2016 Industry Report: False Positives and Card Reissuance

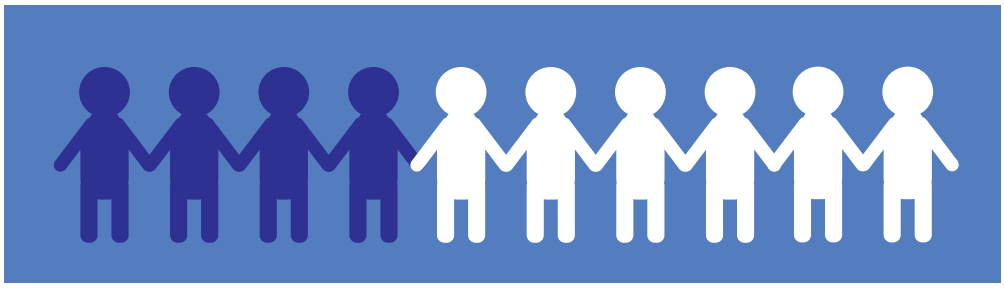
Quantifying the impact of false positives and card reissuance, from revenue losses to diminished customer loyalty

Powered By rippleshot

Table of Contents

False Positives

In a 2015 study, Javelin Strategy estimated that 15% of all cardholders had at least one transaction falsely declined in the past year, and nearly **4 in 10 (39%) declined cardholders reported that they abandoned their card** after being falsely declined.



The History of False Positives

False positives occur when transactions by cardholders are wrongly declined due to suspected fraud. In the past, traditional fraud prevention has been centered around a "better safe than sorry" or "block first, ask questions later" mentality, as banks would decline transactions with even the smallest probability for fraud. At the time, consumer behavior was widely inelastic to this method, only because these customers were accustomed to waiting thirty minutes in line to cash a check at the teller, or a week for a payment to clear.

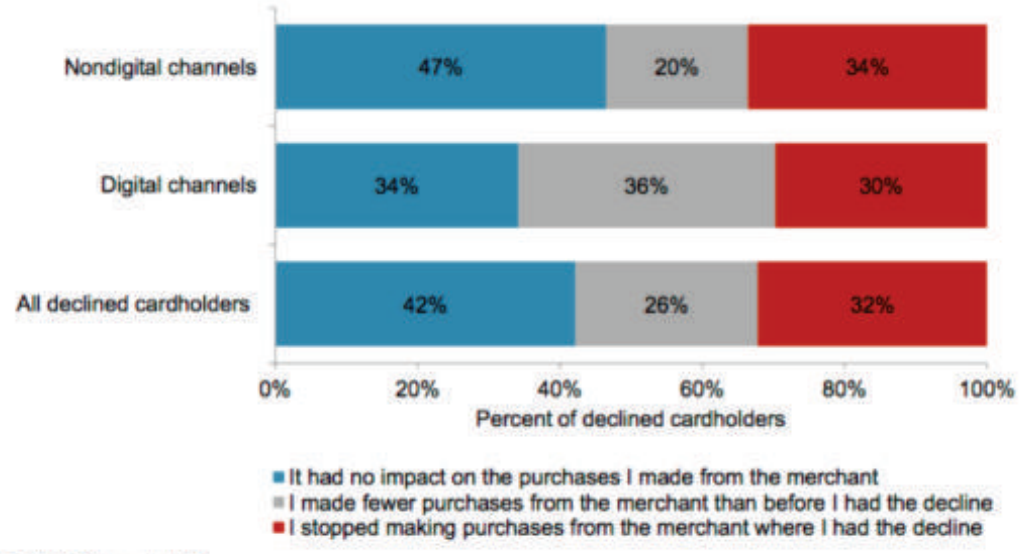
However, with the emergence of instant payments and mobile banking, this historical maxim no longer holds true. In today's world, customers find false positives to be time-consuming, annoying, and even embarrassing. Even worse, since customers are generally unaware of what is happening behind the scenes, and they largely don't care, they will likely continue to blame their bank or credit union for the issues.

The statistics only further support these claims, because as Javelin Strategy pointed out, almost 4 in 10 (39%) cardholders reported abandoning their card after being falsely declined in 2015. This statistic is quite alarming considering Aite Group estimates that **U.S. issuers will decline $264 million in legitimate transactions in 2016 alone**, a number that is projected to rise by 25%, reaching $331 million in the next two years.

Impact on Merchants

Merchants and retailers are significantly affected by false declines, as 6 in 10 consumers report either decreasing or halting card usage at the merchant altogether after a transaction decline.

Figure 3: Impact of a Declined Transaction on Card Usage



- 26% made fewer purchases from the merchant than before they were declined
- 32% stopped making purchases altogether

The Two-Front War for Issuers

"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. Cardholders expect authorization perfection from their issuers and will not stand for fraud or false positives."

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

Customer Disturbances

For many financial institutions, capturing fraud is only as important as how effectively you can do it without disturbing your customers, who are becoming hypersensitive to false declines. In fact, according to Finsphere, 48% of consumers are concerned about false declines. Eighty-two percent of cardholders who experienced a false decline felt the episode was inconvenient, embarrassing or irritating. This means that when their card goes fraudulent or is falsely declined, cardholders will choose to spend on another card, or worse, leave their bank.

The Two-Front War for Issuers

Unfortunately, customer disturbances and the long-term eroding of brand loyalty is not the only cost card issuers have to stomach. For every transaction made, issuing banks collect interchange income from the merchant's acquiring bank as a fee for providing value and benefits associated with allowing a merchant to accept electronic payments.

Although the transaction-based fee is quite small in comparison with the transaction total (ex. $0.10 + 2.00% of transaction), the income generated certainly adds up. According to the Javelin Strategy study, false positive declines totalled $118 billion in lost sales to merchants, with approximately 66% of purchases carrying $100 in value, and 40% of declines over $250. This means that card issuers lost out on, at best, $2.10 per transaction, and at worst, $5.10 per transaction, using the aforementioned sample interchange fee.

The Two-Front War for Issuers

When asked about a $100 purchase...

85% agreed that security is more important than speed

...but in the case of a $5 purchase

Only 70% agreed that security is more important than speed

A Balancing Act

Balancing added security with a frictionless user experience is a growing concern among consumers and financial institutions, and statistics show that the size of the transaction bears a heavy impact.

When asked about a $100 purchase, 85% agreed that security is more important than speed. In the case of a $5 purchase, the number dropped down to 70%, with 30% preferring speed even if it meant fewer security steps.

The Two-Front War for Issuers

Mitigating fraud and maintaining customer convenience should not be mutually exclusive. The reality is, the majority of financial institutions are constantly juggling between two equally poor options:

1) **Broad-brush, widely-blanketed decline rules that interfere with cardholder spending habits**

2) **Small-scale, ineffective, or non-existent decline rules that let fraud permeate**

However, smart financial institutions are leveraging the power of big data and machine learning to help them strike the fine balance between false positives and fraud prevention. By detecting the true (common) points of compromise, card issuers can isolate and identify card compromises exponentially faster, implement smart rule writing, and ultimately keep their cardholders satisfied - and spending.

Reactive Card Reissuance

No Longer "If", but "When"

Every year, data breaches grow in frequency and severity, with over 4.7 billion records (and counting) reported stolen or lost since 2013. This year is no different, as 2016 has been marked by large-scale data breaches grazing newspaper headlines on a weekly basis. Although all data breaches do not result in a compromise of cardholder and payment information, card data accounted for 60% of all data compromised in 2015.

When a payment card data breach is disclosed, unprepared card issuers face a formidable challenge and limited array of choices: wait until a hacker attempts to use the card to transact fraudulently, scramble to implement broad-brush decline rules, or immediately cancel and reissue an entire portfolio of potentially affected cards.

Reactive Card Reissuance

As you may surmise, all three of these methods are reactive in nature, and have multiple pitfalls. Waiting until a hacker attempts to use a card fraudulently is leaving fraud to chance, as issuers are essentially gambling with cardholder security and payment data. As mentioned earlier, implementing broad-brush decline rules results in customer disturbances and lost revenue. Finally, the remaining option is immediately cancelling and reissuing an entire portfolio of potentially affected cards.“basically required” by examiners.

“It’s not a question of if — but when — your organization will experience a serious security breach. Cybercriminals are using more sophisticated and targeted attacks to steal everything from valuable intellectual property to the sensitive personal and financial information of your customers, partners, and employees. With enough time and money, they can breach the security defenses of even the largest enterprises.”

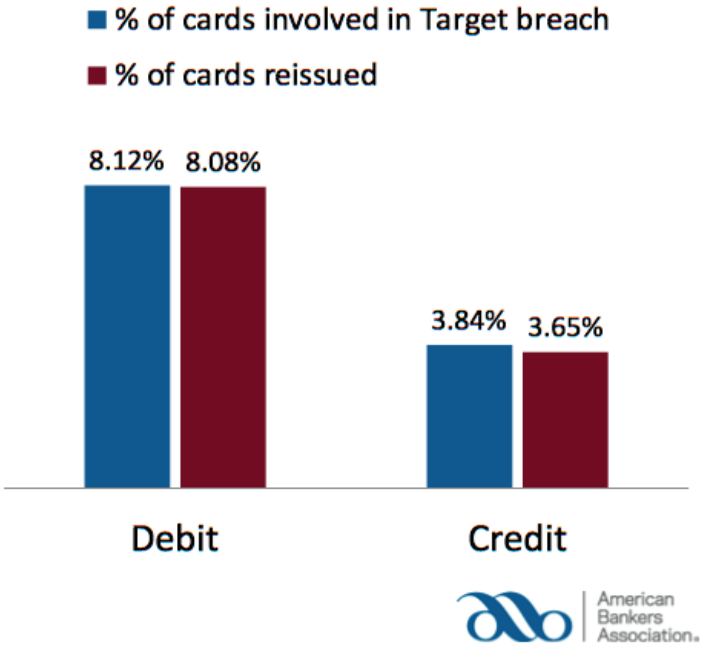
- Forrester Research

Reactive Card Reissuance

The Numbers Don't Lie

When it comes to card reissuance, the numbers don't lie. The costs of reactive card reissuance are exorbitant, and the ROI is almost non-existent. Although some of the larger issuers in the marketplace may be able to afford throwing millions of dollars at the problem in order to maintain customer satisfaction, small banks and credit unions do not have such luxury.

To understand how costly reactive card reissuance strategies can be, let us examine the aftermath of an actual payment card breach through the Target Breach Impact Survey.



The 2014 survey from the American Bankers Association revealed that 8.12% of debit cards were possibly involved in the data breach, and 8.08% of cards were re-issued, meaning that **the vast majority of cards believed to be compromised were re-issued.**

Reactive Card Reissuance

Now, compare the percentage reissued with the percentage that actually resulted in a fraud loss:

Less than .64% of debit cards actually saw fraudulent activity! In Rippleshot's experience, only 1-2% of these affected cards would have eventually gone fraudulent. This means that a whole lot of customers are getting new cards when they don't need to.

What's scary about this? Besides for the fact that the **average cost for reissuing is $9.72 per debit card**, 20% of all re-issued cards never get reactivated. This translates into millions of dollars of revenue disappearing into thin air.

Instant Card Reissuance

Instant Gratification is Not Soon Enough

When a customer has had their card lost, stolen, or breached, they are usually not happy. What makes matters worse is that they are often left walking away with a promise that their card will arrive in 7-10 business days via mail. Not only is this frustrating for the customer, it also opens the door for replacement cards to be stolen in the mail and used fraudulently. Even if the card is successfully received by the consumer, there is a chance that the customer will wait a few days before activating it, foregoing hundreds to thousands of dollars spent, or even worse- switching to a competitor's card. With instant card reissuance, the customer walks away with an activated card on the very same day.

Today, customers expect instant access to everything, including their payment cards. Banks and credit unions that can instantly reissue cards at their branches have a distinct advantage over their competition. They can utilize this opportunity to "effectively explain card features and benefits, encouraging immediate and frequent usage and cross-selling other products and services, such as online banking" according to Fiserv's report: The Role of Instant Card Issuance in Customer Satisfaction and Use.

Instant Card Reissuance

One Size does not fit All

Fiserv also noted that instant card issuance translates directly into 30% of cards being used in the first day, and 70% of those instantly issued cards being used within five days. Over a 45 day period, instant issuance cards performed 53% higher than mailed cards, a significant statistic that can be correlated to increased consumer spending, satisfaction, and brand loyalty.

$12,000- $40,000
cost of offering instant card reissuance per branch

Despite the substantial benefits, instant card reissuance comes with a price tag that is simply not feasible for most banks and credit unions. Fiserv estimates that solutions that offer in-branch issuance for ATM, debit, credit, EMV and photo cards can range from $12,000-40,000 per branch.

The Solution

False positives and card reissuance are costing more money to banks and credit unions than what meets the eye. The tangible costs vary from loss of revenue from false declines of legitimate purchases, expensive and inefficient reissuance of cards, loss of spend on reissued portfolios, and staff time spent on customer service and manual decline rules. However, the most disconcerting consequence of false positives and card reissuance is the loss of customer loyalty. C-Suite level executives understand that inconveniencing a customer through a false decline or reissued card can, at best, translate into a small loss in revenue, and at worst, turn away customers, and their lifetime customer value, forever.

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 in order to help banks lower their fraud losses, reduce customer disturbances, and avoid unnecessary card re-issuance.

rippleshot
stopping fraud at the speed of data