PCBB BID® Daily Newsletter Dec 21, 2017

Interpreting Survey Insights On Customer Fraud

risk management fraud protection

Summary: A recent survey found 60% of bank customers who experienced fraud discovered the issue before their banks told them about it. What can banks learn from this?

Doing a little research, we found out that there are currently 7,102 known languages still spoken around the globe. Of course, many of these are spoken by a small group of people and are even in danger of eventual extinction. To avoid the risk of extinction when it comes to speaking the language of cyber threats, we offer these thoughts to community bankers today.

Start by knowing that you are probably taking big steps already in responding to these threats. You have detection measures in place, you have procedures to follow when breaches are detected, and you strive to keep your fraud avoidance systems current. That is all good, but is it enough?

Before just checking the box that the bank's fraud detection and response system is up to speed, know that customers may be thinking something else. A recent March Networks survey of US bank customers found that 60% of those who experienced fraudulent activity in their accounts discovered the problem before their banks told them about it. That isn't great, but it is admittedly a problem the goes back eons. The survey also found about 15% of customers reported fraudulent bank account activity in 2016.

This issue points to the difficulties in managing the risk of fraud in general and cyber fraud more specifically as customer usage in that area continues to expand.

Interestingly, the survey tracks customer experience and not bank security performance, so perspective is important. Banks may actually be doing a better job of spotting and responding to cyber break-ins than customers realize, for instance. However, the fact that so many customers discovered that their accounts had been compromised before their banks notified them, suggests there is always more room to improve.

Keeping customers informed and updated on cyber breaches has become an important task for banks in this age of burgeoning cybercrime. Customers are bombarded with news on data breaches, which can make them jittery about the security of their bank account too. Continuing to emphasize with customer facing teams that communication is a priority will help with that.

The survey also finds that once banks get involved, customers approve of the results. The survey found 85% of customers said they were satisfied with how their bank handled incidents. That is nothing short of a rousing endorsement of how banks deal with customer account fraud or security issues and is an exceptional way to keep loyal customers.

Fraud detection will always be a critical area of concern for banks, so while things are probably ok now, there can always be more improvement. It doesn't hurt to periodically review processes and procedures to ensure there are no gaps.

While this survey finds there is still work to do with fraud detection customer notification, at the end of the day, banks are doing their best to keep customers safe, and they seem to be responding well.

Regulators and customers alike expect banks to respond quickly to fraud issues as they surface. Some quick links to share with your teams can be the FBI field office, the Anti Phishing Working Group, the postal inspector, the Federal Trade Commission or the internet crime complaint center. In the meantime, keep speaking with your customers to help them understand the language of how your bank protects them.

OUTSOURCED PROFITABILITY SOLUTIONS FOR YOU

ProfitIntel is an outsourced relationship profitability solution that combines a powerful pricing model with full-time consulting support. Contact us today for more information.

Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.