

02/20/2014

By Admin

Earlier this month Javelin Strategy and Research [reported](#) the results of its latest identity fraud survey. Javelin defines identity fraud as the unauthorized use of another person's personal information for illicit financial gain. The survey revealed that there were more than 13 million identity fraud victims last year, an increase of 500,000 over 2012 and the second highest number since the study began 11 years ago. The total dollar amount criminals stole decreased by \$3 billion, however, reflecting more aggressive actions by financial institutions, identity theft protection providers, and consumers to detect ID theft and block criminals from using the stolen information.

Here are some of the key findings from the survey:

- While identity fraud incidents increased, the actual dollar amount stolen decreased to \$18 billion (significantly lower than the \$48 billion stolen in 2004).
- The types of fraud have changed. Account takeovers rose dramatically, hitting new highs for the second year in a row and accounting for 28% of identity fraud losses.
- Data breaches posed the greatest for potential for identity fraud. One in three people who received notifications of data breaches became fraud victims.
- Identity fraud unrelated to payment cards tripled and accounted for \$5 billion in losses. This included compromised lines of credit, Internet accounts (e.g., Ebay, Amazon) and email payments such as PayPal.

Javelin offered these safety tips for consumers:

1. Keep personal data private. Secure your personal and financial records behind a password or in a locked storage device at home, at work and on your mobile device.
2. Opt-in to two factor authentication wherever it is offered. Some financial institutions, alternative payment providers and other service providers offer the option of adding a layer of security to your account beyond the basic username and password.
3. Just say no to SSN authentication. Eighty percent of the top 25 banks and 96 percent of top credit card issuers will allow account access using your Social Security Number (SSN) as an authenticator.
4. Be proactive and enlist others. There are many different levels of identity theft protection and consumers should work in partnership with institutions on identity theft prevention.
5. Take any data breach notification seriously. If you receive a data breach notification, take it very seriously as you are at a much higher risk.
6. Don't wait. Report problems immediately. If you suspect or uncover fraud, contact your bank, credit union, wireless provider or protection services provider to take advantage of resolution services, loss protections and methods to secure your accounts