
The complexity of high-tech fraud

Electronically speaking, the bank is always open. Your fraud department should be, too

I will never give the bad guys credit, but we, as an industry, really need to take the criminal element seriously when it comes to electronic banking.

Internet fraud, card fraud, identity theft, and account take-over crimes are about exploiting the weaknesses between systems and the absence of vigilance more than anything else. Furthermore, the current de facto approach regarding fraud or the fraud potential is to wait until the customer complains before any action is taken. The next step, an investigation, is started which reveals the bad news. The money is gone and can't be recovered.

Many fraud systems are deployed today; some of them are good. The main challenge is that these systems are singular systems meaning that they monitor a single transaction system, such as credit or debit card transactions. Other fraud systems are BSA-AML centric which look for money laundering activity requiring the financial institution to review hundreds of suspicious transactions daily. The crooks know this and they exploit it to their advantage.

Some fraud systems create electronic cases after an unusual transaction and send an alert to the financial institution, which then contacts the customer in a variety of ways. Clearly, it is not a real-time system and more importantly, some institutions do not review these cases after hours, during weekends or holidays. The usual operating procedure is to look into these potential fraud cases on the next business day. I have to point out, however, that some fraud systems contact the customer directly via phone, text message, or even at the check-out counter. These systems are usually deployed by the largest financial institutions in the country.

Changing fraud management

The spectrum for effective fraud management has changed. That is to say that it is no longer an effective strategy to just

monitor your debit card or ACH transactions. These systems typically are managed in separate departments of the financial institution. They are not integrated at the core banking application level bank, nor is the information gathered into a central area and analyzed by a fraud department.

Waiting for the customer to complain about their account or to submit a Reg. E dispute means, more often than not, it is too late. Somebody is going to lose-the customer, a bank, or the merchant.

Transaction enterprise

What systems in your financial institution can generate a transaction-the teller window, the customer's checkbook, the internet, an ACH created when a customer initiated payment using a person-to-person (P2P) app on their cell phone, a billpay transaction, or a check that has been converted to a remote deposit capture transaction? All of these activities represent the transaction enterprise. It is the sum of these transactions all being reviewed and analyzed together that represent the foundation of 21st century fraud management. Each one of these systems is susceptible to fraud in an electronic banking and identity theft world. It is when you can look at all of these transactions together that the picture will be clear! Merely looking at your debit card fraud system is not enough.

Effective fraud management is effective risk management

More than one regulator has sounded the alarm about fraud, the growing number of identity theft crimes, and increasing risk around an electronic payment and banking world. It is a 7 by 24 by 365, anytime, anywhere world and that goes for banking, too. Fraud must be managed and monitored in the same context and by a central department. All activities that flow into and out of the transaction enterprise need to be reviewed in an integrated, automated, and real-time context. Failure to do so gives the crooks time to get away.

The fraud review should include customer history or use profiles, transaction origination point, and the type of transactions. The review must be around the clock each day of the year. Electronically speaking, the bank is always open, even though the doors are locked. Your fraud department, too, should be always on watch and empowered to act.

How can our institution implement such a process? First, the organization needs to come to grips with making a change to the current approach. Second, seek out a vendor that can provide a valid, real-time transaction enterprise fraud monitoring system. FIS and Verafin are two companies that have such systems. Third, be prepared to intervene, stop, and deny potentially fraudulent customer transactions immediately.

That is right. It is always easier to apologize for the inconvenience than explain to the bank president how the bank has just taken a \$50,000 loss and will need to immediately re-issue new debit cards for each customer!

The Wombat!

About the Author

Dan Fisher is president and CEO of The Copper River Group, a consulting firm headquartered in Fargo, N. D., that focuses on technology and payment systems research and consulting for community financial institutions. For nearly 30 years, Fisher has worked in the financial industry using technology to improve the bottom line. He was CIO of Community First Bankshares (now part of BancWest), has served as a director of the Federal Reserve Board of Minneapolis, the chairman of the American Bankers Association Payment Systems Committee, and was a member of the Independent Community Bankers of America Payments Committee. Fisher has written numerous articles on banking technology and the payments system. He has authored or co-authored six books and recently published a book titled, "Capturing Your Customer! The New Technology of Remote Deposit." You can contact Fisher at dan@copperrivergroup.com.

P.S. To understand Dan's nickname, check out "About the Wombat" on his website, www.copperrivergroup.com