

BUSINESS FEB 2 2017, 7:21 AM ET

Identity Fraud Hits Record Number of Americans in 2016

by HERB WEISBAUM

Identity thieves, who commit financial fraud with stolen account information, had a banner year in 2016. These fraudsters successfully hit a record 15.4 million Americans — up 16 percent from 2015, according to the new 2017 Identity Fraud Study from Javelin Strategy & Research.

Despite widespread efforts to fight this crime wave, the crooks successfully netted two million more victims and stole \$16 billion dollars, a nearly billion dollar year-to-year increase. And remember, we all pay for that loss in the form of higher prices and interest rates.

“The criminals are getting better at committing this fraud,” said Al Pascual, research director and head of fraud and security at Javelin Strategy & Research. “They learn and they adapt and they find workarounds to the solutions we put in place.”

A Huge Increase in Internet Fraud

Another big change in the fraud landscape is the significant increase in card-not-present (CNP) fraud that took place last year, as criminals used stolen credit and debit card numbers to buy things online or over the phone. CNP fraud jumped 40 percent, while point-of-sale fraud remained essentially unchanged.

Clearly, ID thieves are moving online as the continued adoption of chip-based EMV cards — which are nearly impossible to counterfeit — makes fraud at the checkout counter more difficult.

“We think of stopping fraud like squeezing Jell-O — when you stop it one place, it squirts out someplace else,” said Stephen Coggeshall, chief analytics and science officer at Lifelock, which sponsored the Javelin study. “These fraudsters

are pretty smart and they continue to look for the weakest points of attack.”

Fraud experts predicted this — that EMV cards would drive criminals to use stolen credit card numbers online. It’s what happened when chip-based cards were introduced in other parts of the world.

Related: New Chip Cards Lead to Dramatic Rise in Online Fraud

Even so, Pascual told NBC News, he was surprised that CNP fraud went up as much as it did.

“Criminals are getting much better at committing fraud online,” Pascual said. “Their skill sets are improving and the tools that they’re using are much more sophisticated. They’re using things like botnets to complete orders at high speed that can overwhelm a merchant’s security defenses.”

Plus, online shopping is convenient — less work and less risk of being caught. That’s why Pascual predicts card-not-present fraud will get worse in the near future — until financial institutions, card issuers and retailers learn to deal with the evolving threat.

Two More Troubling Trends

The Identity Fraud Study found that new account fraud continues to flourish and account takeover fraud rose dramatically. New account fraud nearly doubled last year.

As EMV technology continues to become more widely adopted, criminals are changing their game and opening a new credit account using your name. They simply buy stolen information — name, date of birth, mother’s maiden name, even Social Security number — and use it to open that new account.

New account fraud has another advantage for the thief — it’s more likely to go undetected for longer. Victims don’t see unauthorized charges on their credit card statement because the crooks created new accounts and have the statement go

to them.

Account takeover (ATO) fraud made a big comeback last year. As its name implies, the ID thief uses your stolen personal information to access your account and have a new card sent to them. Javelin found that both the volume of ATO cases and the amount of money stolen this way rose dramatically. The loss is estimated to be \$2.3 billion, up 61 percent.

Another alarming finding: The hijacking of mobile phone accounts nearly doubled from 2015. Using stolen Social Security numbers, the thieves can get themselves onto your account and intercept your email and text messages. Why do that?

“It’s because people get alerts and notifications and one-time passwords sent to their mobile phones,” Pascual explained. “Criminals know that, so they take over the phone account to intercept messages and passwords that let them compromise those people’s financial accounts.”

One Bright Note

Financial institutions, card issuers and retailers are getting better at detecting this fraud sooner, the report noted. Consumers are also paying more attention to their financial accounts — checking them online and setting alerts to spot unauthorized transactions.

While that doesn’t stop the fraud from happening, it does limit the damage that can be done.

“Identity fraud continues to grow, but at the same time we’re catching these incidents earlier and more frequently,” Lifelock’s Coggeshall said. “So even though the attempts continue to grow, the technology is working and the dollar loss per attack is going down.”

The Privacy Rights Clearinghouse has detailed information on how to reduce your risk of identity theft.

Herb Weisbaum is The ConsumerMan. Follow him on Facebook and Twitter or visit The ConsumerMan website.
