Mobile Fraud And Trust

cyber security risk management digital banking

Summary: Suspected fraudulent transactions from mobile devices increased 138% since 2017. Staying on top of this is tough but important.

As you gear up to capture more customers this year, you might find it interesting that JD Power's 2019 US Retail Banking Satisfaction Survey finds only 4% of customers switched banks last year. One reason for low switch rates could be that more customers are fully embedded in their banks and using online and mobile channels heavily too.

As more customers conduct financial transactions via mobile though, bankers know that cyber criminals have flocked in too. This makes it increasingly difficult for bank customers to trust their mobile interactions.

According to research released by TransUnion's fraud prevention unit, iovation, suspected fraudulent transactions from mobile devices increased 138% since 2017. That beats overall mobile transactions by a long shot, which only grew by 30% over the same period. Furthermore, in the first half of 2019, 49% of all risky transactions came from mobile devices vs. 30% in 2018 and 33% in 2017.

The mobile device (typically a smartphone) is not only a conduit for financial transactions, but also for sensitive information of all kinds. It is typically also the platform from which customers authenticate their identity with a fingerprint or shared information. As such, fraudsters will often hide by using emulators to make it look like their desktop device is a mobile device, according to the iovation research.

Because of the rise in mobile fraud, it is more important than ever to evoke trust with your customers. Consumers say that they still value trust as their main priority in choosing and keeping a financial provider. Indeed, 75% feel that keeping their personal information private and having excellent security and fraud prevention protections in place are must-have decision factors, and 70% rate trustworthiness as a must-have.

In the interest of staying more secure, 80% say they would be interested in using an app that notifies users of unusual account activity, and seeks user approval before processing such transactions. Furthermore, 42% of online banking customers would like to receive a push notification each time they make a transaction so they can keep track of things and stop fraud.

The iovation report also shows that trust and security are very important factors when people choose a financial institution for general banking or credit card use. The survey shows 72% of consumers say account security and privacy determine which financial institution they will use. In addition, 64% say they will switch financial services companies if they can provide stronger security protocols (but again given the data in the intro we wonder about this). Also, almost 40% say they have closed an account due to concerns about fraud and account security (again, we wonder).

We know your customers have deep trust in your institution overall. Yet, with the speed of technology, such as mobile payments and authentication, reassuring them of your commitment to safe and secure transactions regularly keeps the trust level high.

SAVE TIME AND MONEY WITH OUR STRESS TESTING SERVICE

It is important to stress test loans of all types from multiple perspectives and on a portfolio basis. Get expert help to save you time and money. Learn more about stress testing today.