State of Card Fraud: 2017

What you need to know about the State of Fraud in 2017, including EMV updates, ongoing threats and how it's impacting financial institutions.

Rippleshot
stopping fraud at the speed of data

State of Card Fraud: 2017
Inside The Report

Introduction: The Good, The Bad, The Ugly

There's a harsh reality issuers have to face in 2017. **Chip readers and EMV aren't fully protecting them from credit card fraud.** Research from Javelin Strategy & Research showed that in 2016, **card fraud totaled $700 million** more in losses than the year prior. The number of fraud victims in the U.S. grew by more than two million people in 2016 (to 15.4 million), which accounted for $16 billion in fraud losses.

While the U.S. is certainly not alone in this problem, nearly 50% of all the credit card fraud around the world occurs in the U.S., despite the fact that the U.S. accounts for only about a quarter of the global card volume.

The good?

EMV had reduced brick-and-mortar fraud. According to Visa, merchants that are using chip-enabled cards have seen a **52 percent decrease in fraud**.

The bad?

CP fraud is shifting online, and fraudsters are getting smarter. Online (CNP) fraud has seen a **40 percent increase** following the EMV shift.

The ugly?

According to a Nilson report, plastic card fraud is expected to grow to **$31.67 billion in 2020**. That's a 42 percent increase.

In 2016, the FTC reported credit **card fraud doubled to more than 32 percent** in just a year's time. By all estimates, those numbers are projected to get worse before they get better.

EMV Adoption Update: New Data

Data from the Nilson Report shows card issuers were bearing 72% share of fraudulent losses in 2015; merchants and ATM acquirers assumed the other 28% of liability. In 2017, EMV changes may be shifting that liability, but card fraud is still happening.

57% → Data from the across the industry indicates that just over half (57 percent) of U.S. merchants are EMV-equipped to accept chip cards.

675M → Data from EMVCo reports there were 675 million EMV cards in circulation in the U.S. at the end of 2016.

85% → Industry estimates indicate 85% of U.S. cards in circulation are EMV-equipped (but acceptance is another issue, as noted above).

45-50% → Data from the U.S. Payments Forum indicates 45-50 percent of U.S. credit and debit transactions are made with EMV chip cards.

Some of the gains in fraud reduction has been offset with the cost of reissuance with EMV cards more expensive to reissue. This has led issuers to spend thousands more per month reissuing cards.

Data Breach Updates: A 5-Year Snapshot

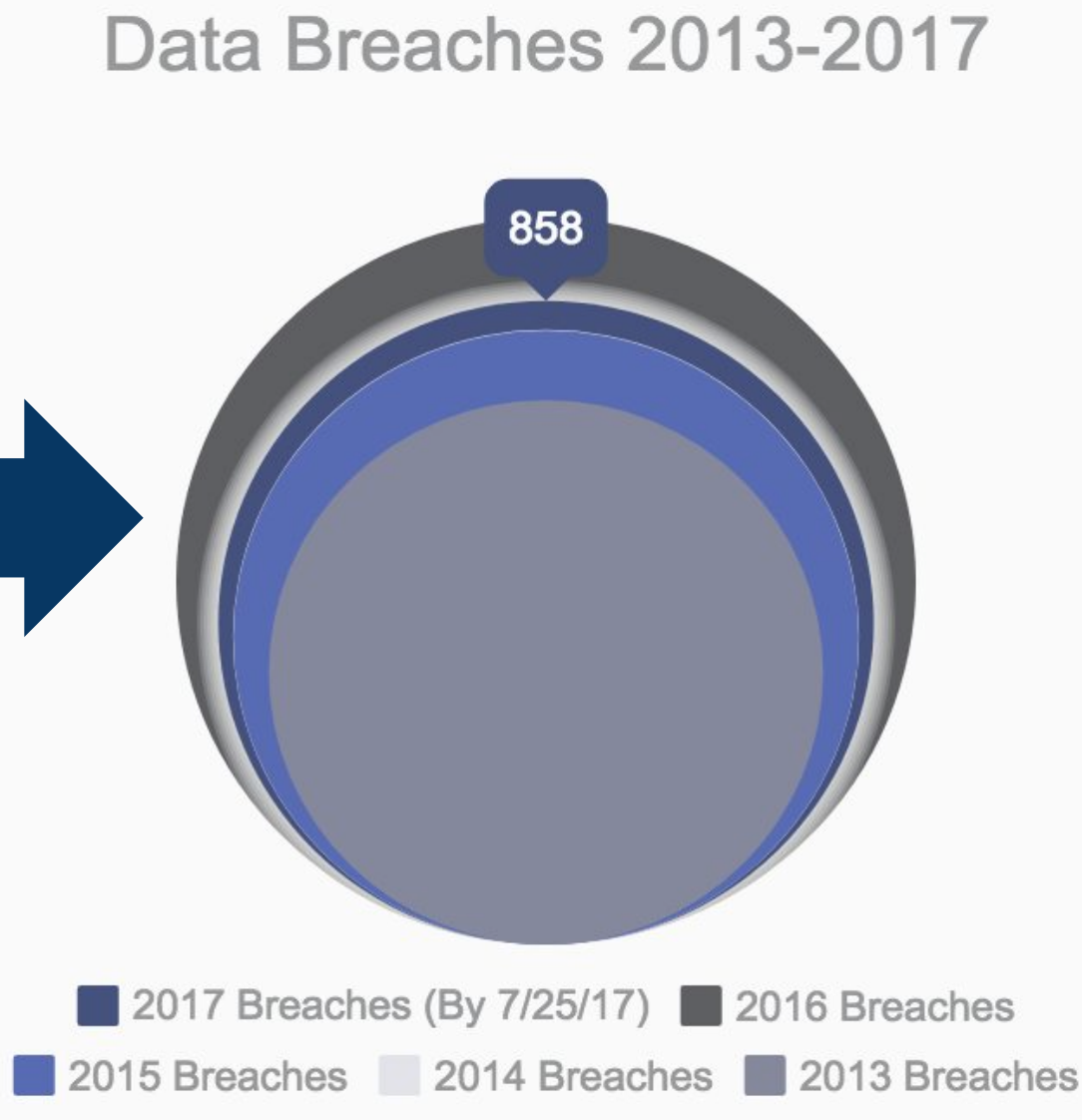
New data from the Identity Theft Resource Center (ITRC) and CyberScout indicates as of July 25, 2017, the U.S. has seen a record high of 858 breaches (roughly a 30% YOY increase).

The ITRC projects breaches to hit 1,500 in 2017 (37% YOY increase).

That's more than 2013 and 2014's data breach figures combined.

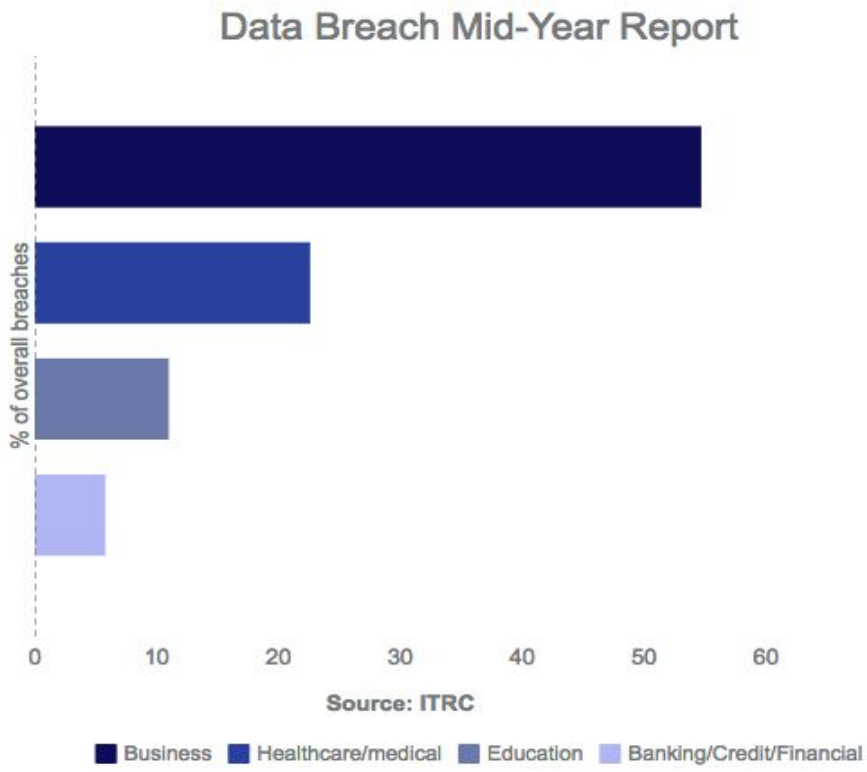
Card issuer losses occur primarily at the point of sale from counterfeit cards.

Merchant losses occur mainly on CNP when customers buy online or pick up in a store.



Data Breach Impact: Across The Marketplace

Despite technology advancements and greater adoption in EMV, major data breaches continue unabated across the payments industry — touching every sector at an alarming rate.



Major Data Breaches Making Headlines In 2017

- **HOSPITALITY | SABRE**: Trump Hotels, Four Seasons, Loews and Hard Rock hotel have all been involved in the hotel booking service breach, meaning the impact could be hundreds of thousands of customers.
- **RESTAURANTS | Wendy's:** This multi-year breach involved at least 1,025 Wendy's locations , which were hit by a malware-driven credit card breach.
- **RETAIL | Neiman Marcus**: Neiman Marcus agreed to pay $1.6 million as part of a settlement stemming from consumer class action lawsuit from a 2013 data breach. It's estimated that 350K customers were impacted in this breach.
- **INSURANCE | Anthem:** Anthem agreed to pay $115 million as part of a class-action lawsuit from a 2015 data breach involving personal data of roughly 80 million people.

Emerging Fraud Trends: What to Look For

Fraudsters are getting more sophisticated with their techniques, using bigger data sets and gaining access to far more than just social security numbers, emails, addresses and birthdates. Payment credentials are getting increasingly tangled in this fast-growing problem as more vulnerabilities are exposed across the ecosystem (as new technologies enter the market).

$35B

EMV Isn't Slowing Fraud Overall

Despite EMV, card fraud losses top $16B annually, and is expected to grow to $35B by 2020.

+33%

Online Fraud Has Ballooned

E-Commerce Fraud increased 33% in 2016, and is projected to continue to rise. Trends will continue as banks test mobile payments, faster payments, same day ACH.

+70%

ATM Fraud Is On The Rise

FICO data showed card skimming losses rose 70% between 2015 and 2016. That's on top of the 546% increase seen in 2015.

+30%

Restaurant and Merchants' ATM Prone For Hacks

FICO data also showed that ATMs and POS terminals used by restaurant and merchants saw a 30% rise in hacks.

+80%

Synthetic Fraud Is A Growing Trend

Synthetic ID fraud accounts for 80% of all credit card fraud losses, and nearly one-fifth of credit card charge-offs.

$11.8B

Friendly Fraud Has Gone Up

Friendly fraud (false claims of unauthorized purchases and misdirected claims) account for $11.8 billion lost per year.

Rippleshot Insider Insights: Getting Ahead

Fraudsters are more sophisticated than ever. Banks are using new tools to fight fraud — machine learning, automation, cloud technology, etc. — but so are the fraudsters. Only better and faster. The monetization of compromised cards has become a sophisticated industry.

From advanced techniques, bots that make online fraudulent purchases to hacking payment systems, the packaging and auctioning of compromised cards across the dark web to commit and monetize card fraud occurs faster than a bank can detect a compromise, identify compromise cards, reissue the cards and call the cardholders.

Getting Ahead Of Fraudsters

Fraud tools today shouldn't take 90 days to implement, require complicated platforms, have integration delays with core systems or complex modeling iterations. Solutions need to be fast, efficient, and actionable before the "horses are out of the barn."

Banks need tools that give them a quick alert on which cards are compromised on a daily basis, the ability to detect skimmers on ATMs in two hours, and the option to reset PINs immediately — opposed to the two week-period associated with CAMS alerts.

Fraudulent purchases using bots have seen a 234% increase; ATM data breaches rose 546% in a one-year time span.

By the time networks alert banks which cards are comprised:

- 80% of fraud has already occurred.
- Number of cards compromised has increased from 3 to 3.7

Machine Learning & Card Fraud Management

Machine learning holds the promise to help many industries in myriads of ways — from customer interactions (Alexa, Siri), revenue generation, to self-driving cars. Machine learning can also be used to help banks and credit unions manage and reduce card fraud. The issue is not the technology's effectiveness (i.e. - seeing patterns in millions of data point and hundreds of variables faster and more accurately than human beings). The real issue is about the realities of implementing such a solution at most banks. Many may not have in-house data scientists to create models, the IT resources to get the data from their internal systems or from their processors, and the expertise to insure that the data is clean and correct.

Key Data Point

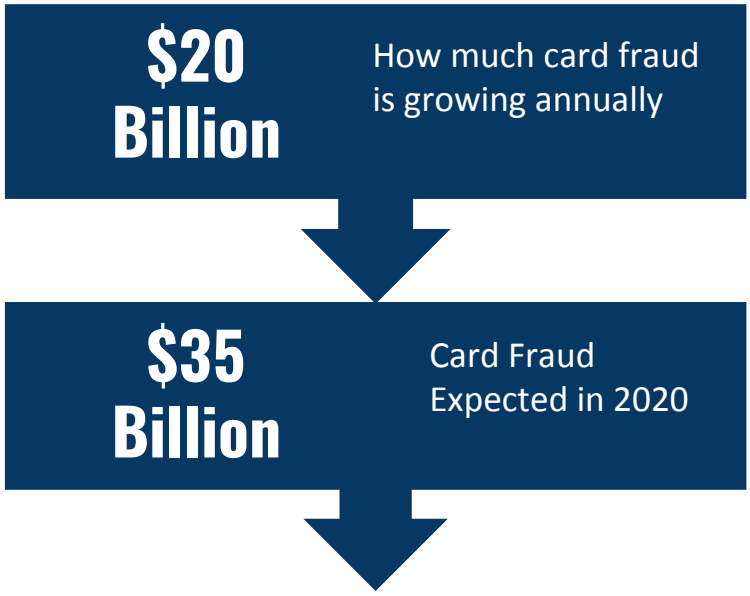
Rippleshot's team discovered that over 60 percent of fraud that's not being caught was correlated to data breaches.

The promise of Machine Learning can fall short usually for one of the three reasons above. Solution providers who want to bring the value of machine learning to banks to help detect ATM breaches, thwart compromised cards, and reduce fraud need to be able to deliver a streamlined solution that takes days (not months) to implement, that does not burden a bank's overloaded IT department, and delivers results in hours (not days or months).

Solutions need to be able to streamline the data feed process, automate the analytics process, offer continuous model refresh, and deliver actionable results within hours — and continue to do so on a daily basis. Successful machine learning solutions for banks and credit unions automates the tasks of gathering and checking data, detecting fraud, and validating the results. This frees managers to make strategic decisions, as opposed to getting mired in the mechanics of machine learning. Successful machine learning solutions also reduces the time from detection of fraud, or of compromised cards, to action to reduce as much fraud as possible from compromised cards/accounts, skimmed ATMs, etc.

With the industry moving toward faster payments (same-day ACH, two-day settlement, etc.), fraud also occurs at the speed of data. Deployed properly, machine learning that continuously sifts through millions of transactions and variables to deliver timely results can help banks and credit unions better and more cost-effectively address the growing card fraud problem.

Conclusion: What's Next?



Banks and credit unions are faced with many challenges today in a financial ecosystem filled with more wide-reaching breaches and increasingly sophisticated hackers.

As financial institutions continue down their digitization transformation — and invest in innovative technology — this opens the floodgates for more touch points for fraudsters to breach, particularly as it relates to card fraud.

Card fraud and data breaches are rising at alarming rates, causing issuers to spend thousands each month reissuing cards, investing in new fraud prevention tools and combating new marketplace threats.

With more sophisticated tools at their disposal, fraudsters are evolving as fast, if not faster than banks, credit unions and payment networks.

Thanks to machine learning, the digitization of data and artificial intelligence, banks and credit unions have access to the infrastructure and tools necessary to fight fraud — if they're willing to invest money where it counts.

Regardless of new innovations to the marketplace, it will take time to build that infrastructure and learn those new skills – which means card fraud will continue to get worse before it gets better. However, proactive organizations that have invested in people, the power of big data, and technology like machine learning can achieve dramatic success in reducing fraud.