
# State of Card Fraud: 2016

What you need to know about the State of Fraud in 2016 and its impact on consumers, retailers, and financial institutions

Powered By rippleshot

# Table of Contents











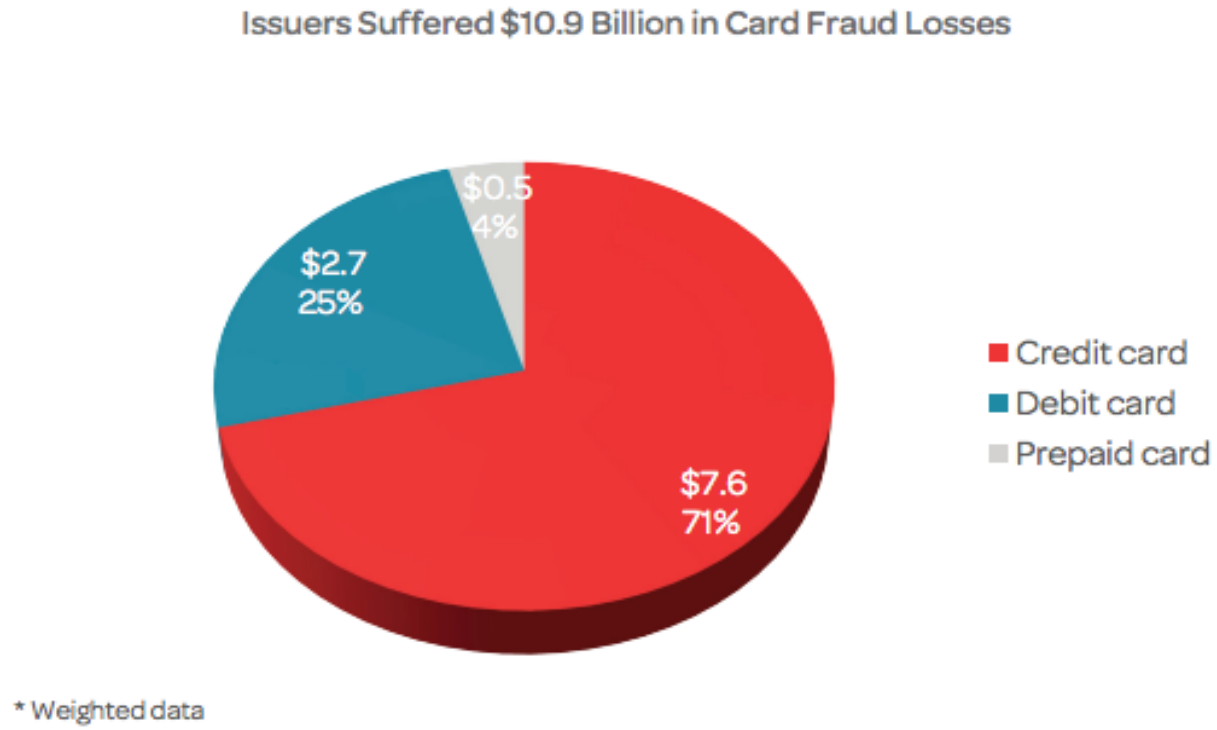


# Issuer Losses

A study recently conducted by LexisNexis and Javelin Research found that **card issuers are directly losing $10.9 billion to card fraud annually**. After surveying 100 risk and fraud decision-makers working at issuing institutions, the report concluded that current fraud schemes employed were spread almost equally across the spectrum, with lost/stolen cards being the largest source of fraud at 28%, and application fraud and account takeover falling closely behind at 20%.

# Issuer Losses

Out of the $10.9 billion in total losses, the vast majority came from credit cards (71%), an intuitive conclusion considering the appeal of credit limits to cybercriminals in comparison with dollars available in a deposit account. Debit card fraud losses claimed another 25% at $2.7 billion, and then prepaid cards with 4%, or $500 million.




With these numbers in mind, it is no surprise that credit cards were reported to have the highest losses on a per card in circulation basis at $9.00, meaning that for every single credit card in an issuer's portfolio, fraudsters are skimming $9.00 off the top. Losses on prepaid amounted to approximately $4.70 per card, and $2.80 per card for debit.

# An Update on EMV Implementation

***"Based on what we've seen in other regions that have migrated to EMV at in-store point-of-sale, fraud moves to other channels"***

*- Alisa Ellis, Vice President of Global Products & Solutions at Discover*

EMV implementation has become one of the most anticipated events in the U.S. payment security industry, and rightly so, as it has many positive and negative connotations for the entire spectrum of card issuers, merchants, and consumers. Although 76% of issuers believe that EMV will reduce losses from fraud for point-of-sale (POS) transactions at brick-and-mortar stores, 62% agreed that fraud would shift to account takeovers, application fraud, counterfeiting cards, and card not present (CNP) environments.

This prediction stems from past experiences in international markets such as the U.K. and Canada, where card fraud shifted similarly to the effect of squeezing a balloon - migrating from card present (CP) to CNP. As historical patterns suggest, cybercriminals are quick to transition to areas where fraud mitigation technology is not up-to-date, and with the EMV roll-out, this will translate into fraud moving towards small businesses who have not yet transitioned to EMV, and gas stations/ATMs where EMV compliance is not federally mandated.

# An Update on EMV Implementation

Throughout 2016, the accelerated pace of EMV compliance imposed on U.S. merchants has led to multiple retailer lawsuits against issuing institutions and card networks.

Some recent developments include:

- Home Depot sued Mastercard and Visa, accusing both payment networks of conspiring to prevent adoption of more secure technology in order to maintain market dominance and profits (using signatures instead of PINs)
- Walmart sued Visa for similar reasons, claiming that Visa demanded that they use "fraud prone" verification, signatures instead of PINS, because Visa stands to make more money processing
- Two Florida retailers, B&R Supermarket Inc and Grove Liquors LLC, filed a federal anti-trust lawsuit against seven payment networks, ten financial institutions, and EMVCo., claiming that the defendants conspired together to create a liability-shift date they knew retailers could not meet

# Where are the data breaches happening?

When it comes to data breach news, it's easy to get caught up in the headlines, especially when stories of large-scale breaches of cardholder information seem to graze the front of newspapers on a weekly basis. However, even though the Targets, Home Depots, Michaels and Wendy's are all-encompassing as far as the media goes, they're actually not the majority of the card compromises that take place - not by a long shot.

## Why Aren't These Being Caught?

Simply, there are not enough resources to be dedicated to investigating tens of thousands of small business data breaches. VISA's own breach response guide says their typical threshold involves looking for the same incident **to be reported by at least four financial institutions with at least 999 affected accounts** before they confirm that a breach has taken place.

"VISA's own breach response guide says their typical threshold involves looking for the same incident **to be reported by at least four financial institutions with at least 999 affected accounts** before they confirm that a breach has taken place."

# Where are the data breaches happening?

## Death by a Thousand Paper Cuts

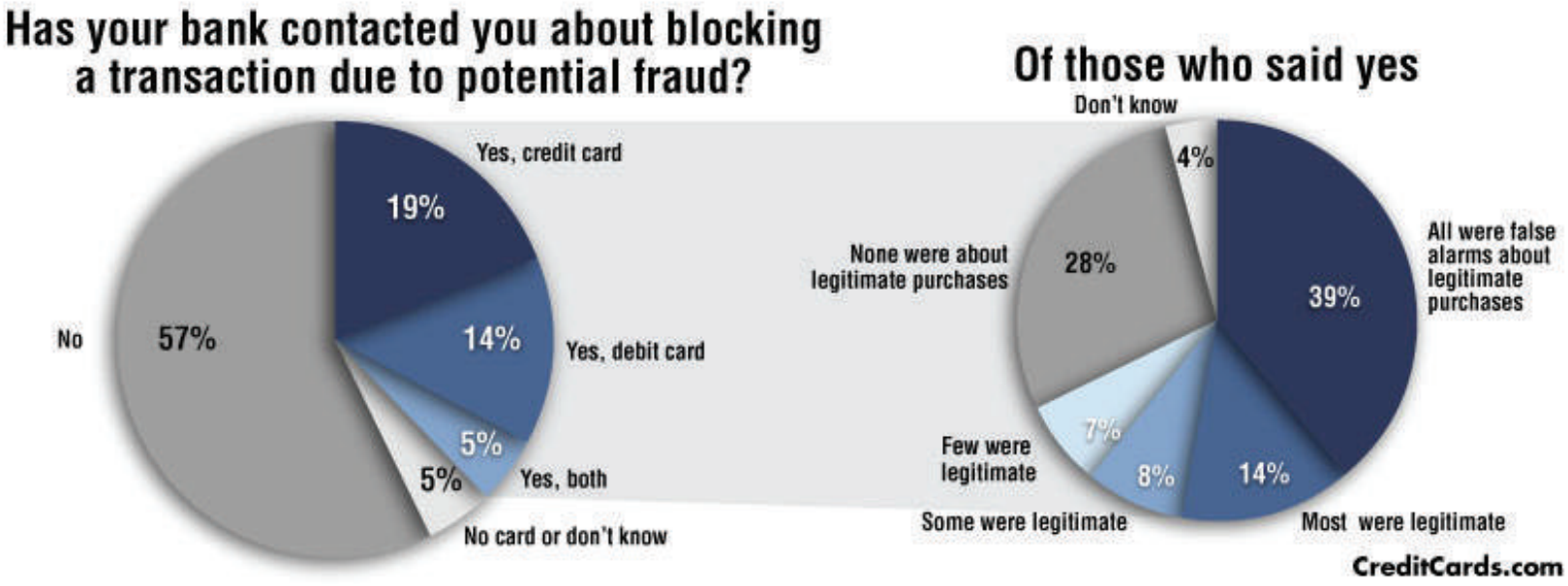
**371 DAYS**
**Longest undetected data breach in 2015**

**83 DAYS**
**Average length of a data breach**

For financial institutions in smaller communities, with more modestly sized cardholder bases, the math on many of these small businesses compromises never quite adds up to card network intervention. There have been reports from banks and credit unions claiming that the card networks don't even start to look at a potential compromise **until they amass 60,000 notifications from their issuers,** explaining why these breaches are going so long undetected.

Of all the compromises Rippleshot detected in 2015, the **longest was 371 days**, but the average was still higher than expected at 83 days. Skimming devices often have very short (12-36 hour) stints on ATMs or gas pumps, so what's driving up the average? It's the malware-type attacks that were responsible for Target and Home Depot, among many others, that are going months without being detected.

# Why False Positives are a Hot Topic

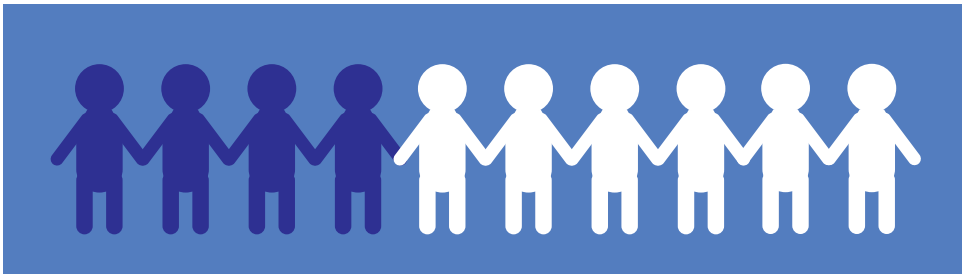



As losses from fraud continue to rise exponentially, financial institutions are struggling to bear the burden. Instead of investing in fraud detection technologies, many banks are turning to more aggressive methods to reduce losses, such as implementing tougher fraud prevention measures. Although this strategy helps mitigate fraud, the higher thresholds have caused many genuine transactions to be mistakenly flagged as fraudulent, turning away loyal customers. These “false alarms”, or false positives, occur when transactions meet a minimum number of criteria determined by financial institutions, and can be incredibly frustrating to the cardholder.

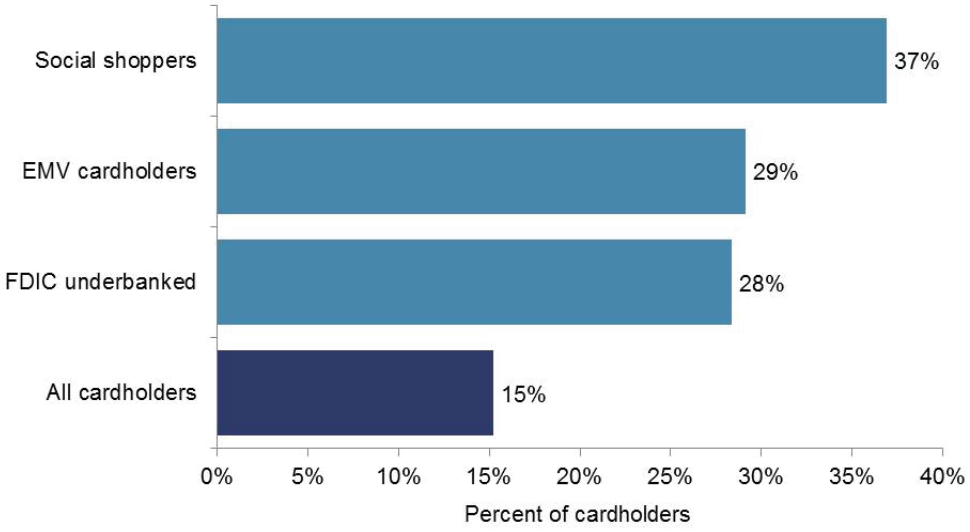
# Why False Positives are a Hot Topic

*"Issuers must invest in high-quality authorization solutions and strategies to improve card authorization practices. Failing to live up to cardholder standards may encourage customers to, at best, decrease their card usage or, at worst, to stop their use of the card entirely"*

*- Al Pascual, Director of Fraud and Security at Javelin*



**Nearly 4 in 10 (39%) declined cardholders report that they abandoned their card after being falsely declined.**






**15% of all cardholders have experienced a false decline in the past year**

# Regulation

To complicate matters further, regulatory institutions such as the FFIEC, CFPB, and FTC are getting more involved with fraud mitigation and cyber security.

## FFIEC

It's been a year since the Federal Financial Institutions Examinations Council (FFIEC) debuted the Cybersecurity Assessment Tool, commonly known in the industry as the CAT, a standard federal assessment that consists of two primary parts:

**1)** The Risk Profile Assessment, a series of questions that financial institutions must answer about their internal operations. The responses are scored and an inherent risk profile is determined - from least to most

**2)** The Cybersecurity Maturity Guidelines - A set of cybersecurity recommendations, laid out by risk profile, that escalate in terms of requirements as the risk profile increases

Although the CAT was initially presented as a voluntary assessment, it has been criticized by banks and credit unions for being "basically required" by examiners. Panelists of ABA's Risk Management Conference last year stressed the importance of passing along CAT guidelines to vendors and other third party service providers, citing how suppliers are notoriously behind financial institutions on security and compliance.

# Regulation

## CFPB

In addition to the FFIEC's regulations, earlier in March, the Consumer Financial Protection Bureau (CFPB) took legal action against Dwolla, a payment platform, costing them $100,000 in penalties and an order to fix any security weaknesses in their systems, put in place and train employees on comprehensive data security policies, and perform consistent risk assessments.

This is the first foray the CFPB has made into the data security space, putting the industry on edge. This decision puts the focus back on how organizations with access to consumer data are ensuring its security, and also highlights the broad reach given to the CFPB as defined by the Dodd-Frank act.

The Dodd-Frank Act states CFPB's jurisdiction as follows: "The CFPB has authority to regulate any person who engages in offering or providing a 'consumer financial product or service,' or any affiliate service provider of such a person.

# Regulation

## FTC

Finally, the end of last year saw Wyndham Hotels and Resorts dodge a major bullet by the Federal Trade Commission (FTC). The controversy can be traced back to 2012, when the FTC filed a lawsuit against Wyndham for three breaches that occurred during 2008 and 2009, exposing credit and debit card information for over 619,000 customers.

In December 2015, Wyndham settled the lawsuit by agreeing to "establish a comprehensive information security program designed to protect cardholder data - including payment card numbers, names and expiration dates. In addition, the company is required to conduct annual information security audits and maintain safeguards in connections to its franchisees' servers." This translated into a big win for the FTC, as the court case will serve as a precedent to establish a federal standard for data protection that governs non-banks.

# Legislation

Yet another variable that is compounding the state of confusion is pending legislation surrounding data security in Congress. The Data Security Act of 2015, a bipartisan bill introduced to Congress as H.R. 2205 on May 1st, 2015 outlines two purposes: “to establish strong and uniform national data security and breach notification standards for electronic data” and “to expressly preempt any related State laws in order to provide the Federal Trade commission with authority to enforce such standards for entities covered under this Act.”

# Legislation

## An Overview of the Bill

The bill requires individuals, merchants, and other non-government entities that handle sensitive financial account information to implement an information security program and notify consumers, federal law enforcement, payment card networks, and consumer reporting agencies of data breaches containing unencrypted sensitive information.

Other salient provisions include:

- Directing entities to require third-party service providers (generally point-of-sale) by contract to implement appropriate safeguards

- Allowing financial institutions to disclose information with account holders regarding breaches

- Expanding compliance procedures for financial institutions under the Gramm-Leach-Bliley-Act (GLBA) to businesses and retailers.

As highlighted in the GLBA, financial institutions have faced stringent compliance procedures in order to protect confidential information since 1999, so the argument is- why shouldn't merchants?

# Legislation

## Establishing a National Standard for Banks and Merchants

Proponents of the bill argue that despite the exponentially growing number and sophistication of data breaches, no federal standard exists for consumer data protection at the merchant level. Currently, there are little to no regulations on data security for merchants, **allowing them to store customer transaction data without any virus or malware protection, firewalls, or data encryption**, and as a result, consumer data is left vulnerable to fraud. At the same time, banks and credit unions must bear the cost of reissuing new credit cards and reimbursing consumers when data breaches occur.

To make matters worse, financial institutions are not allowed to identify who was responsible for the breach. Effectively, this transforms banks into the culprits even when they have done nothing wrong, and provides little motivation for merchants to protect consumer data. By establishing a baseline standard for all players in the chain of commerce, supporters of the bill believe that everyone will be held accountable. Also, by dissolving the conflicting patchwork of current state laws and replacing them with a uniform federal code, consumers will avoid confusion, and companies will not struggle with compliance between states.

# Legislation

## Opposition from Merchants and Consumer Protection Agencies

On the other hand, merchants and consumer protection agencies disagree. First of all, they argue, although the necessary security procedures are scalable, costs such as onboarding and training of employees to update security standards will be difficult for smaller companies to comply with. Also, by superseding all state laws regarding data breach and notification, the Data Security Act of 2015 would suppress developing state laws that protect an individual's email accounts, cloud photo storage, geographic location, and electronic communications. Another potential flaw is that the national "harm trigger" standard for breach notifications outlined in the legislation is weaker than that of seven states and the District of Columbia, preventing the states from taking stronger measures against data breaches.

Although the bill was reported on December 9th, 2015 by the Committee of Financial Services with a majority vote of 46 to 9, it remains to be seen if the Data Security Act of 2015 will become a law.

# Conclusion

## Insights

- EMV implementation will shift the fraud landscape towards application fraud, account takeovers, counterfeiting cards, and CNP environments
- Friction between retailers, payment card networks, and issuing institutions will rise in the form of more lawsuits
- Most data breaches will continue to occur at small businesses and go unnoticed, despite the media's unrelenting attention on major retailers
- False positives will keep driving away customers, giving banks the impetus they need to invest in fraud detection solutions and strategies to improve card authorization practices
- Regulatory institutions such as the FFIEC, CFPB, and FTC will play a bigger role in fraud mitigation and cyber security
- Pending legislation will determine liability for data breaches among retailers, payment card networks, and issuing institutions.

# Conclusion

The underlying theme of card fraud in 2016 is uncertainty, which fraudsters are continuing to capitalize on. Ultimately, consumers are unaware of the battles fought in the trenches -- but they do know they are continuing to see fraud on their cards, and until significant change is made, they will continue to blame card issuers. As fraud shifts from CP to CNP, institutions that adopt fraud prevention and detection technologies will gain a competitive advantage in the marketplace.

Rippleshot is transforming the way that banks detect fraud through a cloud-based technology solution that leverages machine learning and data analytics to distinguish fraudulent activity more quickly and efficiently. Rippleshot's award-winning technology processes millions of payment card transactions to proactively pinpoint when and where a data breach occurred.

Following detection, Rippleshot provides banks with the tools they need to update fraud detection rules in order to lower their fraud losses while avoiding unnecessary card re-issuance.

rippleshot
stopping fraud at the speed of data