

Why Apple Pay Is Our Best Hope To Stop Online Fraud

Heists used to be so much effort — you'd need a gang, machine guns, a getaway car and long, meticulous planning. Nowadays, all you need is a couch, a laptop and some stolen data. When the barrier to entry is so low, it's no surprise that online fraud is a huge problem. In fact, according to the authoritative annual True Cost of Fraud report from LexisNexis/Javelin Group, fraud losses as a percentage of revenue for retailers grew to 1.32 percent in 2015, nearly doubling from 2014.

To make matters worse, the past year has been a perfect storm for online criminals, which will sharply escalate the rate of e-commerce fraud in the coming years. Hacks of T-Mobile/Experian, Ashley Madison, Chase, Anthem Blue Cross, OPM and many more released huge amounts of sensitive personal data like names, addresses, email addresses, phone numbers and social security numbers onto the dark web.

These PII (personally identifiable information) leaks were compounded by payment data leaks: millions of credit card numbers released in the Target and Home Depot hacks, plus other data raids. Together, fraudsters have more than enough material to paint a full picture of an individual's financial identity, enabling them to apply for loans, lines of credits and other financial products, as well as order goods online, fraudulently, in someone else's name.

With all these hacks, it makes sense that financial institutions are bolstering security. The EMV deadline is just that — now that the deadline has passed, brick-and-mortar retailers must have chip-enabled point-of-sale terminals, or be held liable for any fraudulent transactions that happen in their stores. The U.S. EMV liability shift is being hailed as a firewall against fraud; in reality, it's nothing more than a half-measure taken by credit card companies and banks to protect themselves while leaving retailers holding the bag.

Banks have no incentive to change the status quo for online transactions, as retailers are responsible for any fraud that happens there.

First, most point-of-sale terminals will require chip-and-signature, which is far less secure than chip-and-pin — a security shortcut chosen by the financial industry. And second, EMV will not fix the big growth area in fraud: the Internet. Past switches to EMV in countries like Australia and the U.K. show that fraud will simply migrate online as criminals look to exploit the next weakest target — sending a tidal wave of criminals straight toward unprepared online merchants.

When taken together, the situation for businesses looks bleak. To mitigate losses due to fraud over the long term, merchants and consumers alike need to move en masse to next-generation tokenized payment systems — which, like two-factor authentication to protect passwords, adds an extra barrier to the payment process, keeping sensitive data out of merchants' fragile systems and safe from hackers.

And these payment systems haven't been doing too well. Despite big promotion, use of Apple Pay is very low — a recent survey from the Aite Group found that it accounts for just 1 percent of all U.S. retail transactions. That's still far above Android Pay (the product formerly known as "Google Wallet," and now on its umpteenth rebranding) and Samsung Pay, which only launched recently.

This begs the question: What will it take to bring Apple Pay (or a similarly secure solution) mainstream, and save online merchants and banks from huge losses due to fraud?

From TechCrunch, Posted Oct 27, 2015 by Pat Phelan (@patphelan)