3/13/18

By Susan Grant, Director of Consumer Protection and Privacy, Consumer Federation of America

Last week was National Consumer Protection Week, but when it comes to fraud and identity theft, consumers don't have much to celebrate. Statistics recently released by the Federal Trade Commission (FTC) and a private consulting company, Javelin Strategy & Research, are truly alarming. Consumers are losing lots of money – money that they could be saving and spending on legitimate products and services. They're also losing confidence in their ability to protect their personal information.

Javelin has been tracking identity fraud (the fraudulent use of consumers' stolen personal information) through surveys since 2003. In its latest report , Javelin said that there were 16.7 million identity fraud victims in the U.S. in 2017, up by eight percent from 2016. Losses rose from $16.2 to $16.8 billion. Fraudulent takeovers of consumers' accounts jumped by a whopping 120 percent, and victims spent an average of $290 and 16 hours to fix those problems. Javelin also found that there was a 200 percent increase in fraudsters shifting money from consumers' existing financial accounts into new accounts that they opened with companies such as PayPal and Amazon using the victims' identities.

Not surprisingly given the massive Equifax data breach and other breaches last year, 30 percent of the consumers surveyed said that they'd received a data breach notice in 2017, compared to 18 percent in 2016, and the proportion of consumers who said that they were concerned about identity fraud rose from 51 to 69 percent. For the first time ever, more Social Security numbers were compromised than credit card numbers. Sixty-four percent of breach victims believe that breach notices don't do much to protect them. And many consumers are unsure that they can effectively protect themselves from identity fraud and feel that it's the responsibility of the companies that hold their personal information.

The FTC's annual report is based on consumer complaints. Since the statistics are not from a random survey, they don't necessarily paint the full picture. So while there were fewer identity theft complaints in 2017 (1,166,244) than in 2016 (1,390,102), that doesn't mean that identity theft decreased. Indeed, Equifax recently announced that there were

2.4 million more
U.S. consumers affected by its
2017 data breach
, though unlike the other 145.5 million victims, their Social Security numbers weren't exposed.

While there are some positive signs from the FTC's identity theft statistics – complaints concerning tax fraud dropped by 46 percent, for instance – there are some disturbing signs as well. Complaints about new landline telephone accounts being opened using consumers' stolen information jumped 150 percent and there was a 109 percent increase in complaints about fraudulent takeovers of consumers' existing landline accounts. Fraudulent new accounts and account takeovers for mobile service also rose, by 19 and 11 percent, respectively. What's behind these numbers is unclear but they raise the question: how can we make it harder for identity thieves to get phone service using victims' personal information?

There were also significant increases in complaints about identity thieves obtaining student loans (121 percent), medical services (40 percent) and auto loans or leases (43 percent), making online purchases, (43 percent), renting houses or apartments (39 percent) and getting government benefits (34 percent) in their victims' names. Complaints about taking over consumers' bank accounts rose by 24 percent, and there was a 20 percent increase in complaints concerning credit card account takeovers.

The FTC report doesn't include information about the amount of money that identity theft victims lost or what they spent to recover from the problems, but it does provide statistics about losses in complaints about other types of fraud. The total loss was $905 million, an increase of $63 million from 2016, even though there were 56,413 fewer fraud complaints. Imposter scams topped the list of fraud complaints. These are when crooks trick consumers to give them money by pretending to be from a government agency, a bank, a tech support company or others that they trust. The median loss in those scams was $500, but in some fraud categories it was much more. The highest median losses were: $1,063 in business and job opportunity scams; $1,200 in bogus offers to help settle their debts or save their homes from foreclosure; and $1,710 in false promises involving travel, vacations, and timeshares.

Two other things jump out from the FTC's fraud statistics. One is that in 70 percent of these complaints, the fraud began with a phone call to the consumer. The FTC received more than seven million complaints about unwanted calls last year, a jump of nearly two million from 2016, and 4.5 million of them were robocalls (these statistics are released in a separate report). It's illegal to make robocalls for sales purposes without consumers' prior consent, and few people would knowingly agree to it. Caller ID that is falsified with the intent to harm someone is also

illegal and is often a feature in imposter scams and other fraudulent calls. So it's likely that many of these unwanted calls were from crooks.

It's also notable that in the fraud complaints where the payment method was known, more than 46 percent of the payments were made using wire transfer services, for a total of $333 million. In January 2017 Western Union settled with federal law enforcement agencies and state attorneys general to resolve charges that it knew that fraudsters were using its services to get victims' money and didn't do enough to stop it. This wasn't the first time these issues were raised with Western Union; it settled similar accusations from a number of states in 2005. In 2009 MoneyGram made a settlement with the FTC and, more recently, with state attorneys general concerning the same kinds of problems. Yet these services are still the preferred method of payment for scammers and they continue to get away with it.

Here are some recommendations for fighting identity theft and fraud more effectively:

- Consumers should put freezes on their credit reports and take other steps to make it harder for fraudsters to use their stolen personal information. Freezes should be free for all.

- Consumers should be entitled to better security for their personal information, not weaker data breach notice standards, and to hold companies liable for lax security.

- Consumers should understand their telemarketing rights and assume that any caller who appears to be violating them is a crook.

- The federal government should require phone companies to do more about robocalls, fraudulent Caller ID spoofing and other violations of consumers' no-call rights.

- Payment services and financial institutions should make significant and sustained efforts to prevent fraudsters from using them to get victims' money, and educate their employees, business partners and consumers about how to spot and stop scams.