Managing Online Customer ID Fraud

risk management digital banking

Summary: Internet-based fraud is expected to hit $6T in 2021. We provide tips to help keep your online onboarding secure.

If you are trying to build deposits, you might want to alert your customers about a new survey from Fidelity Investments. It found 38% of baby boomers are too heavily invested in stocks. Good luck here, and let's hope some customers make the move to you.

As you think about this, you might also want to think about the best way to onboard new customers too. After all, the onboarding of new online or mobile customers is often when the most fraud happens, so managing that risk is critical.

As a result, the industry is increasingly looking to mitigate risk in the digital onboarding process, with an eye to reducing the identity fraud that often crops up at this initial stage. Indeed, internet-based fraud overall totaled $3T in 2015, and is expected to double by 2021 to $6T, according to Cybersecurity Ventures.

"Whenever technology changes the way people do business, it's only a matter of time until new types of fraud emerge," a 2019 IDnow report expounds. Not surprisingly, social engineering topped the list of the most common fraud attempts--underscoring the fact that the human is the most risky link in the security chain.

IDnow lists the most frequent fraud attempts as: social engineering at 73%; followed by the use of counterfeit or stolen ID cards, 16% and 11%, respectively. Fraudsters have been using social engineering to persuade unsuspecting end users to open online accounts for criminal activities for a long time. However, in 2019 the number of social engineering attempts increased in comparison to other fraud techniques (such as through bogus job ads, app trial offers or cut-rate loans to entice their victims into a deal with an online bank).

Security experts say there are techniques to combat this onslaught. First off, companies can try "device binding", which ensures that the account can only be used with the device that was used to open it. As soon as the account is accessed from another device, the user is required to verify their identity once again. Another option is to use well-trained personnel who can utilize psychological questions and detect inconsistencies during the video identification process to determine whether a customer is a potential social engineering victim. Lastly, multifactor authentication can also help you be extra sure that the online account user is not a fraud.

Opening and managing accounts online is something that is not going away. So, it is important to stay on top of the identities of these new online customers. Be diligent and ensure you have as many layers of security as possible, without pushing away new customers. This is an ongoing battle, but hopefully, we have helped in a little way today.

NEED MORE FEE INCOME? TRY HEDGING.

Financial institutions seeing long-term, fixed-rate demand from business clients can transform payments into a floating rate on their books using Borrowers' Loan Protection (BLP). Contact us today for more information.