COMMENTARY
3/18/2014
09:06 AM

Pat Carroll
Commentary

Connect Directly

2 comments
Comment Now

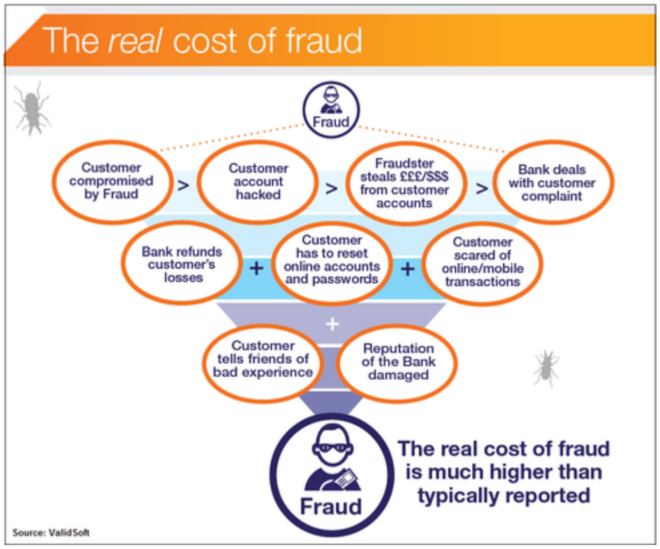
Login

Voice, Proximity Key To Cutting E-Payment Fraud

While we wait for EMV, US companies should lay the groundwork for strong security.

In my previous column, I talked about US adoption of EMV (the Europay, MasterCard, and Visa initiative) and how it can help reduce fraud when data is stolen from merchants or card payment processors. However, EMV alone can't solve the problem.

And the problem? It's severe. The 2013 LexisNexis True Cost of Fraud Study says merchants paid $2.79 for each dollar of losses they incur, up $0.10 on the dollar from 2012. Last year, the United States accounted for 47% of global fraud, while processing just 24% of payments by volume, according to the Nilson Report. In response, as I previously discussed, some non-US issuing banks are declining transactions on a massive scale, even though most are on the up and up. When a legitimate transaction is declined -- called a "false positive" in the trade -- costs can be 2-3 times higher than the actual potential fraud figure, and that doesn't include lost customer goodwill for someone standing at a checkout and having a card declined. The infographic below shows where that money goes.


The real cost of fraud
Fraud
Customer compromised by Fraud
>
Customer account hacked
>
Fraudster steals £££/$$$ from customer accounts
>
Bank deals with customer complaint
Bank refunds customer's losses
+
Customer has to reset online accounts and passwords
+
Customer scared of online/mobile transactions
+
Customer tells friends of bad experience
Reputation of the Bank damaged
Fraud
The real cost of fraud is much higher than typically reported

Source: ValidSoft

Let's start with two points.

First, countries that have adopted EMV have enjoyed significant reductions in domestic and cross-border "card present" (at an ATM or a point of sale) fraud when the card is used in an EMV country. (The UK represents a terrific case study on EMV migration, and the fraud statistics before, during, and after are a very interesting read.) However, globally, we've also witnessed a significant increase in "card not present" fraud, such as during online purchases or mobile-device-based transactions, that isn't solved by EMV. While it clearly has a strong role to play in solving the problem of card present fraud, EMV alone won't reduce total payment card fraud, in the US or elsewhere.

Meanwhile, against the background of US EMV adoption, a payment revolution is occurring. I'm talking about the rise of contactless card payments (also known as "tap and go") and contactless mobile payments via mobile devices. Both are about as customer friendly and convenient as it gets, so it's no surprise they're among the fastest-growing payment methods.

However, these technologies bring their own security problems. For example, contactless technology (typically based on the ISO 14443 standard) introduces increased fraud risk, because no PIN or signature is required.

Fortunately, the EMV standard has evolved to include specifications for contactless and mobile payments. In addition to the standard EMV security model, the EMV contactless security model incorporates an extra digital certificate for signing contactless data and an extra master key to encrypt the cardholder's transmitted data.

EMV is not a prerequisite for secure contactless card payments. However, there's no reason it can't be combined with emerging security technologies to address the fraud issue, thereby enabling secure contactless card and mobile transactions. That could spell profit -- today, contactless card use tends to be limited to low-value transactions.

Fraud protection layers

Retailers need a multi-layered defense system that includes not only conventional data security mechanisms but also novel ways to authenticate users. That's so regardless of which channel or protocol they choose: EMV, RFID, NFC, or any other technology.

One possible approach to this authentication challenge that is already being adopted involves invisible, real-time, multilayer authentication systems featuring voice biometrics and/or location proximity (proximity correlation) technology.

It may seem like science fiction, but financial firms, including Wells Fargo, US Bank, and Barclays, use a customer's voice to authenticate transactions, as opposed to forcing them to type passwords on small screens. It's a natural as people become accustomed to interacting with mobile devices verbally.

Proximity correlation involves knowing that two elements are close to each other (in proximity) but with no detail shared as to *where* the party actually is, so privacy concerns are alleviated. This is very different from geolocation, where there's absolute clarity on where the party to a transaction actually is. Companies such as FICO and the Mastercard/Syniverse partnership have recently announced proximity capabilities.

Today, we're forcing a choice between security and convenience. But it doesn't have to be this way. The combination of a contactlesspayment card or smartphone and voice biometrics or proximity correlation provides convenience *and* security.

EMV is not a prerequisite -- these technologies are here today and could virtually eliminate fraud and false positives. Neither are they mutually exclusive. In fact, they're highly complementary. Proximity correlation can address those fraud situations not covered by EMV, such as stolen card + PIN, or stolen card + forged signature. Best of all, both voice biometrics and proximity correlation work as well, if not better, for mobile payments as they do for payment cards, so investments are forward looking and protected. EMV can follow in due course, and the savings to the industry over the next 2-3 years might just pay for the investment needed for EMV.

Pat Carroll is the executive chairman and founder of ValidSoft, a global supplier of cybersecurity and transaction authentication solutions utilized by banks, financial services companies, and governments to secure and authorize payment transactions. He has more than 25 years ... View Full Bio

Comment | Email This | Print | RSS

More Insights

Webcasts

Performance from the User’s Perspective
App Ratings: How to Drive Them Up
More Webcasts

White Papers

Why Passwords Aren't Strong Enough - Making the Case for Strong Authentication
The Industrialization of Fraud
More White Papers

Reports

IBM System Storage Interactive Product Guide: Intelligent, efficient and automated storage for your IT infrastructure
Skirting the Big Data Expertise Shortage
More Reports

Comments

Newest First | Oldest First | Threaded View

aaronAshfield,
User Rank: Apprentice
3/18/2014 | 11:27:17 PM

Login
50%50%

Re: The Tipping Point

SecureAccessTechnologies.com provides transaction authentication as well as application security with vocie auth, proximity, geo-fencing and a lot more. They also have step up auth and continuous authentication. 20+ patents issued.

Reply | Post Message | Messages List | Start a Board

kgordon597,
User Rank: Apprentice
3/18/2014 | 2:05:33 PM

Login
50%50%

The Tipping Point

As expected, this was great addition to yesterday's column. Media focused around the data breaches has convinced the average Joe of the needed changes in card security protocols and portrayed EMV as an inevitable fraud solution. Your content today, however, is the marketing message that needs to be conveyed to consumers. A complete leap-frog of EMV implementation is not likely, but at the very least, contactless technology can run beside it (and over time EMV can be retired alongside Windows 95 and cassette tapes). As mentioned, setting up multi-layer fraud protection with biometrics and proximity correlation will eventually cause a tipping point without sacrificing convenience for security.

Reply | Post Message | Messages List | Start a Board

Infographics

SECURITY
JOB #1 FOR FEDS
NIST plans to release in February 2014 a cyber-security framework to prioritize actions and align policy, business, and technology efforts to manage risk.
NIST

Security Job #1 For Feds

The 2014 InformationWeek Government IT Priorities Survey shows federal IT pros care about security - it's rated as very important by 69% of respondents, 30 percentage points ahead of the No. 2 priority, disaster recovery. Will the upcoming NIST cyber-security framework help manage risk?

2 comments | Read | Post a Comment

More Infographics

Subscribe to Newsletters

Live Events Webinars

Enterprise Connect Lync Tour

Check out the Applications Track at Interop Las Vegas, March 31-April 4, 2014

Software-Defined Networking & Network Virtualization

UBM Tech

More UBM Tech Live Events