social technologies in order to not make it easier for fraudsters to perpetrate crimes. Our survey found data breaches are increasingly putting consumers at risk. Consumers and organizations should always carefully and actively monitor accounts, but they should pay particular attention after an incident."

Key Findings

The study found four overall fraud trends:

- **Identity fraud incidents increased, amount stolen remained steady—**The number of identity fraud incidents increased by 13 percent over the past year, but the dollar amount stolen remained steady. Additionally, consumer out-of-pocket costs have decreased by 44 percent since 2004, likely due to the improved prevention and detection tools that have come available as well as fraud alerts leading to reduced detection time.

- **Social behaviors put consumers at risk—**For the first time, Javelin examined social media and mobile phone behaviors and identified certain social and mobile behaviors that had higher incidence rates of fraud than all consumers. LinkedIn, Google+, Twitter and Facebook users had the highest incidence of fraud although there is no proof of direct causation. The survey found that despite warnings that social networks are a great resource for fraudsters, consumers are still sharing a significant amount of personal information frequently used to authenticate a consumer's identity. Surprisingly those with public profiles (those visible to everyone) were more likely to expose this personal information. Specifically, 68 percent of people with public social media profiles shared their birthday information (with 45 percent sharing month, date and year); 63 percent shared their high school name; 18 percent shared their phone number; and 12 percent shared their pet's name—all are prime examples of personal information a company would use to verify your identity.

- **Smartphone owners experience greater incidence of fraud—**The survey found seven percent of smartphone owners were victims of identity fraud. This is a 1/3rd higher incidence rate compared to the general public. Part of this increase may be attributable to consumer behavior: 32 percent of smartphone owners do not update to a new operating system when it becomes available; 62 percent do not use a password on their home screen—enabling anyone to access their information if the phone is lost; and 32 percent save login information on their device

- **Data Breaches increasing and more damaging —** One likely contributing factor to the fraud increase was the 67 percent increase in the number of Americans impacted by data breaches compared to 2010. Javelin Strategy & Research found victims of data breaches are 9.5 times more likely to be a victim of identity fraud than consumers who did not receive such a data breach letter.

Understanding the Findings

Approximately 1.4 million more adults were victimized by identity fraud in 2011, compared to 2010. Countering this rise is the successful effort to combat identity fraud coupled with greater consumer awareness of the issue. While the number of fraud incidents increased, the total amount lost remained steady.

One of the key factors potentially contributing to the increase in incidents was the significant rise in data breaches. The survey found 15 percent of Americans, or about 36 million people, were notified of a data breach in 2011. Consumers receiving a data breach notification were 9.5 times more likely to become a victim of identify fraud.

According to the survey the three most common items exposed during a data breach are:

- Credit card number
- Debit card number
- Social Security number

Some factors contributing to the decline in overall fraud amounts are the more stringent criteria financial institutions are applying to authenticate users and determine credit risk, as well as more Americans monitoring accounts online and using monitoring protection services that can provide alerts and updates. For the first time, more Americans detected fraud by monitoring accounts through the internet, ATM or other electronic means than by examining paper records (24 percent vs. 11 percent). Additionally, there was a 42 percent decline in new account fraud, which can be the most costly and difficult to detect.

When it comes to social networks, LinkedIn users are more than twice as likely to have reported being a victim. Fraud incidence among MySpace users is lower compared to the general consumer. Additionally, those consumers who regularly check-in with GPS-enabled information also reported fraud rates more than double the average.

Eight Safety Tips to Protect Consumers

Javelin Strategy & Research recommends that consumers follow a three-step approach to minimize their risk and impact of identity fraud: Prevention, Detection and Resolution™.

Prevention

1. **Keep personal data private—**At home, at work and on your mobile devices, secure your personal and financial records in a locked storage device or behind a password. Of those consumers who knew how the crimes were committed, nine percent of all identity fraud crimes were committed by someone previously known to the victim in 2011. Avoid mailing checks to pay bills or to deposit funds in your banking account. Use online bill payment on a secure Internet access (not a public Wi-Fi hotspot) instead and direct deposit payroll checks.

2. **Be social, be responsible**—While social networks are popular, be careful about publicly exposing personal information that is typically used for authentication (full birthdate, high school name). This applies to all social networks.

3. **Use mobile devices responsibly—**Mobile devices are a treasure trove of information for fraudsters. The "always on" functionality of mobile devices provides fraudsters with new avenues for securing information. Be sure of the applications you download, the data you share over public Wi-Fi and where you leave your devices.

4. **Ask questions—** Before providing any information on mobile phones, social media sites and transactions sites, question who is asking for the information? Why do they need it? How is the information being used? If volunteering information, ask yourself if you have more to gain or more to lose by sharing personal and unnecessary details.

Detection

5. **Take control—**In 2011, 43 percent of fraud was first detected by the victims. By monitoring accounts online at bank and credit card websites, and setting up alerts that can be sent via e-mail and to a mobile device, consumers can more quickly detect if they are a victim of identity fraud and stop it early.

6. **Learn about methods to protect your identity—**There is a wide array of services available to consumers who want extra protection and peace of mind. These include credit monitoring, fraud alerts, credit freezes and database scanning. Some services can be obtained for a fee and others at no cost. These services can detect potentially fraudulent information from credit reports, public records, and online activity that are difficult to track on your own.

Resolution

7. **Report problems immediately—**Work with your bank, credit union or protection services provider to take advantage of resolution services, loss protections and methods to secure your accounts. A fast response can enhance the likelihood that losses are reduced, and law enforcement can pursue fraudsters so they experience consequences for their actions**.**

8. **Take any data breach notification seriously—**If you receive a data breach notification, take it very seriously as you are at much higher risk according to the 2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier. If you receive an offer from your financial institution or retailer for a free monitoring service after a breach, you should take advantage of the offer or closely monitor your accounts directly.

For Additional Educational Tips, Consumers Should Visit:

- Fiserv
  http://www.ebillplace.com/staysafe
- Intersections Inc.
  http://www.identityguard.com/identity-theft/protect-identity
- Wells Fargo
  www.wellsfargo.com/privacy_security/fraud_prevention/
- Better Business Bureau
  www.us.bbb.org

To take an identity fraud safety quiz and download a free consumer version of Javelin's identity fraud report, and get additional safety tips, visit www.idsafety.net.

Law enforcement professionals who are sworn officers and are interested in obtaining a copy of the complete report, please contact: nozawa@javelinstrategy.com.

About Javelin Strategy & Research
Javelin Strategy & Research is the leading provider of quantitative and qualitative research focused on the global financial services industry. Our extensive quantitative data and deep analyst experience enable us to forecast the direction of the financial services market and make recommendations that empower you and your business to succeed.
For more information on this project or other Javelin studies, visit www.javelinstrategy.com/research.

###

Keywords: Identity Theft, Identity Fraud, Fraud Victims