12 Signs Your Identity Might Have Been Stolen

by Brian O'Connell October 17, 2017 www.experian.com

A record 15.4 million Americans were victimized by identity theft last year, with fraudsters netting $16 billion in ill-gotten gains, according to the 2017 Identity Fraud Study by Javelin Strategy & Research. Since 2011, Javelin reports, identity thieves have stolen $107 billion from U.S. consumers.

Identity Theft: How Do You Know When You've Been Victimized?

With so much at stake, Americans may (and should) wonder: "How would I even know if my identity was stolen?"

There is no single answer to that question, as data security experts state there are myriad signs that an individual's identity has been compromised. Meanwhile, cyber-fraudsters are using that data to steal the victim's money, especially with bank account, credit card, Social Security number and tax return fraud campaigns.

"There are plenty of signs that your identity may have been stolen," says Robert Siciliano, an identity theft expert and CEO of IDTheftSecurity.com. "You notice accounts you didn't open and debts on your accounts that you can't explain, or you see fraudulent or inaccurate information on your credit reports, including accounts and personal information, such as your Social Security number, address, name or initials, or employer."

What other major signs raise a "red flag" that your identity has been compromised or stolen? Here are some high-risk scenarios that worry even experienced data protection specialists:

1. Failing to receive bills or other mail

This could indicate that an identity thief has taken over your account and changed your billing address, says Siciliano. "Make sure to follow up with creditors if your bills don't arrive on time,".

2. You're rejected for credit

"Being denied credit or being offered less favorable credit terms, like a high-interest rate, for no apparent reason, is a sign your identity may have been compromised," Siciliano says.

3. You're getting bills for purchases you didn't make

If you start receiving bills or notices of overdue payments in regard to accounts you don't have, you have probably become a victim of identity theft, says Steven J.J. Weisman, a college professor who teaches white-collar crime at Bentley University and is the author of the book Identity Theft Alert. "In this case, you should contact the creditor and inform them that you have been a victim of identity theft and it is not your debt, and also file a police report. "While there is little chance of the criminal being caught. It helps prove that you have been a victim of this crime."

4. Your bank account, brokerage account, credit card account or other accounts have unauthorized transactions

"Again, look into the specific charges, file a police report and demand that the fraudulent activity be stopped and the institution reimburse you for any losses," Weisman says. "You should also be regularly monitoring your credit reports and all of your financial accounts to recognize fraud as soon as possible.".

5. You receive a tax transcript in the mail that you didn't request

"Under this scenario, a fraudster logged on to the Internal Revenue Service website and tried to get your information and couldn't download it immediately because some security test failed," says Abby Eisenkraft, chief executive officer of Choice Tax Solutions, Inc. "Consequently, the IRS mailed it to you, instead, under the assumption you requested the document."

6. Your electronically filed tax return is rejected

This a big sign your identity has been compromised, says Eisenkraft. "That's especially the case if your return is rejected and there are no typos and the Social Security number is correct. What likely happened is that an identity thief filed a tax return in your name, claiming a fraudulent refund."

7. You receive a tax refund you did not request

Here, you may get a check or pre-loaded debit card. "What happened is that an identity thief filed a fraudulent return and will try to find the refund in your mailbox," says Eisenkraft.

8. Your employer lets you know you've got a data security problem

If a hacker has your Social Security number and the name of your current employer, they can try to collect unemployment benefits in your name. "In this case, if your company is on the ball you might hear from someone in human resources," states David Cox, an identity theft expert and CEO and founder of LiquidVPN, in Cheyenne, Wyo. "Most hackers will check your social media to see if you just quit a job or just started a new job. With this information, they are much more likely to get away with it for quite a bit longer. Eventually, you will hear from your former employer or the unemployment agency."

9. You get two-factor authentication alerts

It's a problem when you get a text message sending you a six-digit pin to enter into a service or membership you don't recognize, says Ralph Rodriguez, an MIT Fellow, and chief technology officer at Confirm.io, a personal data security firm. "Maybe it's a new account," Rodriguez says. "Perhaps it's account recovery for your bank. The point is you don't know. And it's a very eerie feeling when it happens."

10. Your credit score is actually rising

Strange, but true, Rodriguez says – a rising credit score can mean trouble on the identity fraud front. "Check your credit reports frequently for accounts you didn't open and hard inquiries which could suggest fraudsters are trying to extend credit in your name," he advises.

11. You get small "test charges" on your credit card

Hackers often place a small charge for a couple of bucks on the card to see if it will go through before they initiate an attempt at a larger fraud later, says Ross Federgreen, CEO of CSR, a compliance solutions firm, and a data privacy expert. "If you have a small charge you don't recognize, don't ignore it," says Federgreen.

12. You get increased direct mail and phone solicitations for expensive items

The notices could be for cars, loans, and home improvement, and other big-ticket items," Federgreen says. "This could be the result of new high-ticket activity run on your account."