ID theft stings, but it's hard to pin on specific data hacks

August 3 2019, by Anick Jesdanun

In this Tuesday, July 30, 2019, file photo, the logo for Capital One Financial appears above a trading post on the floor of the New York Stock Exchange. Data breaches through hacking attacks are common these days, and personal details about you can lead to identity theft, such as credit cards and loans in your name. Yet few victims can ever pin the blame on any specific breach, whether that's Equifax from 2017 or the recently disclosed breach at Capital One. (AP Photo/Richard Drew, File)

Equifax 2017. Marriott 2018. Capital One 2019.

Data breaches through hacking attacks are distressingly common these days, and personal details about you can lead to identity theft, such as credit cards and loans in your name. But it's hard to pin the blame on any specific hack, as the most sophisticated criminals combine data from multiple attacks to better impersonate you.

"That's why fraud can be emotionally challenging," said Kyle Marchini, a specialist in fraud management at the financial research group Javelin. "It just comes out of the blue, and there's no way to identify where it came from or what I could have done to prevent that."

While the number of reported breaches decreased slightly last year to 1,244, according to the nonprofit Identity Theft Resource Center, the total number of records exposed more than doubled to 447 million. That suggests hackers are focusing on larger organizations with bigger payoffs. Last year's figures include data on about 383 million . Marriott guests in a breach that investigators suspect was tied to the Chinese government.

Criminal rings often buy datasets from multiple hacks to commit fraud. The idea is to collect enough information to get past ID verification and authentication checks that banks and other institutions employ. One database with your Social Security number might have your old address, but hackers can simply sub in your current one from a more recent database.

"We're in this vicious cycle," said Eva Velasquez, the ID theft center's CEO. "We create and capture and use more and more data points about a specific individual in order to fight fraud and authenticate people. That, in turns, makes data more valuable to the thieves, so they are going to increase the efforts to get that data."

Fraudulent card charges are relatively easy to reverse, and U.S. law limits credit card liability for consumers. But fraud involving new accounts is tougher to deal with.

Javelin estimates that the average victim spends 18 hours dealing with the fallout, including convincing collection agencies and credit-ratings agencies that the accounts weren't really theirs. And victims wind up spending hundreds of dollars out of pocket. Javelin estimated that more than 3 million U.S. adults were victims of new account fraud last year, nearly triple the number in 2013.

Much of the increase can be attributed to the cumulative effect of data breaches and the types of information stolen.

While credit card numbers and passwords can be changed, birth dates and Social Security numbers typically stay with you for life. And U.S. passport numbers stick around for 10 years. Hackers in the 2017 breach of credit monitoring firm Equifax got some or all of that from 147 million people. Equifax agreed last week to pay at least $700 million to settle lawsuits.

Just a few days later, the bank Capital One disclosed a breach of personal information of 106 million Capital One credit card holders or applicants in the U.S. and Canada. The data included self-reported income, credit scores and account balances. Although Capital One said it doesn't believe the information was used for fraud, the breach further increases worries about leaked data—in this case, the very types of information needed to submit credit card applications.

"Every breach increases the risk because different pieces of information come out," said Deepak Patel, a vice president at the security firm PerimeterX.

Beyond financial applications, personal data can be useful for telemarketing and email phishing scams, as fraudsters try to trick you by claiming they already know you. And criminals armed with such data can impersonate you on calls with financial institutions to get money transferred or a mailing address changed.

You can take such precautions as freezing your credit, which stops thieves from opening new credit cards or loans in your name. Doing so is now free, though you'll have to temporarily unfreeze your credit if you apply for a new credit card or loan.

You can also sign up for a credit monitoring service, which alerts you when someone is pinging your credit report, a precursor to opening a new account. There are also ID protection services that will scan the internet underground for signs your personal data is for sale. Some of these services are available for free to customers hit with data breaches, including the one at Equifax.

But Jason Wang, who founded TrueVault to help companies protect data, said there's not a lot consumers can do once their data is in the wild. A better approach, he said, is to minimize what data is sitting on servers—something a California privacy law may do if it takes effect as planned on Jan. 1. Among other things, customers can seek information on what data companies have on them and request its deletion—although companies wouldn't have to do anything unless they get such requests.