The Impact of Fraud and Chargeback Management on Operations

Sponsored by:

VESTA

Americas | Europe | Asia

JAVELIN

September 2015

FORWARD

This original research report, sponsored by Vesta, examines the investments in fraud and chargeback management made by merchants and how apportioning financial resources to manage for these two related challenges diverts funds from investing in a merchant's core competency: selling goods and services. This research report was independently produced by JAVELIN.

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

TABLE OF CONTENTS

TABLE OF FIGURES

OVERVIEW

Providing a valued product and positive customer experience are not the only considerations for merchants looking after their bottom line. While merchants may not have gone into business to become experts on fraud and chargebacks, managing for them requires hefty investment that comprises up to 20% of operational spending. Hiring and training personnel and investing in fraud prevention and chargeback management technology solutions divert funds from revenue-generating activity, leaving merchants feeling as though they are chasing bad money with good. This study explores the burden and underlying drivers and motivations for investment in fraud and chargeback management, as well as its impact on the ability of merchants to be successful in growing their businesses.

KEY FINDINGS

Fraud and chargeback management consume between 13% and 20% of operational budget. As card-not-present (CNP) fraud continues to increase, merchants dealing in digital goods are feeling the pinch. Fraud and chargeback spend is front and center for digital goods merchants, with these merchants dedicating significant proportion of operational costs to keeping fraud in check.

Nearly 3 out of 4 hybrid merchants agree that chargeback management has a major impact on operational budget. Merchants are frustrated in dealing with chargebacks and the associated burden of proof. This is unsurprising, as the increased burden of managing for chargebacks, which includes collecting required documentation and meeting established timelines, takes them away from growing their businesses and revenue.

Nearly half of digital goods merchants are concerned about risks associated with mobile payments. Merchants across all segments expect an increase in fraud in coming years, necessitating an increase in fraud spend. Digital goods merchants plan to dedicate additional operational budget to managing the growing threat of fraud, especially in mobile channels.

The effect on resource allocation related to dedicated fraud and chargeback staff is a serious concern for merchants. While 58% of digital goods merchants believe it is essential to maintain in-house fraud and chargeback management staff, nearly as many (53%) agree that dedicating full-time staff takes away budget from other revenue-generating departments.

Remote channels make managing fraud threats an expensive proposition for digital goods merchants. In order to handle fraud in a non-face-to-face environment, digital goods merchants employ nearly five times the fraud personnel as physical goods merchants, and nearly twice as many as hybrid merchants.

Personnel costs represent more than a third of fraud and chargeback spend. Not surprisingly, personnel costs represent the largest portion of fraud/chargeback spend, accounting for 36% to 41% of fraud- and chargeback-related spend across all merchant segments.

Outsourcing may be a viable option. Vendors who specialize in mitigating evolving fraud threats and managing the shifting sands of network chargeback rules could help merchants focus on their core competency areas. This in turn would allow merchants to reduce fraud- and chargeback-related spend that diverts resources from revenue-generating departments. While digital goods merchants haven't completely made up their minds about outsourcing costs, 63% of physical goods merchants believe that outsourcing fraud mitigation and chargeback management is cost-effective.

Digital goods exposure leads to concerns over the future of CNP fraud. The impending EMV rollout has left merchants troubled about CNP fraud, with nearly half of merchants that deal in digital goods expecting increased concern for the next 12 months. This concern has also instigated an increase in future fraud spend, with just over half of digital merchants expecting to set more aside for managing fraud and dealing with chargeback issues.

RECOMMENDATIONS

Outsource to keep operational budget under control and assist in business growth. There is a compelling business case that digital goods merchants would be better off outsourcing their fraud to solution providers, allowing them to focus on their core business. The amount they have to put into building, managing, and maintaining in-house solutions has significant negative impact on their ability to scale their business over time.

Be mindful of maintaining and building customer relationships while elevating security checkpoints to combat CNP fraud. The projected growth of CNP fraud will introduce a new level of burden for digital merchants, which they will be unable to combat from a resource and scalability perspective. This will increase the pressure and negative impacts on them because they will be hit by fraud that they can’t handle. Their inability to scale quickly enough may result in measures that will hinder customer experience. It is imperative that merchants stay customer-friendly in the face of growing fraud pressure.

CURRENT FRAUD TRENDS AND THE HIDDEN EFFECT ON EXPENSES

The year 2014 has the dubious honor of being the year when the very real threat posed by identity theft burst into the public consciousness. Hundreds of millions of credentials were breached, impacting over a quarter of U.S. consumers. In 2015, little has changed. As institutions of all industries and sizes are pummeled by data breaches, black markets are awash in stolen card data, driving down the price of stolen credentials and making it easier than ever for fraudsters to attack existing card accounts.

Easy access to compromised card data has driven a monumental shift in fraud over the past two years. From 2009 to 2012, card fraud hovered around 60% of total fraud volume, but then precipitously leapt to 85% in 2013 (see Figure 11). In 2013 and 2014, fraud on existing card accounts reached the two highest incidence levels recorded. While the shift to card fraud has resulted in somewhat lower fraud losses for consumers, fraud is a $16 billion problem, and the annual number of victims remains stable, at around 13 million.[1] Even with the rollout of EMV, this threat is not going away anytime soon.

The growing prevalence of card fraud has very real implications for merchants, since it means that more than ever before, the fight against fraud is occurring at their cash registers and checkout screens. While fraudsters opening new accounts and attacking noncard accounts can move stolen funds directly to their accounts through the banking system, card fraud is almost invariably channeled through merchants. As fraudsters seek to capitalize on stolen credentials, more and more frequently they turn to high-value goods that can be either resold easily or returned for cash.

The direct costs are obvious – merchants hit with fraudulent transactions lose merchandise and revenue. However, even if merchants are able to recover their direct losses, they still suffer from being forced to devote limited employee hours to implementing antifraud measures, manually reviewing risky transactions, and

[1] http://www.reuters.com/article/2015/03/03/ca-javelin-strategy-idUSnBw035247a+100+BSW20150303, published March 3, 2015; accessed September 16, 2015.

resolving chargeback disputes. What can be most demoralizing about this process is that much of the battle seems to be happening between the “good guys” – merchants and issuers who fight to allocate liability for fraud, while they should be fighting to prevent it in the first place.

While fraudsters may walk away scot-free, merchants and issuers have to bear the brunt of chargeback management costs. This is especially burdensome in cases of friendly fraud, where customers dispute legitimate transactions. In these cases, the cardholder will be able to pass through most conventional antifraud measures, but still leave the merchant fighting chargebacks. The cost of chargebacks is likely to grow as card transactions continue to displace cash, giving consumers an ever-greater opportunity to dispute transactions, and as e-commerce and m-commerce transactions become increasingly popular, removing the interpersonal interaction that made friendly fraud a less savory endeavor for consumers to undertake.

> “Now it is just so easy to dispute a credit or debit card charge and it is so biased toward the consumer. On the business side, it is pretty tough to prove that they purchased or used the product.”[2,3]

Digital Goods Merchants Face the Greatest Burden

It is undeniable that transacting in the digital world provides consumers and merchants with several benefits; however, it also comes with its share of worries about fraud. E-commerce merchants have not been free of data breaches as sophisticated techniques are used to hack into merchant systems to steal consumers’ card information. Just as consumers can place their orders from anywhere with an Internet connection, fraudsters can also benefit from the non-face-to-face environment to conduct fraud from across the globe.

Digital goods, such as software, gift cards, and tickets, pose additional challenges, since they eliminate data points typically used for validating customer identities and assessing the risk level for transactions. Moreover, in a retail environment where customers demand immediate access to their purchase, there is no room for time-consuming scrutiny of risky sales. Digital goods merchants face the choice between declining legitimate customers and losing business to competitors, or facing escalating fraud and chargeback losses.

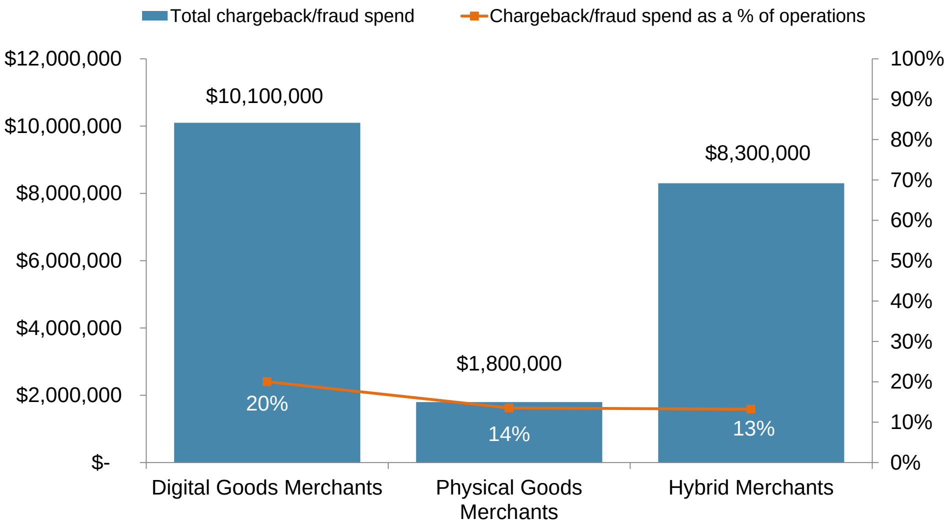
[2] **2014 Retail Point of Sale Payment Forecast: The Mobile Payment Square-Effect and Prepaid Card Popularity Drive Case Down by 10%**, Javelin Strategy & Research, May 2014.

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

Unsurprisingly, digital goods merchants, who operate only in this higher-risk realm, dedicate the greatest proportion of their operational budget to fraud and chargeback management. They set aside 20% of their operational budget toward fraud- and chargeback-related expenses, while physical and hybrid merchants spend only 14% and 13% of operational costs, respectively, toward fraud- and

Digital Goods Merchants Outspend Hybrid and Physical Goods Merchants in Managing for Fraud and Chargeback Management by a Significant Margin

Figure 1: Total Chargeback/Fraud Spend and Portion of Operational Expenses, by Merchant Type

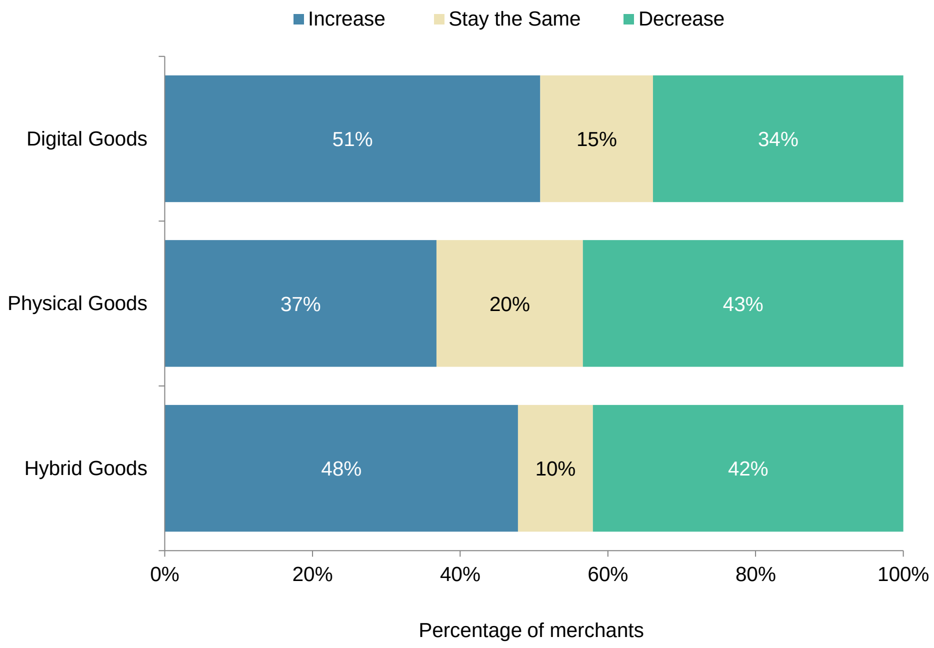


FACTORS AFFECTING FUTURE SPENDING

When examining the factors that will motivate budget planning for fraud and chargeback management expenses, the advent of EMV is a subject that clearly adds to the digital goods merchants' existing agony over fraud. Over half of digital goods merchants expect fraud- and chargeback-related spending to increase in the next 12 months (see Figure 2). In anticipation of EMV motivating some point-of-sale (POS) card fraudsters to shift to the CNP environment, digital goods merchants will add stricter CNP authorization rules and hinder customer relationships.[4] (See "Anticipating the Side Effects of EMV," page 17.)

Just Over Half of Digital Goods Merchants Expect Chargeback/ Fraud Spend to Increase in the Next 12 Months

Figure 2: Impact on Chargeback/Fraud Spend in the Next 12 Months



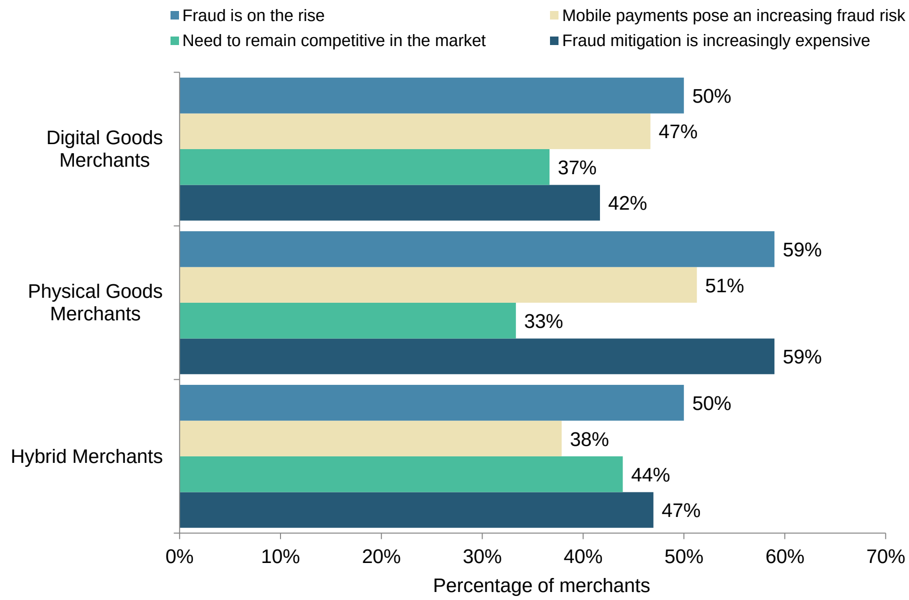
© 2015 GA Javelin LLC

[4] **Future-Proofing Card Authorization**, Javelin Strategy & Research, August 2015.

More than half of merchants across all segments expect fraud to rise, demanding an increase in fraud- and chargeback-related spending. While general price hikes in fraud mitigation solutions may well necessitate increased spending, merchants are also concerned about the potential risks associated with accepting mobile payments. While merchants that are new to mobile payments certainly have their work cut out for them, this is an evolving space with new payment solutions and threats, meaning that even experienced merchants may find themselves in a position to dedicate additional resources to this challenge in the coming year.

Half or More of Merchants Across all Segments Believe Fraud Is on the Rise, Demanding an Increased Spend

Figure 3: Reasons for Increasing Chargeback/Fraud Spend in the Next 12 Months



© 2015 GA Javelin LLC

Merchant Perspectives

In direct conversations with merchants, one expressed that concerns about the risks associated with accepting payments through remote channels led the company to accepting only physical corporate checks as payments.[5] Another merchant interviewed has plans to push online booking and payments, but has a follow-up confirmation process to keep friendly fraud in check.[6] While these methods have the potential to keep fraud at bay, they may also result in business challenges due to delay in payments and inconveniences to their respective customers, especially when compared to competing merchants.

[5] Qual report.

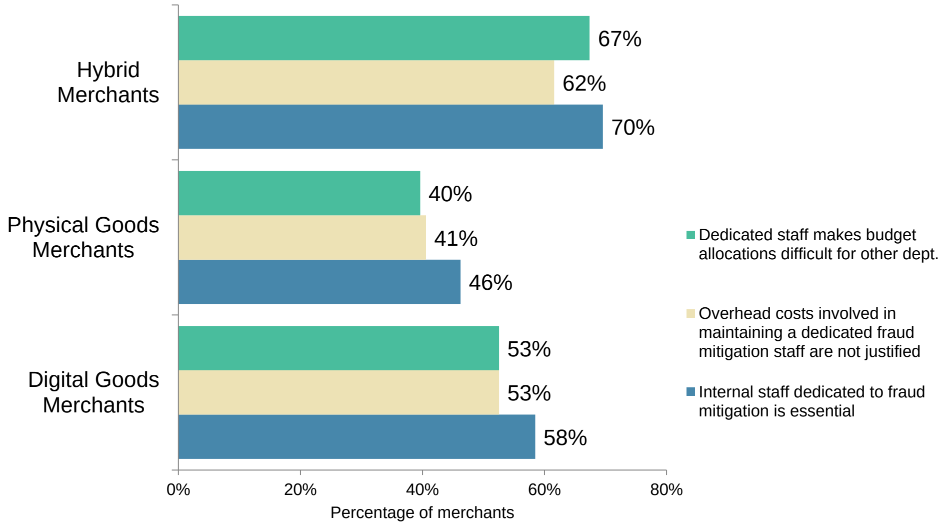
[6] Ibid.

STAFFING INVESTMENT AND THE IMPACT ON BUSINESS

Staff dedicated to managing for fraud and chargebacks, albeit indispensable for many merchants, is a significant pain point. Merchants employ significant manpower to deal with chargebacks and false-positives, instead of the conduction and growth of their business – it's a consequence of controlling for fraud and chargebacks that doesn't get enough discussion. Over half of digital and hybrid merchants agree that dedicated internal staff is essential (58%) (see Figure 4), but the majority of these merchants also believe that it hinders business growth (53%).

Over Half of Digital Goods and Hybrid Merchants Agree Dedicated Staff Is Essential, but Also Inconvenient

Figure 4: Merchant Challenges on Dedicated Internal Team – Showing Top 2 Boxes



© 2015 GA Javelin LLC

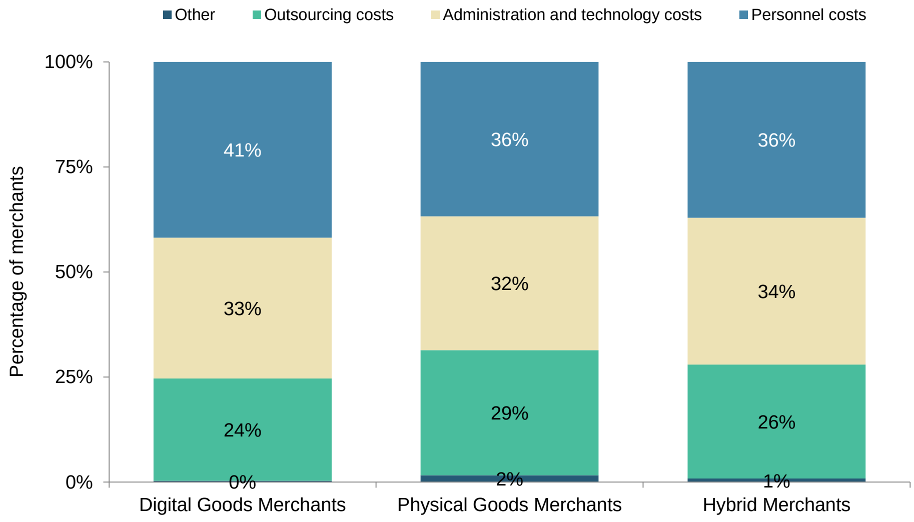
Among smaller merchants, dedicating staff time to manage for these challenges may involve senior managers taking time from running the business and finding ways to generate additional profits, and instead manually reviewing orders.[7] Frustrations from this type of example can be seen in the majority of hybrid merchants, and over 2 in 5 physical merchants who believe that overhead costs involved in maintaining an internal staff is not justified and impacts budget allocations to other departments (see Figure 4).

In addition to the lost opportunity to allocate resources to other departments, staffing dedicated fraud and chargeback personnel is simply not an inexpensive proposition for merchants. Personnel costs make up the majority of fraud and chargeback management-related expenses. Personnel costs accounted for 35% to 39% of fraud spend across all merchant segments, and even exceeded fraud related administration and outsourcing costs (see Figure 5).

> "While we have not had any successful claims against us we definitely see time, productivity and resources lost"

Personnel Costs and Admin/Technology Account for the Majority of Fraud and Chargeback Management Spend

Figure 5: Key Factor for Chargeback/Fraud Spend



© 2015 GA Javelin LLC

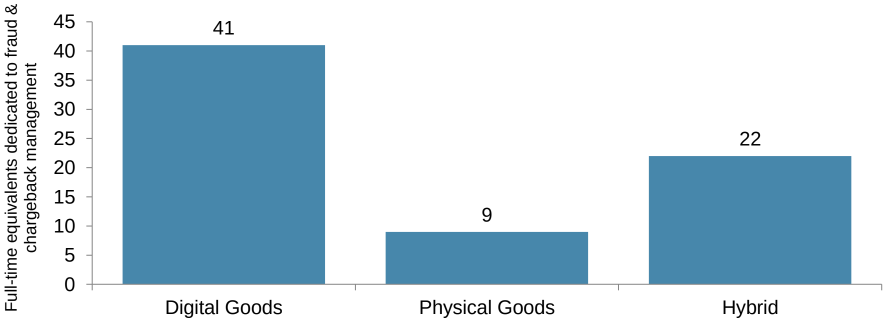
[7] Qual report.

Managing for fraud in an environment where merchants do not interact with consumers face-to-face, though consumers have equal or even higher shopping experience expectations, can lead e-commerce and m-commerce merchants to overcompensate for deficiencies in their controls with a human touch. This may be a seemingly necessary component for merchants who want to avoid false-positives and chargebacks from fraud. Over 15% of all cardholders had a transaction falsely declined due to suspected fraud in 2014.[8] Today's card authorization rules and strategies cast a wide net to stop fraudsters, but false-positive declines are detrimental and costly in their own right. The total amount lost due to false declines in 2014 ($118 billion) was vastly greater than the total amount lost due to actual card fraud ($9 billion)[9], and avoiding that lost business is a priority in an industry where customer loyalty is at a premium.

One particular segment of merchants, those that sell only digital goods, are forced to dedicate more of their fraud- and chargeback-related spending to specialized personnel than any other segment, due to the nature of the channel in which they do business. Digital goods merchants employ nearly five times the fraud personnel as physical goods merchants, and nearly twice that of hybrid merchants (see Figure 6). For digital goods merchants in particular, they may avoid manual reviews and accept a higher rate of chargebacks as the cost of quickly approving a transaction, and instead resign themselves to hiring and maintaining the staff necessary to manage those chargebacks.

Digital Goods Merchants Employ Nearly 5x as Many Staff Dedicated to Fraud and Chargebacks as Physical Goods Merchants

Figure 6: Number of Employees Dedicated to Fraud and Chargeback Management



© 2015 GA Javelin LLC

[8] **Future-Proofing Card Authorization**, Javelin Strategy & Research, August 2015.

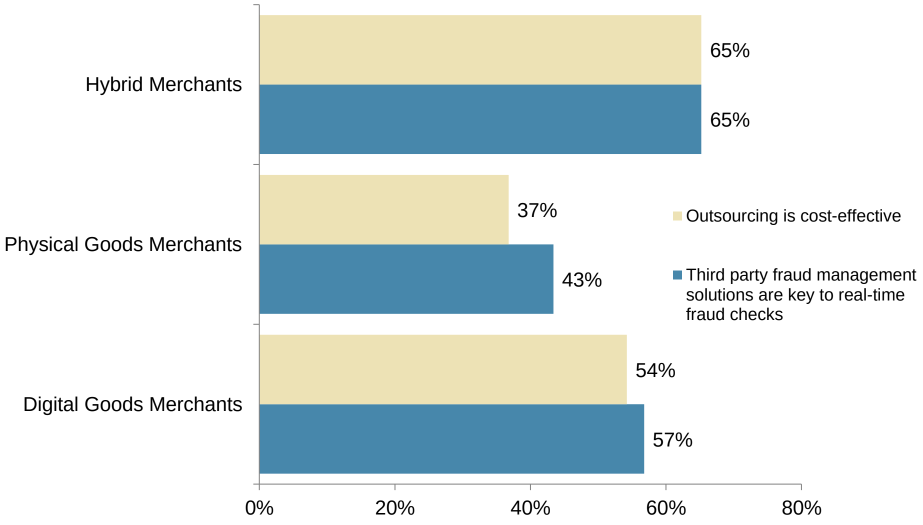
[9] Ibid.

Hybrid Merchants See the Value in Outsourcing

Outsourcing can make a lot of sense for merchants as it shifts responsibility for navigating new fraud trends and the complex web of chargeback rules to vendors that specialize in these spaces, leaving merchants to run their business and free from having to be fraud or chargeback experts.

Nearly Two-Thirds of Hybrid Merchants Believe Outsourcing Is Cost-Effective

Figure 7: Merchant Challenges on Outsourcing

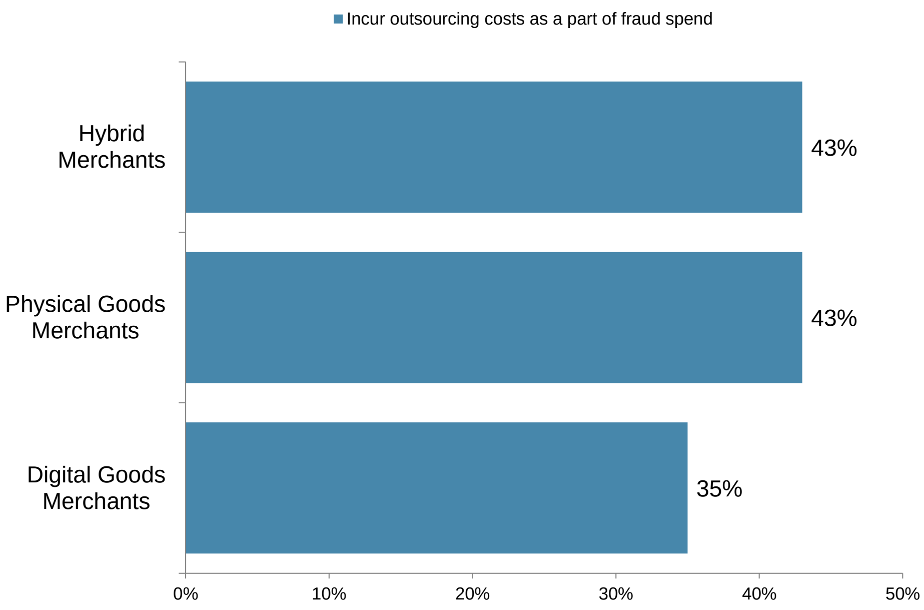


© 2015 GA Javelin LLC

And despite more than 3 in 5 hybrid merchants agreeing that their operational budget is significantly impacted by fraud and chargeback management, outsourcing is an area of spending where this segment of merchants is more positive than others. Approximately three quarters of all merchant types report that their fraud spending includes outsourcing costs, 65% of hybrid merchants believe that outsourcing fraud mitigation and chargeback management is in fact cost-effective (see Figure 7) and 2 in 5 of them rely on outsourcing to keep fraud at bay (see Figure 8).

Over 2 in 5 Hybrid Merchants Incur Outsourcing Costs as Part of Fraud Spend

Figure 8: Outsourcing Costs as Part of Fraud and Chargeback Management Spend



© 2015 GA Javelin LLC

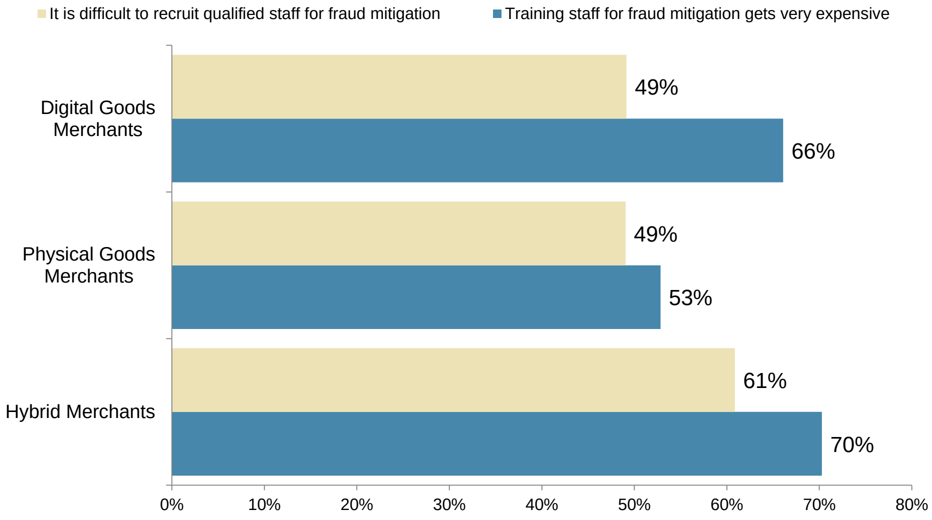
More Than Just Salaries: Finding and Training Staff

If personnel costs and keeping resources from revenue-generating tasks aren't serious enough challenges, two other issues associated with maintaining an internal staff that create difficulties for merchants are staff recruitment and training. Over 60% of hybrid merchants and nearly half of digital and physical goods merchants believe that finding qualified personnel for fraud and chargeback management is difficult (see Figure 9).

Moreover, training employees is no menial task. Over 60% of merchants with a digital presence agree that training employees for fraud and chargeback management is cost-prohibitive. Changing fraud trends can mean that training is a continual process and cost, along with the continued need to train new employees as rollover inevitably occurs. Nearly 3 in 4 hybrid merchants and over half of digital merchants agree that the changing nature of fraud across multiple channels makes dynamic training difficult (see Figure 9).

Hybrid Merchants Feel the Most Stress with Training and Recruiting Staff for Fraud Mitigation

Figure 9: Merchant Challenges With Recruiting and Training Fraud Staff



© 2015 GA Javelin LLC

ANTICIPATING THE SIDE EFFECTS OF EMV

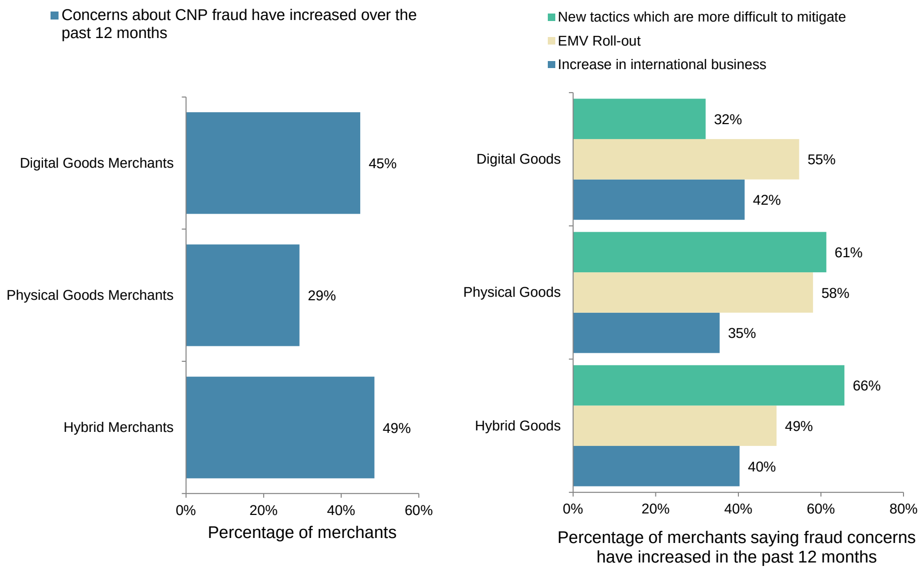
As the U.S. continues to migrate to EMV from traditional magnetic stripe transactions, the fraud landscape will shift accordingly. Due to the comparatively simple and inexpensive nature of producing counterfeit magnetic stripe cards, counterfeit – rather than lost/stolen – card fraud is at present the dominant threat against brick-and-mortar merchants. Since it is extremely difficult to counterfeit EMV cards, card fraud at physical points of sale will decline as more cardholders are issued chip cards and more merchants accept them. Unfortunately, with many small merchants and issuers slow to adopt EMV, even in the face of the liability shift, the decline in POS fraud will be more of a slow fade than a rapid drop – falling from $6 billion in 2014 to $5 billion in 2018 (see Figure 12).

As fraudsters transition away from counterfeit card fraud, fraud rings that specialize in POS fraud will transition to other means of obtaining physical cards, most notably new account fraud and account takeover. By opening new accounts or convincing financial institutions to issue new cards from existing accounts, these rings are still able to obtain physical cards to conduct transactions at brick-and-mortar stores.

However, chip technology on a physical card does nothing to prevent e-commerce fraud. With CNP fraud already a major issue, this creates a significant concern among e-commerce merchants that online card fraud will dramatically increase as EMV becomes more prevalent. Nearly half of digital goods and hybrid merchants indicate that their concerns over CNP fraud have increased over the past 12 months, with many directly tying this concern to the EMV rollout (see Figure 10). E -commerce merchants selling digital goods strongly believe that the EMV shift will drive their increased fraud exposure. Merchants selling physical or hybrid goods tend to face more general concerns about changing fraud tactics, regardless of the specific factor influencing the change.

Triggered by Potential Fraud Shift After EMV Rollout, Hybrid Merchants Are Most Concerned About CNP Fraud

Figure 10: Concerns Around CNP Fraud in Last 12 Months – Increased



© 2015 GA Javelin LLC

This position is an intuitive response to EMV, but fails to account for how fraud rings currently operate. POS fraud rings rely on a geographically concentrated group of card printers and runners who take physical counterfeit cards to brick-and-mortar stores to purchase physical goods. CNP fraud rings can be much more geographically diverse and require more technical aptitude to circumvent increasingly common fraud controls, such as IP address-based geolocation. These divergent methodologies make it unlikely that POS fraud rings will jump directly into CNP fraud.[10]

While CNP fraud is indeed expected to grow significantly over the next five years, the primary driver is the growing volume of online card transactions.[11] The increased volume of commerce brings with it more merchant portals for fraudsters to target for potential cardholder verification vulnerabilities, and more legitimate commerce to hide within. It also raises the stakes for merchants' antifraud efforts by increasing the potential cost of false-positives – the more that

[10] **2015 Data Breach Fraud Impact Report**, Javelin Strategy & Research, June 2015.

[11] **Future-Proofing Card Authorization**, Javelin Strategy & Research, August 2015.

consumers transition to online transactions, the greater the risk of aggressive fraud prevention diverting legitimate customers to competitors' sites. Together, these factors drive up the risk associated with CNP fraud, regardless of the EMV rollout.

These escalating risks highlight the challenge that fraud poses to growth. The acceleration of e-commerce offers tremendous opportunities for merchants in both streamlining their sales process and in discovering new business opportunities. However, as merchants strive to balance the greater demand from legitimate customers and the growing risk of fraud, every dollar and employee that merchants allocate to fraud prevention is one that they cannot allocate to revenue-generating activities. Over half of digital merchants and 2 in 3 hybrid merchants agree that maintaining an internal staff for fraud and chargeback management makes it challenging to hire and divert resources to other revenue-generating departments (see Figure 4).

Digital goods merchants, the segment with the most to gain from expanding e-commerce, are also the most likely to increase the amount they spend on fraud/ chargeback management. In anticipation of increased fraud threats, more than half of digital merchants expect to increase their fraud expenditures in the next 12 months (see Figure 2). These expenses cover the cost of personnel, fraud mitigation solutions, and any additional fraud liability incurred.

The anticipated growth of CNP fraud puts added pressure on merchants who are struggling to keep fraud and chargeback management costs in check. The direct risks and indirect costs of fraud mitigation will only make business opportunities and growth even more problematic for merchants with a digital presence that already have to combat sophisticated techniques, spread across multiple digital channels, used by fraudsters.

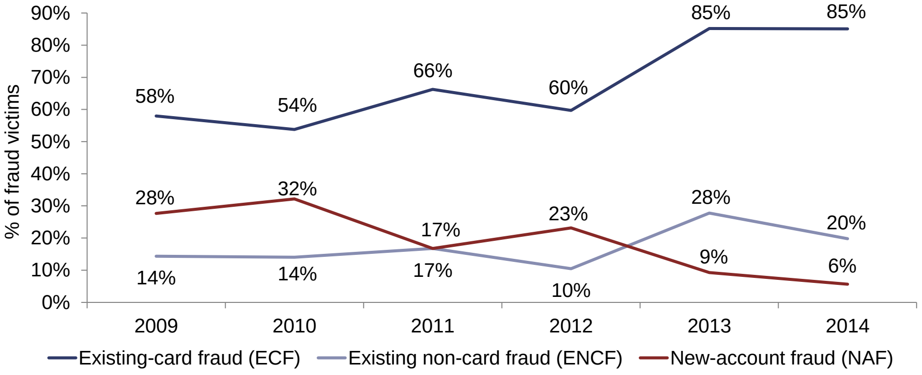
CONCLUSION

Merchants are frustrated not only by losing hard-earned revenue to fraud, but also by having to divert operational costs to preventing it and chasing chargebacks. Digital goods merchants in particular would be better off by outsourcing their fraud mitigation to experienced solution providers, allowing them to focus on their core business, given that they keep an average of 41 full-time employees on staff to address these issues and dedicate fully 20% of their operational costs to fraud and chargeback mitigation. Building, managing and maintaining in-house solutions not only entail hefty startup costs, but can be difficult to scale along with a growing business. The expected growth of CNP fraud will introduce a new level of burden for digital goods merchants, which they will be unable to combat from a resource and scalability perspective. This will increase the pressure and negative impacts on them, as an inability to scale quickly enough will result in deploying measures that hinder the customer experience.

APPENDIX

Attacks on Existing Card Accounts Growing as a Proportion of Fraud

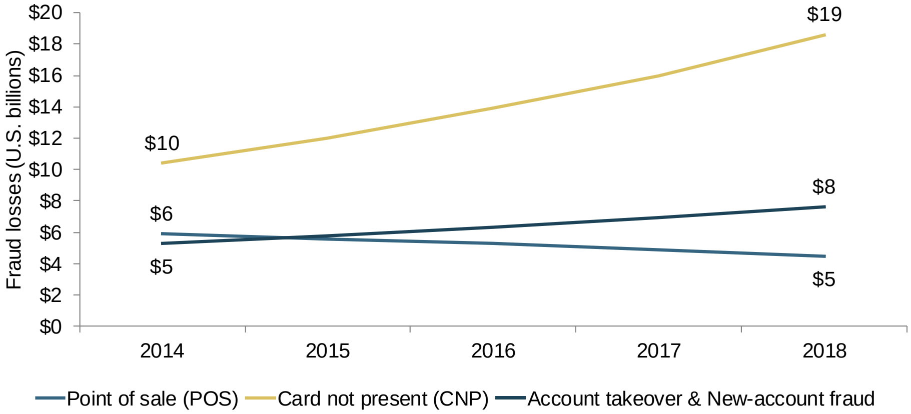
Figure 11: Fraud Types as Proportions of All Fraud Victims, 2009–2014



Note: Categories are not mutually exclusive.

CNP Fraud Will Grow to $19 Billion by 2018, as U.S. Merchants Contend With $5 Billion in Fraud at the POS Despite EMV

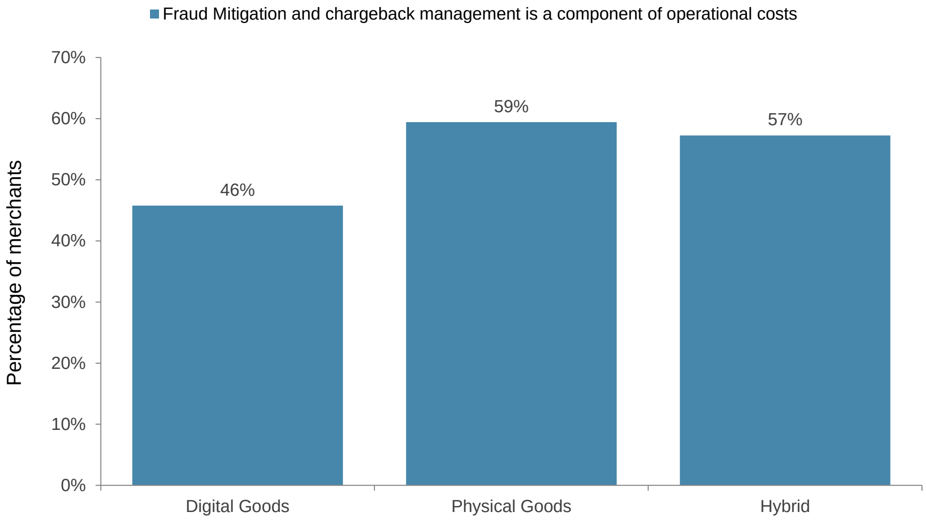
Figure 12: Total Losses by Fraud Type, Forecast (2014–2018)



Projections based on Javelin internal data, United Kingdom, and Canadian card fraud data.

Digital Goods Merchants Most Likely to Include Fraud Mitigation and Chargeback Management in Operational Expenses

Figure 13: Merchants Indicating Fraud Mitigation and Chargeback Management Is Part of Their Operational Expenses



© 2015 GA Javelin LLC

METHODOLOGY

In June 2015, Vesta retained JAVELIN to conduct a comprehensive independent study on merchant spending on all operations associated with fraud and chargeback management.

JAVELIN conducted an online survey of 362 merchants earning $1 million or more annually, falling into three key merchant segments:

- 118 merchants selling only digital goods
- 106 merchants selling only physical goods
- 138 hybrid merchants, selling both types of goods

Additionally, in-depth interviews were conducted with industry executives in roles influencing operation expenses related to fraud and chargeback management.

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.

Author: Al Pascual, Director, Fraud & Security

ABOUT VESTA

Vesta Corporation is the global leader of revenue-generating payment solutions for enterprise partners in the telecommunications, media, financial, and digital sectors. The company's patented fraud protection technology is proven to increase conversion and acceptance while eliminating fraudulent transactions and merchant liability. Vesta has been recognized as a leading innovator in payments technologies, holds multiple patents, and has won numerous awards as one of America's fastest growing companies. Founded in 1995 and headquartered in Atlanta, Vesta's operations span the Americas, Europe and Asia. For more information, visit trustvesta.com.