Fighting The Disease Of ID Fraud

cyber security technology

Summary: The number of identity fraud victims last year rose by 8% to 16.7mm US consumers, despite widespread efforts to stop this type of fraud. What more can your bank do?

There is a strange process that unfolds when doctors prescribe you medicine. They apparently look to pooled cohort equations (PCEs) to help determine your risk of heart attack or stroke. In so doing, doctors leverage data to be sure the exact level of medication is effective and safe for the patient. Interestingly, Stanford University research finds some 11mm people may have been given the wrong prescription for a host of drugs, based on PCEs. A key problem is that PCEs use datasets that are outdated. In fact, one dataset cited in the research is from 1948. Given how much more we now know about diet, exercise, genes and other factors, the math finds people's risks may have been estimated 20% higher than they actually were in today's terms - ouch!

When it comes to data theft though, bankers in some cases may feel like they have been under-prescribed medicine to fight the disease of online fraudsters.

In fact, research by Javelin Strategy & Research finds online fraudsters are more actively targeting and creating the "identities" of individuals in an effort to steal money directly from legitimate accounts or create lines of credit tied to fake personas or breach systems. The number of identity fraud victims last year increased by 8% to 16.7mm US consumers, despite widespread efforts to decrease this type of fraud. This also marks an all-time high for identity theft in the 15Ys that the researcher has been tracking it.

Successful data thieves are morphing and some have upped their game to stealing Social Security numbers and other personal identifiers. This lets them create "synthetic" identities, which can be used to access legitimate customers' accounts or to create new accounts where money can be stolen.

Cases in point: The Javelin study found that 30% of US consumers suffered a breach in 2017 vs. 12% in 2016. Also, for the first time, the number of individuals who had their Social Security number stolen or compromised (35%) outpaced the number that had their credit card number swiped (30%). Synthetic identity theft cost US banks nearly $6B in 2016, according to Auriemma Consulting Group.

As fraudsters become more sophisticated, we have some suggestions to help keep your bank and customers safe:

Consider stronger authentication. As the criminal element pushes the envelope, banks need a more definitive means of verifying that their customers are indeed their customers. Biometrics can be much less expensive and are more commonplace too. Increasingly, third parties also offer cross-referencing on background checks for new customers. Geolocation and IP address matching can also be used to determine if an online or mobile customer is for real.

Educate customers for better security posture. Encourage customers to use two-factor authentication when they have the choice and educate them (as well as employees) about the necessity of using strong passwords and changing them on a regular basis. During online or mobile banking registration, make a point of

reminding customers to lock their device screens, not to share logon information, to use encryption, and avoid public WiFi access on the same device where they store banking and payment data.

Stay updated on recent scams. Whether it is through the FS-ISAC or another organization, executives or IT security staff should be keeping tabs on emerging forms of fraud so that they know what to pinpoint. Experts say that many industry and enforcement groups issue bulletins on up-and-coming attacks, in the hopes of getting the word out.

CECL SOLUTION - BUILT BY OUR BANK FOR YOUR BANK

CECL is one of the biggest challenges for community bankers these days. Our experts are ready to guide you every step of the way through this integration with no software to maintain. Learn more about our CECL Solution.