mobile payments today
technology, trends & insights

The ever changing challenge of payments fraud detection

By Mike Lemanski, principal technical writer - security, Samsung Research America

Call it a case of good news masking bad. According to the 2019 Identity Study from Javelin Strategy & Research, credit card fraud dropped by nearly 25% in 2018, or $6.4 billion, compared to $8.1 billion in 2017. The bad news reflects rapidly changing tactics among cybercriminals — and threatens to make payment fraud detection harder than ever before.

That's because as defenses against card-not-present have hardened, fraudsters have begun shifting their focus to account takeover (ATO) and new account fraud, which are far more threatening — and much harder to detect. CNP losses remain unacceptably high and ATO losses are actually down, from $5.2 billion to $4 billion.

But that's still three times higher than 2016. And when you factor in a $400 million increase in new account fraud in just 12 months time, to at least $3.4 billion, you're talking about total fraud losses approaching $15 billion annually in the U.S. alone. But what's driving these shifts? And what can merchants, issuing banks, and other payment processors do to protect themselves and their customers?

ATO and New Account Fraud

According to Javelin, existing account takeover fraud, in which a criminal hacks into a victim's account to place purchases and change contact information so thefts go unnoticed, tripled in 2018 to 1.5% of all U.S.-based consumers.

Instead of merely placing purchases until a credit card is maxed out, ATOs enable thieves to drain checking, savings, or retirement accounts. Thanks to beefed up bank security controls, merchant cards and pre-paid credit cards accounts are increasingly popular alternatives for fraudsters. After cutting their teeth on bank rewards programs, fraudsters have also branched out into travel rewards programs.

In new account fraud, cybercriminals use manufactured, "synthetic identities" to take out mortgages, car or student loans, merchant lines of credit, new credit cards and more—with no intention of repaying them. Javelin estimates fraudsters get away with an average of $15,000 per attack. But one fraud ring successfully stole $200 million by acquiring 25,000 credit cards using 7,000 false identities.

Crimes perpetrated from compromised or fraudulently-created accounts are enormously difficult to detect, primarily because for all intents and purposes, their transactions are trusted, the motivation behind them assumed legit.

Group effort

Payment fraud detection systems must look beyond static identity data in order to make better informed risk decisions. Look for more adroit issuers and merchants to turn to digital identity solutions that enable them to connect the dots between users, their historical behaviors, their devices, and their accounts in order to detect anomalies that may signal fraudulent identities and risky transactions.

Some organizations will gravitate toward region or industry-specific consortiums and other options that grant them shared, global, and anonymized identity intelligence combined with behavioral and device biometrics so they can instantly recognize legitimate customers while blocking out those wielding stolen identity information. This concept of consortium is particularly helpful in pinpointing and stopping money mule activity. Traditional approaches often fail to create the linkages between separate accounts and identities, which may be part of a complex network of mules.

The bottom line

In a constantly evolving, hyper-competitive environment where growing transaction volumes could easily top $520 billion in sales in just the U.S. this year, and up to $3 trillion worldwide, it's imperative for payment providers to find ways to help their merchants accept more orders, reduce chargebacks, and attract loyal customers. It's a tall order, but the online payment fraud detection systems they deploy had better be up to the challenge.

Cover photo: iStock

Topics: Mobile Payments, Security