Overcoming False Positives:

Saving the Sale and the Customer Relationship

Sponsored by:

riskified

JAVELIN

September 2015

FORWARD

This whitepaper, sponsored by Riskified, analyzes the prevalence of false-positive declines in the U.S., explores key consumer segments disproportionately affected by incorrect declines, and presents best-practice solutions for merchants. The whitepaper was independently produced by JAVELIN.

JAVELIN maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

Merchants face a serious challenge in today’s marketplace as they try to balance the need for strong antifraud measures with consumers’ desire for fast, easy, and digital purchases. Quite often, security measures incorrectly flag legitimate transactions, which potentially alienate customers and result in reduced revenue for merchants. One in six (15%) of all legitimate cardholders experienced at least one decline because of suspected fraud in the past year, resulting in a total of $118 billion declined. Unfortunately for merchants, 26% of declined cardholders reduced their patronage of a merchant following a decline and 32% stopped shopping with the merchant entirely.

EXECUTIVE SUMMARY

The percentage of consumers affected by false-positive declines is three times greater than the percentage affected by card fraud. One in six (15%) of all cardholders has had at least one transaction declined because of suspected fraud in the past year, compared to just 4.42% of defrauded consumers. The disparity between total amount falsely declined vs. amount lost to fraud is even more drastic: In 2014, $118 billion was incorrectly declined compared to just $9 billion lost to fraud. Antifraud efforts are an important element of every merchant's business strategy, but overly restrictive or incorrect fraud measures may be equally detrimental to the bottom line.

Two-thirds of cardholders who were declined during an e-commerce or m-commerce transaction reduced or stopped their patronage of the merchant following a false-positive decline (vs. 54% for all declined cardholders). There is a growing problem as increasing sales volume, changing consumer behavior, and evolving fraud schemes have all increased the difficulty in validating legitimate shoppers from fraudsters during e-commerce and m-commerce transactions. This, coupled with the fact that merchants today are typically more liable for card-not-present (CNP) transactions, leaves many merchants on high alert for illicit transactions. But merchants cannot afford to alienate consumers purchasing through these channels and should tread carefully when considering a purchase decline.

Gen Y consumers are especially at risk for false positives, with 24% experiencing at least one declines on transactions in the past year. Younger consumers' propensity for high-risk merchants — especially e-commerce and m-commerce retailers — increases the risk of red flags and the chance for a false decline. But Gen Y consumers are also more likely to switch merchants after a decline, with 42% abandoning their merchant after their transaction did not go through. This trend is especially worrying, as Gen Y consumers represent the future powerhouse shoppers and merchants cannot afford to lose their long-term loyalty.

High-income consumers — those earning $100K or more a year — are significantly more likely to report false-positive declines on transactions over $250 (51% vs. 40% for all declined cardholders). Twenty-two percent of high-income cardholders experienced a false-positive decline over the past year, and over half (58%) reported that they either limited or stopped their patronage of the merchant following the decline. High-income consumers are a crucial shopping segment for merchants, as they have greater discretionary spending that means more revenue for merchants.

RECOMMENDATIONS

Don’t base your customer validation scheme on personally identifiable information (PII). PII includes such static data as name, address, or Social Security Number. Unfortunately, a series of recent data breaches has resulted in the proliferation of PII online, enabling fraudsters to easily obtain fake credentials. Base your authorization strategies on dynamic information, rather than static, when possible.

Move beyond knowing your customer — seek to understand them. Merchants should invest in antifraud solutions that offer multidimensional intelligence such as device identification or the user’s reputation across multiple merchants and verticals. Analyze behavior patterns of both legitimate and fraudulent transactions in order to better flag future purchases. Linking data across transactions can be useful for identifying patterns such as IP range, shipping address, payment method, etc. Detecting patterns is a useful tool to combat fraud, and additional data from external databases can provide a more detailed picture of shoppers.

Never issue a decline based on a single data point. Address verification system (AVS), distance between billing and shipping addresses, and device identification are all helpful in combating fraud, but they should not be used in isolation. Merchants should instead adopt a holistic, customized approach that attempts to understand the complete picture of the purchaser in context of the specific order.

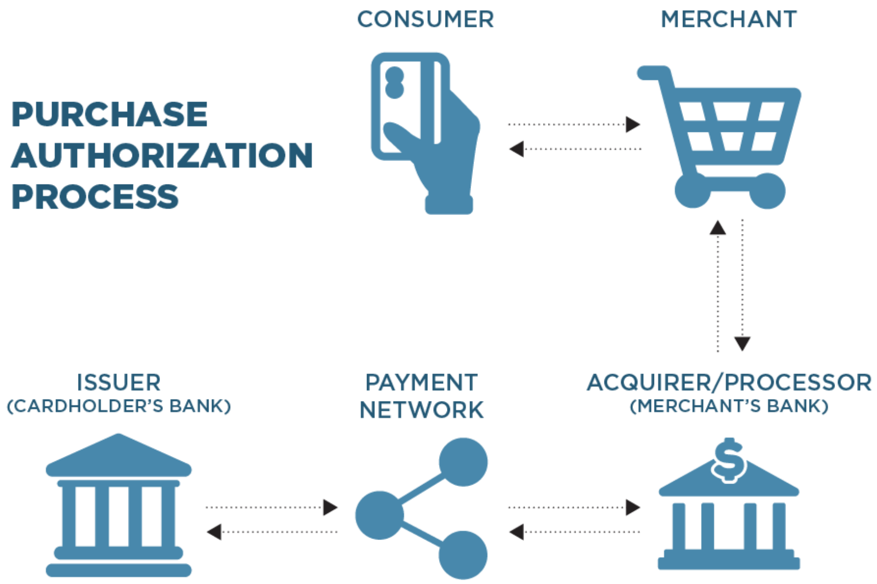
Accurate tagging is crucial for merchants who rely on machine learning or rules-based fraud systems. A rules-based system will begin to degrade if orders are simply tagged as “fraud” without additional clarification. Tags need to indicate what element of the transaction was problematic and the degree of certainty about fraud. In some cases, an order is declined because of insufficent information rather than absolute certainty of fraud. Specific tagging will help merchants gather a better idea of their decline patterns and adjust their authorization rules.

THREAT OVERVIEW: AUTHORIZING PURCHASES

Purchase authorization has grown increasingly more complicated in recent years given the growth of e-commerce and m-commerce purchases, electronic payment options, and resourceful fraudsters. When a card or other electronic transaction is made today, the card networks (Visa, MasterCard, American Express, or Discover) employ a complicated algorithm that examines hundreds of elements to produce a risk score that is shared with the issuer.[1] Issuers then rely on their unique identity authentication strategies and rules to quickly determine the legitimacy of a transaction based on the risk score. Merchants and their acquirer/processors incorporate the information provided by the networks and issuers to decide which transactions to approve or deny, as shown in Figure 1. Getting the process right means happier customers and more revenue; getting it wrong yields the opposite.

Purchase Authorization Is a Multistep Process

Figure 1: Payment Card Authorization Process



© 2015 GA Javelin LLC

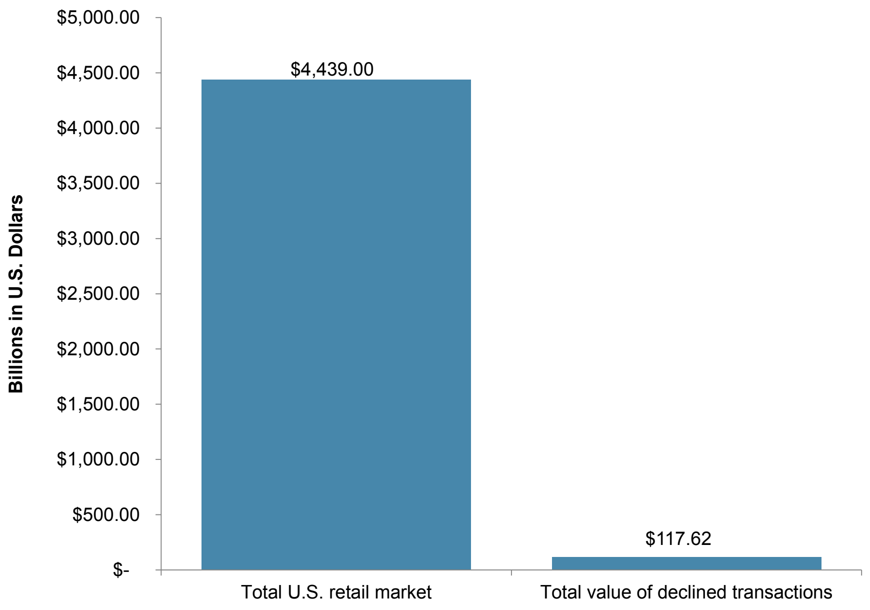
[1] "Poll: Fraud Alert False Alarms Common," http://www.creditcards.com/credit-card-news/fraud-alert-blocked-poll.php, accessed June 24, 2015.

The Challenge of Both Authorizing Purchases and Stopping Fraud

Unfortunately, today's authorization rules and strategies often lead to what is known as a "false positive," or a legitimate transaction that is falsely denied because of suspected fraud. False-positive declines are a serious, costly threat to merchants, as each incorrectly denied purchase means lost revenue and erosion of customer trust. And while authorization rules certainly do stop some instances of fraud, total U.S. fraud losses are minor compared to the total amount of retail transactions denied to suspected fraud. Javelin estimates that 33 million cardholders, or 15% of all cardholders, had a transaction denied because of suspected fraud in 2014, resulting in a loss of nearly $118 billion (see Figure 2). In total, an estimated 127 million legitimate transactions are denied each year because of a false suspicion of fraud. The rate of false-positive declines is over three times that of existing-card fraud: In 2014, 4.42% of customers were affected by existing-card fraud, representing a loss of $9 billion.

Declined Transactions Represent Nearly 3% of the Total U.S. Retail Market

Figure 2: Total U.S. Retail Market Spend vs. Total Value of All Suspected Fraud Transactions

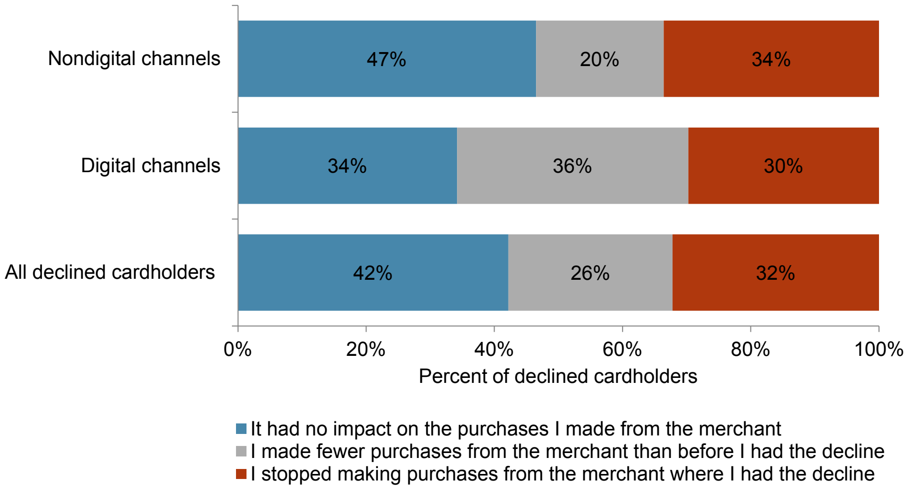


Merchants are well-versed in the danger of fraud, but the prevalence of false-positive card declines is equally threatening. Today, the bulk (57%) of false positives occur at physical stores, followed by digital channels, which is made up of two subsections: online using a computer (e-commerce), which represents 31% of all false-positive declines, and online using a mobile app or browser (m-commerce), representing 5%, or $1.69 billion. Purchases made by calling a business — ordering from a catalog or ordering by phone from a store — are less common than online or e-commerce sales and thus make up just 2% of all false-positive declines. Other shopping channels total 3% of all false declines.

Although false-positive declines are greater at the point of sale (POS) than during CNP transactions, the proportion of total sales volume lost to declines is fairly similar across these channels. As shown in Appendix Figure 9, Javelin estimates that annual POS retail sales reached $4.06 trillion in 2014, meaning that in-store false-positive declines represented 2.7% of the total annual sales volume. Combined e-commerce and m-commerce retail sales reached a total of $351.90 billion in 2014 — with $295.30 billion coming through e-commerce and $56.60 coming through m-commerce. Total digital false positives represent 2.4% of e-commerce retail sales and 3% of m-commerce transactions.

6 in 10 Consumers Report Decreasing Card Usage After Transaction Decline

Figure 3: Impact of a Declined Transaction on Card Usage



© 2015 GA Javelin LLC

In total, 5.6% of all cardholders faced falsely declined CNP purchases in 2014. On average, each of these consumers was attempting to purchase a total annual amount of $723 on e-commerce sites. Merchants who employ overly restrictive fraud measures may have the best intentions, but a false decline can seriously diminish future purchasing revenue: nearly 6 in 10 (58%) declined cardholders report that they either limited or ceased their patronage of the merchant following the decline, and 32% report that they stopped shopping with the merchant entirely (see Figure 4).

In total, 11 million shoppers abandoned merchants following a false-positive decline, and an additional 9 million limited their patronage of the retailer. Furthermore, 34% of individuals who were declined in a nondigital channel (in store or by telephone) and 30% of cardholders who were declined in the e-commerce or m-commerce channel report that they stopped shopping at the merchant following a false decline. The impact of false positives is serious and results in lost sales and increased overhead.

A Growing Problem in the Digital Retail Realm

During the past five years, card transactions — in particular, CNP purchases — have grown dramatically and are expected to continue growing. Online purchases grew from a measly $28 billion (1.1% of total retail sales) in 2000 to $352 billion (8% of total retail sales) in 2013.[2] E-commerce sales are expected to maintain a 6.7% compound annual growth rate (CAGR) through the next five years, reaching $486.3 billion in 2018.

While this growth spells enormous opportunity for merchants, it also creates a lucrative opportunity for thieves. In 2013, U.S. e-commerce fraud reached $9 billion and is expected to grow to $18.4 billion by 2018.[3] In contrast, POS fraud was only $6 billion in 2013 and is projected to fall to $4.5 billion by 2018 with the expected implementation of EMV chip cards. The ratio of fraud to sales is considerably different for digital vs. in-store shopping, as the $4.06 trillion POS

[2] **Online Retail Payments Forecast 2013–2018: Alternative Payments Go Mainstream,** Javelin Strategy & Research, February 2014.

[3] **Fixing CNP Fraud: Solutions for a Pre- and Post-EMV U.S. Market,** Javelin Strategy & Research, October 2014.

retail market absolutely dwarfs total e-commerce sales — yet online fraud is significantly more substantial.

Increasing e-commerce and m-commerce shopping volume, changing consumer behaviors, and evolving fraud schemes all increase the difficulty in separating legitimate purchasers from thieves. The rise of digital goods (e.g., music, games, or other intangible items) has reduced the effectiveness of traditional fraud mitigation. Virtual delivery capabilities remove traditional geographic restrictions on fraud and offer no shipping address for merchants to verify. Furthermore, consumer demand for immediate delivery of digital and physical goods thwarts manual reviews of e-commerce and m-commerce purchases so that merchants are expected to immediately approve transactions, or risk losing the sale. This risk is especially pertinent as consumers use these channels to comparison shop at multiple merchants for the best price and shopping experience.

The digital goods market is a bountiful paradise for opportunistic fraudsters. The channel's anonymity, easy resale of stolen items, and lack of physical shipping make digital goods especially appealing to thieves. Merchants today have limited liability for POS fraud — this will change with the October 2015 EMV liability shift[4] — but those who maintain a digital storefront bear the brunt of CNP fraud losses. Accurate assessment of purchases has never been more important to merchants: Failing to identify thieves may result in fraud loss, while applying overly restrictive fraud controls may result in additional loss by pushing declined shoppers to competitors.

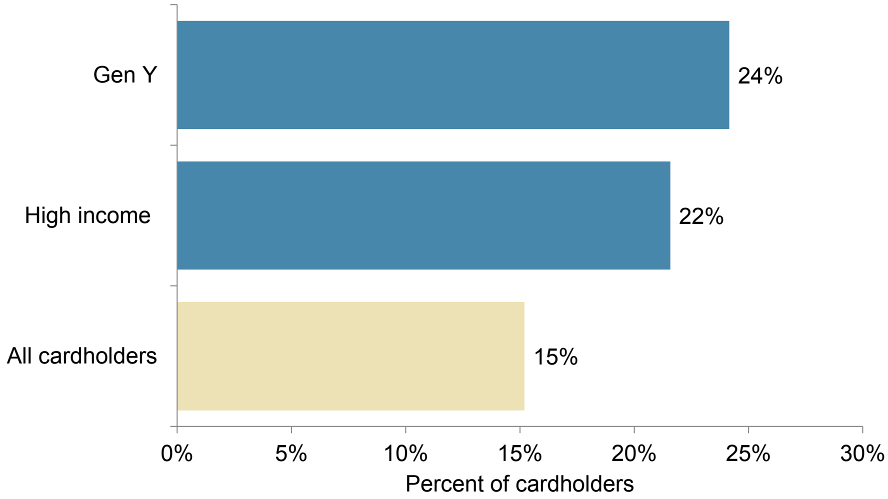
[4] **State of EMV Cardholders: Opportunities to Capitalize on the Halo Effect,** Javelin Strategy & Research, June 2015.

DEMOGRAPHICS

False-positive declines are a widespread issue, affecting 33 million individuals, or 15% of all cardholders (see Figure 4). However, overly stringent fraud measures have a disproportionate impact on two key segments: Gen Y and high-income consumers. The Gen Y consumer segment includes those individuals born in 1980 or later — they are important to merchants because of their spending behavior. Gen Y consumers may be young today, but they are quickly becoming financially independent and merchants would be wise to capture their loyalty early on. However, doing so is complicated by the fact that nearly one-quarter (24%) of Gen Y cardholders have experienced a false decline. Likewise, high-income consumers (i.e., those who earn more than $100K a year) are also disproportionately affected by false positives, with 22% report being falsely declined in the past year. High-income consumers are an extremely important segment for merchants, as they have more discretionary spending.

1 in 6 Cardholders Has Had a Transaction Declined Because of Suspected Card Fraud

Figure 4: Percent of Cardholders Who Had a Transaction Declined Because of Suspected Card Fraud in the Past 12 Months



© 2015 GA Javelin LLC

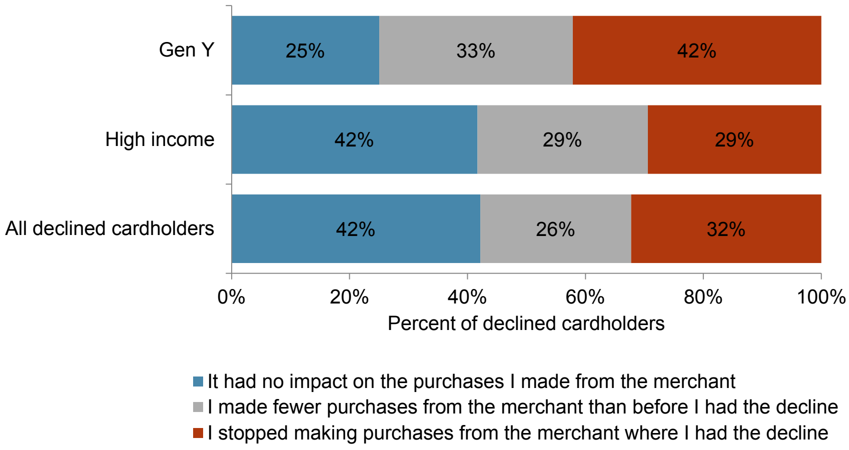
Gen Y

Gen Y consumers face higher decline rates for a variety of reasons: These individuals do not have as much disposable income as more wealthy or established groups, and thus any deviation from normal spending behavior might trigger an authorization decline. Furthermore, their propensity for shopping at certain merchants — such as those who sell digital goods — may increase the risk of a red flag being raised on a transaction. Over one-third (34%) of declined Gen Y cardholders indicate that they were declined while making an e-commerce purchase, compared to 32% for all declined cardholders (see Appendix, Figure 7).

Gen Y consumers are a crucial demographic because they represent the shoppers of the future, and obtaining their loyalty now means long-term revenue for merchants. However, merchants must be careful when authorizing or denying transactions, as Gen Y consumers report the strongest negative response to false-positive declines. Three-quarters (75%) of Gen Y cardholders limited or ceased shopping at a merchant following an illegitimate decline, with 42% reporting that they stopped their patronage of the retailer (see Figure 6).

Three-Fourths (75%) of Gen Y Declined Cardholders Limited Their Usage of the Merchant Following a False Positive

Figure 5: Impact of a Declined Transaction on Card Usage, by Gen Y, High Income, and All Declined Cardholders



Young adults (18 to 24 years of age) are especially likely to abandon a merchant, with almost half (49%) of these declined cardholders indicating that they abandon a merchant altogether after a false-positive decline.

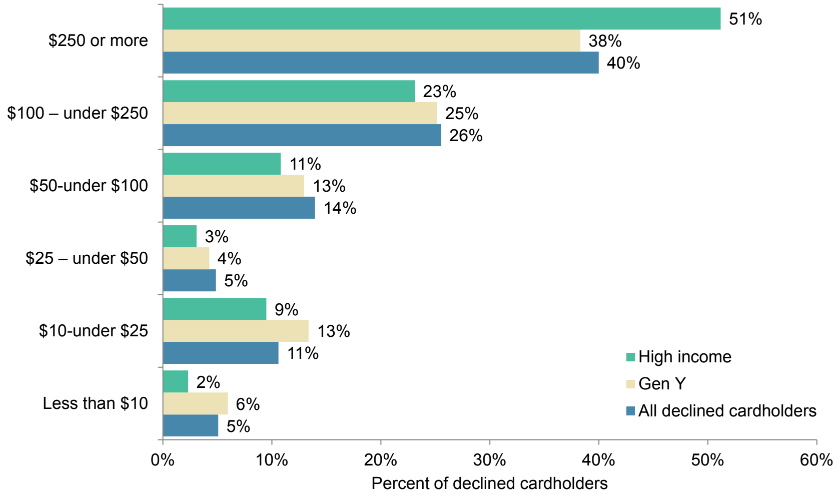
As Gen Y consumers come into their financial and shopping maturity, they may be prone to switching merchants after a negative experience. Research shows that they are more likely to report a smaller total declined transaction amount than other cardholders, with 19% indicating that their annual declined amount was less than $25 vs. 16% for all declined cardholders (see Figure 7). However, an additional 63% of Gen Y cardholders report a total decline amount of $100 or more, which hints at this group's future spending potential. Merchants will have to carefully balance their need for preventing fraud with their desire to build relationships, as these may be mutually exclusive options at times.

High-Income Consumers

High-income consumers are obviously a desirable segment to merchants because of their ability to spend. Perhaps due to their higher transaction volume compared to all cardholders, high-income consumers are declined at a significantly higher

Over Half of High-Income Cardholders Experienced $250+ in False Positives in 2014

Figure 6: Total Amount Declined During the Past 12 Months, by High Income, Gen Y, and All Declined Cardholders



rate than that of cardholders as a whole (22% vs. 15%). Understandably due to the elevated risk involved, high-income consumers are especially vulnerable to declines on high-value transactions. As shown in Figure 7, over half (51%) of high-income consumers report an annual decline value of $250 or more.

In contrast, just 11% of high-income cardholders report a total decline value of less than $25. The higher likelihood of a decline on a bigger transaction is doubly concerning for merchants, since they are not only losing more revenue on the transaction, but are also more likely to lose this high-value relationship. High-income consumers report a troubling propensity to avoid a merchant following a decline. Fifty-eight percent of high-income consumers indicate that they reduced their patronage of the merchant after a false-positive decline, with 29% indicating that they stopped shopping with the merchant. Losing the loyalty of high-income consumers can result in serious future revenue loss, which goes far beyond the fraud loss the transaction decline was intended to prevent. Once again, the key lies in authorization practices that can both stop fraud and approve legitimate transactions.

SOLUTION

In today's digital marketplace, the stakes for proper authorization strategies have never been higher. A key lesson in today's overly fraudulent shopping environment is that validation of PII (e.g., name, birthdate, and Social Security number) alone is insufficient, because the information is static and widely available to fraudsters. The proliferation of PII online, including on black market websites, makes false credentials easy to come by. The static nature of PII makes it easy for fraudsters to adopt a stolen identity. Even basic device verification or reputation can be spoofed by tech-savvy thieves, who can falsify device identifiers or hide behind proxies, making it harder for merchants to differentiate fraudulent transactions from those that are legitimate.

The solution to combating fraud and improving authorization strategies lies in knowing and understanding the customers. Invest in solutions that provide multidimensional intelligence, such as device identification or reputation across multiple shopping verticals. Know if a customer has a good (or bad) reputation shopping at other merchants. Study the patterns of behavior in both legitimate and fraudulent transactions. Monitor patterns such as the average length of time spent on a page, the referring website, browsing patterns, or the use of proxies to gain a more complete picture of a customer.

Linking data such as IP range, shipping address, and payment method across transactions is useful for identifying patterns of fraud and legitimacy. Incorporate additional data from external databases and sources, including social media websites, email addresses, and even physical address verification tools.

Merchants should avoid declining a transaction based on a single suspicious data point (e.g., address verification system (AVS), distance between billing and shipping addresses, and computer proxy). Rather, merchants should adopt a holistic approach to validation and authorization. This approach would entail looking at multiple characteristics of a shopper to determine if all the available data indicate the purchase is legitimate. In essence, this approach calls for a customized understanding of each and every transaction.

Employing a holistic, customized solution is the best approach to combating fraud. Recognizing that automation is crucial for timely transaction authorization, especially for larger merchants, machine learning and rules-based systems will continue to have a central role in merchants' validation and authorization needs. To maximize the effectiveness of these systems, accurate tagging is crucial. A better approach than simple tagging is tagging that specifies which transaction element raised a red flag. Occasionally, transactions are declined because there is insufficient information to validate the legitimacy rather than actual fraud. Accurately tagging each transaction can help shape future authorization rules and may help decrease the rate of false-positive declines.

METHODOLOGY

The consumer data in this report is based primarily on information collected in a random-sample panel of 3,200 consumers in a November 2014 online survey. The margin of sampling error is ±1.65% at the 95% confidence level. Javelin targeted respondents based on proportions of gender, age, and income representative of those of the overall U.S. population.

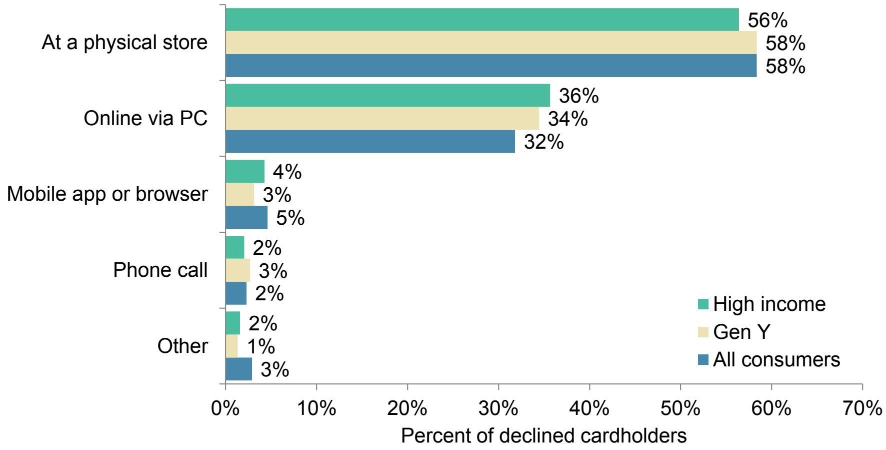
Market Sizing

The false-positive market sizing is derived though survey results, Javelin industry analysis of reported means and frequencies, regularly revised U.S. Census population data, and Javelin's previously published POS, online, and mobile proximity purchasing forecasts.

APPENDIX

Over One-Third of Declined Cardholders Report Having an E-Commerce or M-Commerce Transaction Declined

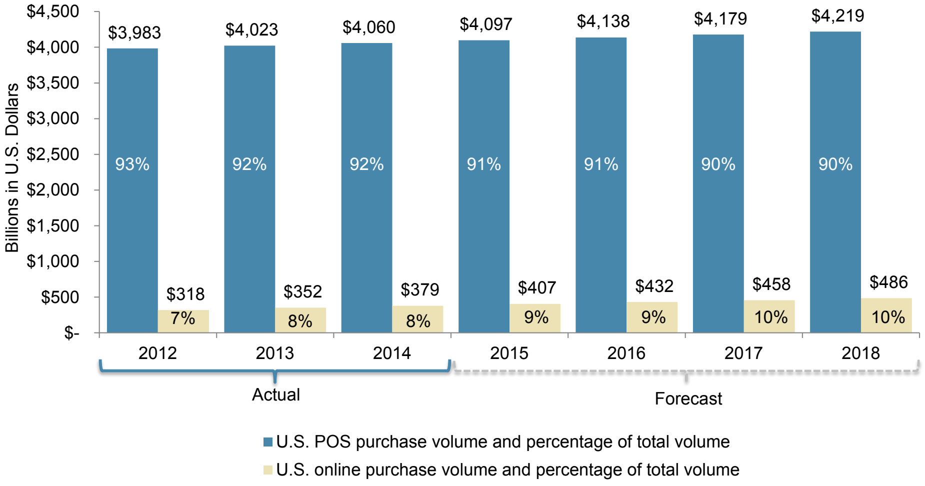
Figure 7: Breakdown of False-Positive Decline by Channel, High Income, Gen Y, and All Declined Cardholders



© 2015 GA Javelin LLC

The Ratio of Total U.S. Retail Spend Online and In-Store Mirrors the Ratio of Losses to Card Declines Between the Same Channels

Figure 8: Total POS and Online Retail Spend and Percent Market Share



© 2015 GA Javelin LLC

ABOUT JAVELIN

JAVELIN, a Greenwich Associates LLC company, provides strategic insights into customer transactions, increasing sustainable profits and creating efficiencies for financial institutions, government agencies, payments companies, merchants, and other technology providers. JAVELIN's independent insights result from a uniquely rigorous three-dimensional research process that assesses customers, providers, and the transactions ecosystem.

Authors: Al Pascual, Director, Fraud & Security
Kyle Marchini, Research Specialist, Fraud & Security
Aleia Van Dyke, Research Consultant

ABOUT RISKIFIED

Riskified is a leading eCommerce fraud management solution trusted by hundreds of brands across the world. Headquartered in Tel Aviv with offices in the US, Riskified utilizes machine learning models, behavioral analytics, device fingerprinting and other fraud detection methodologies to accurately analyze and approve eCommerce orders. Thanks to the exceptional accuracy of its fraud review process, Riskified can identify and prevent fraud while ensuring good customers are not turned away. With full chargeback insurance on approved orders and a pay-for-performance model, Riskified is an economical and effective solution that helps merchants fight fraud and improve their top- and bottom-line sales. For more information, please visit us at www.riskified.com.