THE FINANCIAL IMPACT OF FRAUD:
MERCHANTS CHALLENGED AS E-COMMERCE FRAUD RISES POST-EMV

October 2016

Sponsored by:

VESTA
Americas | Europe | Asia

Independently produced by:

JAVELIN

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

This original research report, sponsored by Vesta, examines the challenges faced by e-commerce merchants in balancing customer experience with the financial realities of combatting fraud. E-commerce merchants are broken into three distinct segments within this report, based on the types of goods they sell: digital goods merchants sell products such as digital media, electronic tickets or virtual gift cards, physical goods merchants sell tangible products such as clothing or electronics, and hybrid goods merchants sell a mix of both physical and digital goods. This research report was independently produced by Javelin Strategy & Research. Javelin Strategy & Research maintains complete independence in its data collection findings and analysis.

OVERVIEW

As e-commerce continues to evolve, it is bringing change to what types of products are being sold, and how they are marketed and delivered. This evolution, too, is challenging merchants' ability to manage fraud. Meanwhile fraudsters are adapting their techniques and shifting their attention to online merchants. This is resulting in rising costs for all merchants, as investments in fraud management, losses from chargebacks, and false-positive declines are increasingly undermining their profitability. In order to effectively defend themselves against fraudsters, merchants must navigate a complex web of solutions to find the right approach — one that does not sacrifice profitability or erode customer experience for the sake of security.

EXECUTIVE SUMMARY

Key Findings

In total, fraud costs merchants more than 7.5% of their annual revenue. Between fraud management costs, false positives, and chargeback losses, merchants are losing a significant portion of revenue to fraud. Digital goods merchants suffered the worst losses, at 8.6% of revenue on average, but hybrid goods merchants faced similar costs at 8.1% of revenue. The majority of these costs came from fraud management expenditures, accounting for around 75% of costs.

Fraud management constitutes a consistently greater portion of merchants' operational costs. All merchant segments are dedicating more of their operational costs to managing fraud when compared with 2015. Digital goods merchants are still at the top of the list (23%), followed by hybrid merchants (16.6%) and physical goods merchants (14.9%), increasing from 20%, 13%, and 14%, respectively in the previous year.

Fraud after EMV is taking a toll on merchants' psyches and their bottom lines, especially for digital goods**.** Both digital goods (44%) and hybrid (43%) merchants indicated that they had seen increases in fraud over the past year. This reflects the growing pressure on digital channels as fraudsters use digital goods to circumvent traditional fraud controls. Following the U.S. transition to EMV, concerns about fraud moving to e-commerce have been rampant, heightening the impression of it being under attack.

False positives eat into merchant revenue. Nearly a third (30%) of all transactions that are declined due to suspected fraud are believed to be legitimate. Digital goods merchants face the worst plight here, with 34% of declined transactions believed to be legitimate. This translates into 2.8% of revenue lost due to suboptimal fraud controls.

Digital goods merchants worry about continuing increases in fraud. Nearly half (49%) of digital goods merchants indicated that their concerns about fraud had increased over the past year. Much of this increase is tied to changing tactics by fraudsters, which merchants find more difficult to mitigate. Among merchants with lower concerns, much of this security came from confidence in their fraud mitigation solutions, which they expect to more effectively address fraud.

Spending increases are expected, especially for digital goods merchants. In keeping with the increased concern, a majority (53%) of digital goods merchants indicated that they expect to increase their fraud management spending over the next 12 months. No one reason stands out for increasing spending, indicating that it is driven by a combination of expected business growth and changing fraud concerns.

Outsourcing appeals to digital merchants. Among digital goods merchants, 43% reported outsourcing all or part of their fraud management services. Because of the need to rely on complex solutions that fall outside of their business expertise, digital goods merchants are more likely than the physical goods or hybrid merchants to benefit from these services.

Digital goods merchants explore new types of tools. While merchants as a whole turned to data validation, digital goods merchants are more inclined to explore next-generation security systems. These merchants are particularly likely to turn to alternate sources of identity information such as geolocation, device identification, and behavioral analytics. These systems are supported by background analytics systems such as transaction scoring and machine learning.

Data validation still tops security solution usage. The top four fraud management tools used include customer identity verification, address verification service (AVS), card verification value (CVC2/CVV2/CID), and static knowledge-based authentication. All of these solution types are vulnerable to deception in an era when consumer data are readily available through breaches, social engineering, or public resources.

Strong authentication comes slowly, leaving the accounts of good customers exposed. Armed with credentials from large data breaches, fraudsters face little difficulty gaining access to customers' accounts as the majority (65%) of merchants still rely on usernames and passwords to authenticate customers accessing existing accounts. Only 40% are using two-factor authentication, and far fewer are using tools such as geolocation (30%) or device reputation (22%).

Merchants are confident in their ability to prevent fraud now, but unsure about how to adapt. A strong majority (68%) of merchants indicated that they are confident in their ability to identify fraudulent transactions. At the same time, many (42%) believe that their fraud mitigation adds too much friction to the customer experience or worry that they cannot reduce false-positive rates with existing tools and personnel (46%).

Recommendations

Move beyond using static data to mitigate fraud, especially for digital goods transactions. Card-centric solutions that use static data elements, such as CVV2 and AVS, are suboptimal when managing fraud in an environment where data are being compromised en masse through malware, social engineering, and breaches. Instead, tools that inspect a customer's device, behavior, and purchase activity are more difficult for criminals to overcome and can be leveraged invisibly and quickly — making them well-suited for preserving the customer experience during digital goods transactions.

Bolster authentication to mitigate the risk of account takeover. Fraudsters are looking beyond just compromising or purchasing card data to commit card-not-present (CNP) fraud. Armed with customer credentials, fraudsters take advantage of weak authentication on merchant sites to infiltrate existing customer accounts and order products using on-file payment information. Stronger solutions, such as device fingerprinting and out-of-band authentication, raise the bar for account security — forcing fraudsters to seek softer targets.

Invest in the timely training of fraud management staff. Fraud management solutions are only as effective as the people behind them. Ensuring top performance from staff requires them to have an up-to-date understanding of new fraud threats and optimal mitigation strategies.

Leverage the experience of other merchants and stay ahead of new fraud trends. Merchants can benefit from the experiences of their peers by sharing information, either informally or through a third-party solution, to prevent fraud and improve the customer experience. This information can include the positive and negative experiences associated with certain customers, individual PII (personally identifiable information) components, devices, locations, and payment accounts.

Weigh all costs related to managing fraud when considering the option to outsource functions. Without a thorough understanding of the different elements that comprise a merchant's fraud-related costs and the investment that comes with managing effective in-house fraud staff and solutions, merchants cannot accurately assess the viability of outsourcing functions to firms that manage merchant fraud.

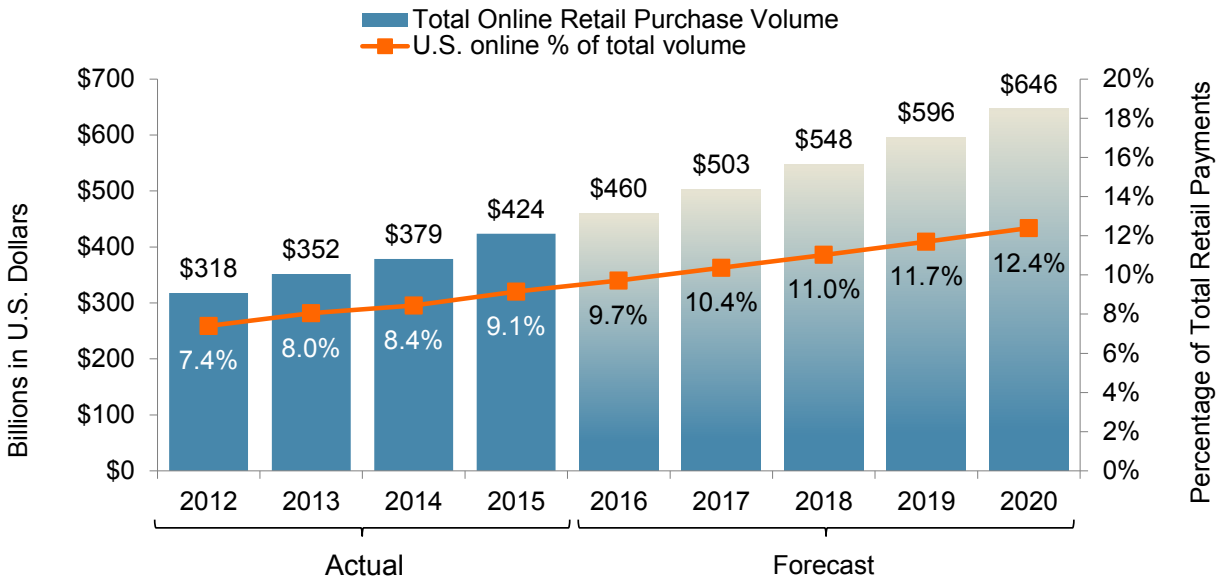
INTRODUCTION

Growth in E-Commerce and the Effect on Digital Goods Merchants

Over the past 20 years the Internet has played an increasingly larger role in the daily lives of consumers. Mirroring that trend, e-commerce has seen constant growth, both in absolute terms and as a proportion of total retail payments. As of 2015, e-commerce transactions made up 9.1% of the retail payment volume; it is expected to reach 12.4% by 2020 (see Figure 1). As e-commerce continues to evolve, it is bringing change to what types of products are being sold, and how they are marketed and delivered. This evolution, too, is challenging merchants' ability to manage fraud. This is especially true for newer segments of merchants that are thriving thanks to online and mobile channels, specifically digital goods merchants.

Growth in Online Retail Transactions Is Accelerating

Figure 1: Total Online Retail Purchase Volume, Actual and Forecast (2012–2020)



	2015	2015–2020	2020
Metric	Online total payments volume	Dollar growth in online total payments volume	Online total payments volume
Online retail purchases	$424B	$222B	$646B

Amenities like immediate product delivery, an easy checkout, and low false-positive rates have become table stakes. No e-commerce merchant segment faces more of a challenge from this new set of expectations than digital goods merchants, who are cautiously eager to capitalize on the growing e-commerce market (see *Changing Nature of Fraud* section, pg. 10). Digital goods merchants recognize that their ambition will be tempered by the need to find a balance between customer experience and fraud management. Merchants must walk a tightrope between the inversely related variables of consumer satisfaction and low fraud rates. And as the volume of digital goods transactions grows, so will expectations on the part of consumers for merchants to deliver products quickly in order to stay competitive.

THE CHANGING NATURE OF FRAUD: DRIVERS AND TRENDS

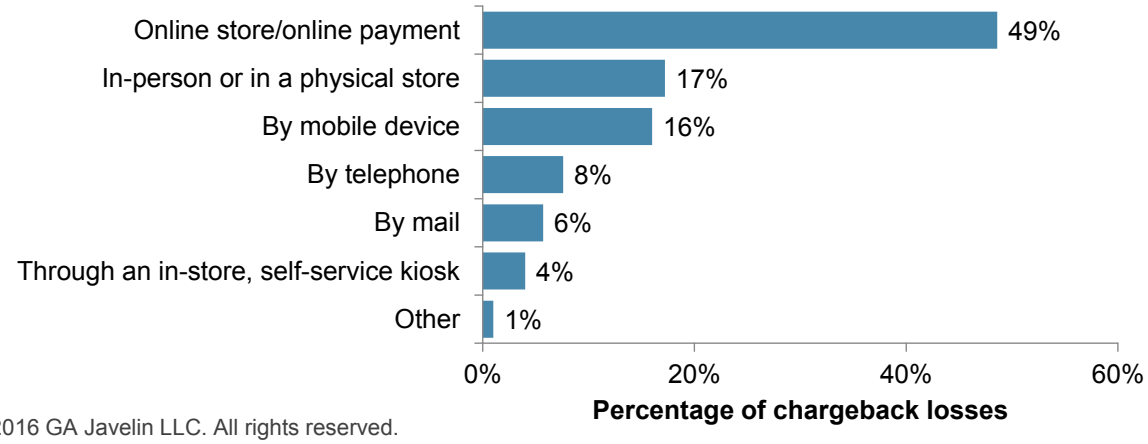
The Impact of EMV

The largest factor in the long-term growth of e-commerce fraud is the rapid growth of the e-commerce channel itself (see *Introduction* section, pg. 10). As the volume of e-commerce transactions increases, it becomes harder for merchants to discern between legitimate and fraudulent activity. Combined with other factors that effect greater anonymity, online channels have been increasingly attractive to fraudsters when compared with physical stores. Rather than risking being apprehended while committing fraud in-person, fraudsters are increasingly turning to online merchants where the risk vs. reward calculus is more favorable. The introduction of EMV in the U.S. is further increasing the risk and diminishing the reward for point-of-sale (POS) card fraud, motivating a further shift to e-commerce by fraudsters.

One year after the fraud liability shift — for merchants still not accepting EMV for eligible transactions — the anticipated surge in online channel fraud is beginning to manifest.[1] EMV proliferation eliminates the opportunity for fraudsters to use counterfeit cards at the point of sale. Armed with CNP data from compromised merchants, fraudsters are finding ways to avoid contending with the challenge that EMV presents at the point of sale. E-commerce merchants reported that 49% of their chargeback losses come from the online channel, roughly three times the amount of in-person fraud for this group — which will increase significantly as more merchants upgrade their POS terminals to accept EMV payment cards and their collective liability for fraud at the point of sale declines.

Online Channels Disproportionately Drive Fraud

Figure 2: Percentage of Chargeback Losses by Payment Channel



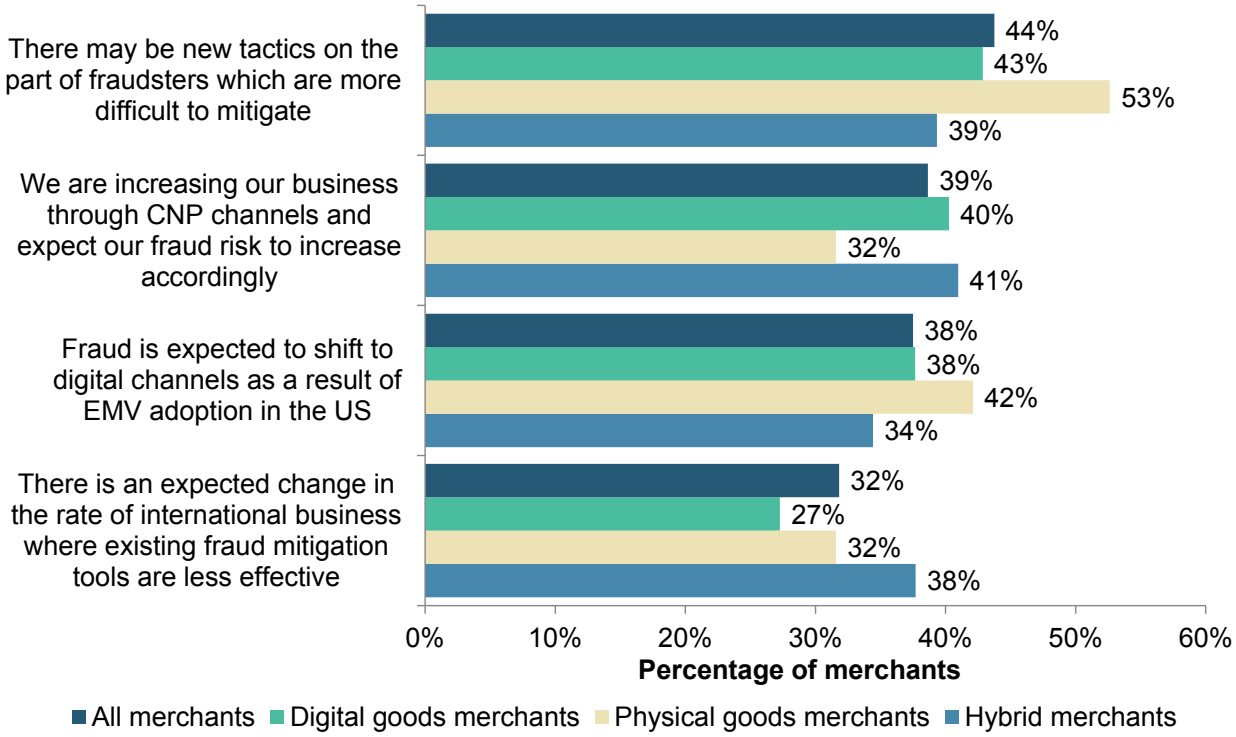
[1] 2016 Data Breach Fraud Impact Report, Javelin Strategy & Research, June 2016

Fraud Grows Alongside Overall Transaction Volume

The number and diversity of e-commerce merchants present fraudsters with a wealth of opportunity to challenge their creativity. While roughly 2 in 5 merchants agree that CNP fraud will increase as a result of EMV, the same number believes that CNP fraud will increase simply because they expect their online sales to increase (see Figure 3). With every retail sector now having an established presence in the online marketplace, the online channel is an increasingly attractive target, and fraudsters are directing their attention toward uncovering each and every unique opportunity to circumvent controls and defraud merchants.

Merchants Show Concern Over a Range of Factors Driving E-Commerce Fraud

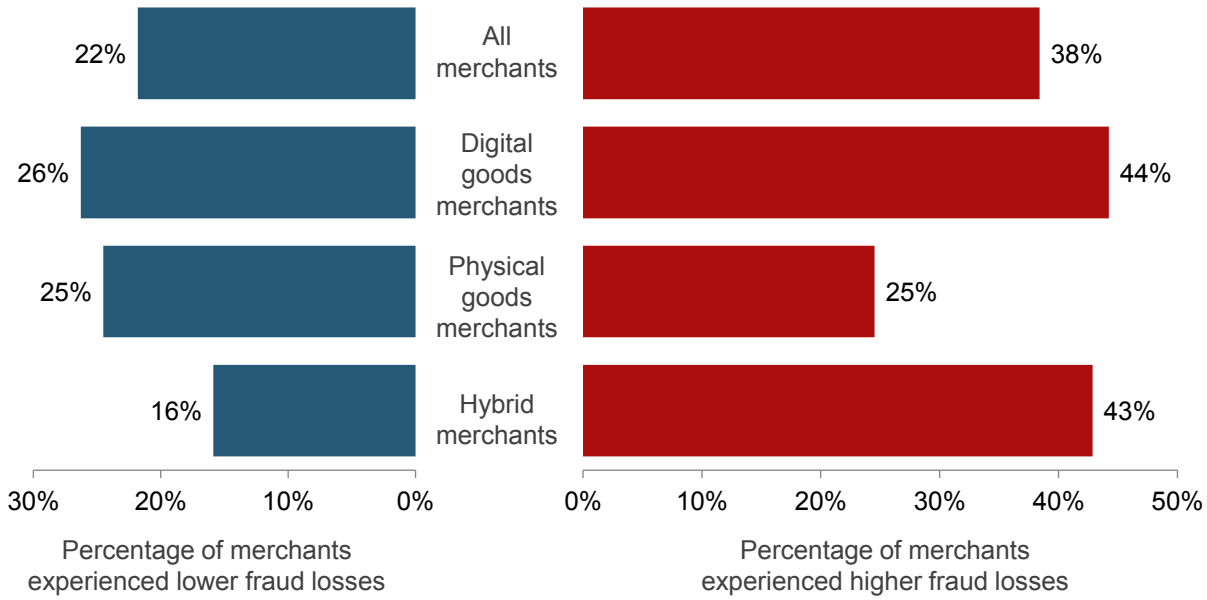
Figure 3: Merchant Concerns Over Fraud Drivers



Digital goods merchants' vulnerabilities in particular place them in fraudsters' sights all too frequently. Nearly half of digital goods merchants (44%) and hybrid merchants (43%) indicated that they experienced greater fraud over the past 12 months than they did in the preceding year (see Figure 4). This is, in part, a function of growth in the market as a whole, but it's greatly facilitated by the nature of delivering digital goods. With little window between payment and delivery, all authentication measures need to be completed either before the purchase is made or instantly upon payment. This precludes manual reviews, and without a physical delivery address, merchants lose important data points that can be used to verify identity.

Digital Goods Merchants Experienced the Greatest Increases in Fraud Losses

Figure 4: Change in Fraud Losses Over the Past 12 Months by Merchant Type



Complicating Fraud Management: Mobile Wallets and In-Store Pickups

Another aspect of how the retail experience continues to evolve is in facilitating easier transactions not only within but across channels, whether that is during the payment or delivery phase of a retail interaction. Two major initiatives that are leveraging technology to improve the retail experience include the mobile wallet and in-store pickups. Unfortunately, along with increasing convenience for consumers, these initiatives are introducing new ways for fraudsters to attack merchants.

Mobile wallets will allow fraudsters to bypass the restrictions imposed by EMV at the point of sale by provisioning compromised cards to the wallet. Rather than realizing the security promises of EMV, merchants are dependent on the identification and verification (ID&V) methods of the mobile wallet provider to ensure that the true accountholder is enrolling a card — and these ID&V methods tend to vary in strength. Ironically, the data used to provision cards to a mobile wallet are the same information used during CNP transactions (e.g., the primary account number, expiration date, and CVV2). Besides fraudsters being able to misuse data from EMV cards at the point of sale, there will be long-term ramifications for e-commerce merchants as mobile wallets begin to integrate with mobile shopping apps and browsers to facilitate online purchases.[2] Managing fraud from mobile wallets will add complexity to merchant operations, regardless of the channel in which they operate.

> "... As for digital channels, I think we are seeing more (mobile wallet) challenges than we would have anticipated. Apple and PayPal are very protected, but there are a lot of third-party wallets that allow a customer to enter an EMV card in them and that is higher than we expected."
>
> - Senior Executive, Physical Goods Merchant

Another prominent circumvention method for merchant fraud controls is the use of in-store pickups of online orders. This is often more effective than purchasing physical goods online for delivery to an address under the fraudster's control, as there is less risk that fraudsters will not receive the merchandise should the transaction not pass a validation check for delivery to their physical address. These schemes highlight trade-offs merchants face in providing customers these conveniences. Accepting customers' preferred payment types, and giving them flexibility over payment and pickup, open the doors to exploitation. For fraudsters looking to make the transition from the point of sale to e-commerce, in-store pickups are reducing the learning curve.

[2] The Evolution of Tokenization in a Mobile Payments Environment, Javelin Strategy & Research, December 2015

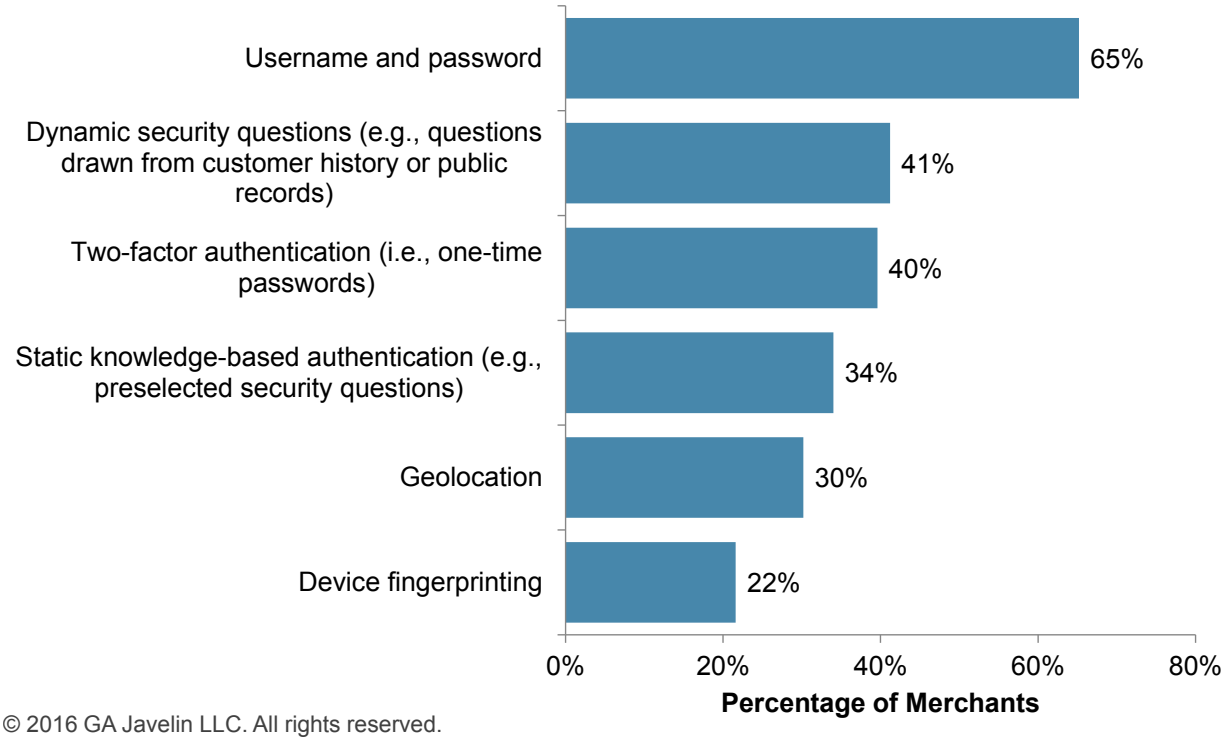
Account Takeover: Merchant Solutions Are No Match

Account takeovers are a particularly challenging breed of fraud for merchants. If customers are angered by having their cards erroneously declined, the negative feelings are compounded by being locked out of their accounts. The expectation of increased CNP fraud is galvanizing card networks to implement tokenization to secure cards over e-commerce channels.[3] A byproduct of closing this avenue for gaining access to card data is that it will push fraudsters toward remaining vulnerabilities that were once thought to be less convenient to exploit than stolen card credentials. This specifically includes taking over existing e-commerce accounts, placing merchants under increasing pressure to improve their authentication capabilities.

Unfortunately, merchants are still overly reliant on usernames and passwords to secure customer accounts. Fewer than half of merchants implement any single authentication solution beyond the standard account login credentials. Dynamic security questions (or knowledge-based authentication, also KBA) and two-factor authentication are gaining

Nearly Half of Merchants Employ Secondary Authentication

Figure 5: Authentication Methods' Usage Rates



[3] http://investor.visa.com/news/news-details/2015/Visa-Brings-Token-Security-to-eCommerce/default.aspx, accessed September 26, 2016

traction with 2 in 5 merchants using each of these solutions, but not all solutions are created equal in their ability to balance fraud prevention with customer experience (see *Technology Solutions* section for more details on dynamic KBA, pg. 27). While geolocation and device fingerprinting are particularly effective for digital goods merchants since physical address matching is not an option, all e-commerce merchants can benefit from reduced checkout friction, and these solutions form an invisible facet of the checkout process. Yet these solutions are used by less than one-third and one-quarter of merchants, respectively (see Figure 5).

> "We have in our system two factor authentication. So you know usually the person doesn't have a password, they're trying to sniff for the password. There's nobody in our system, our call center agents don't have the password. They have to reset the password, this two factor authentication is part of it. So I think we've done a lot to mitigate that 'cause it's just hard to break through those things. I think that there's certainly always a risk or an exposure."
>
> - Co-founder,
> Digital Goods Merchant

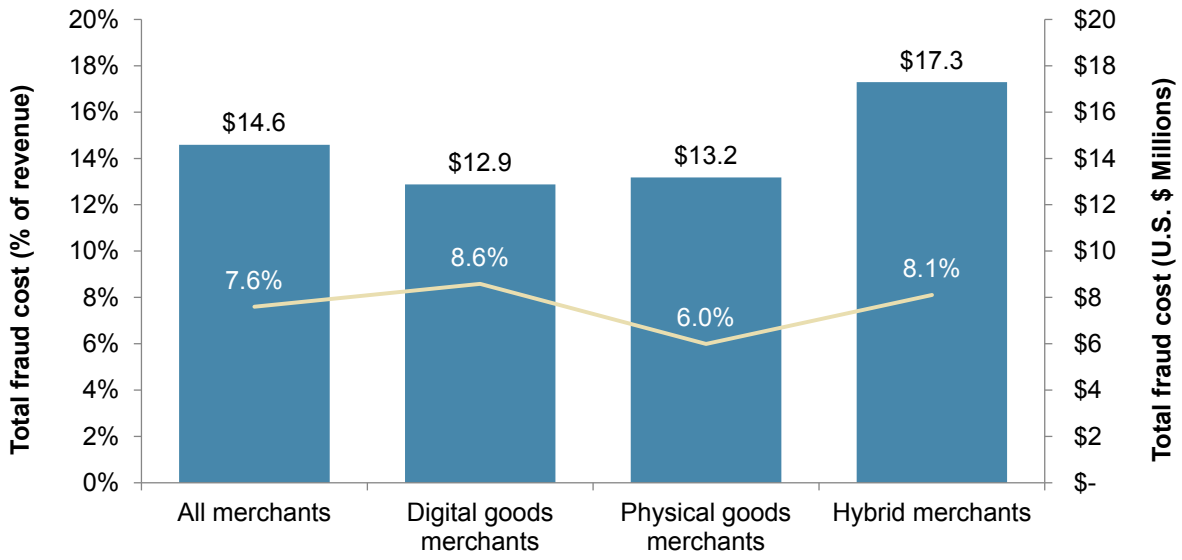
QUANTIFYING THE FINANCIAL IMPACT OF FRAUD

The financial impact of fraud is more complex than many merchants may realize, but it must be accurately assessed in order to determine the appropriate level of investment for managing risk. Merchants run the risk of miscalculating the total financial impact of fraud if they fail to consider all of its requisite, though not always readily apparent, components. The most obvious cost merchants face from fraud is direct chargebacks, but this is just one small part of the total bill — accounting for only 7% of all fraud-related costs. In order to combat fraud both proactively and reactively, merchants implement costly fraud management tools. Software and hardware provide the initial tools, but human capital is often required to manually review suspicious activity. Combined, these fraud management costs account for a staggering 74% of fraud-related costs, but the cost analysis cannot end with fraud management and chargebacks.

Furthermore there are the oft-unconsidered costs related to false positives, which are legitimate transactions that are declined because they appear fraudulent, negatively affect a merchant's bottom line and contributing to 19% of fraud-related costs (see Appendix, Figure 19). Not only do they prevent the sale, but there is also serious damage to the merchant's brand as customers feel frustrated with the rejected transaction. In aggregate, all of these factors contributed to the loss of 7.6% of total revenue for e-commerce merchants in 2016 (see Figure 6).

In Total, Fraud Costs an Average E-Commerce Merchant 7.6% of Revenue

Figure 6: Fraud Management Expenditures, Chargeback Losses, and False Positives

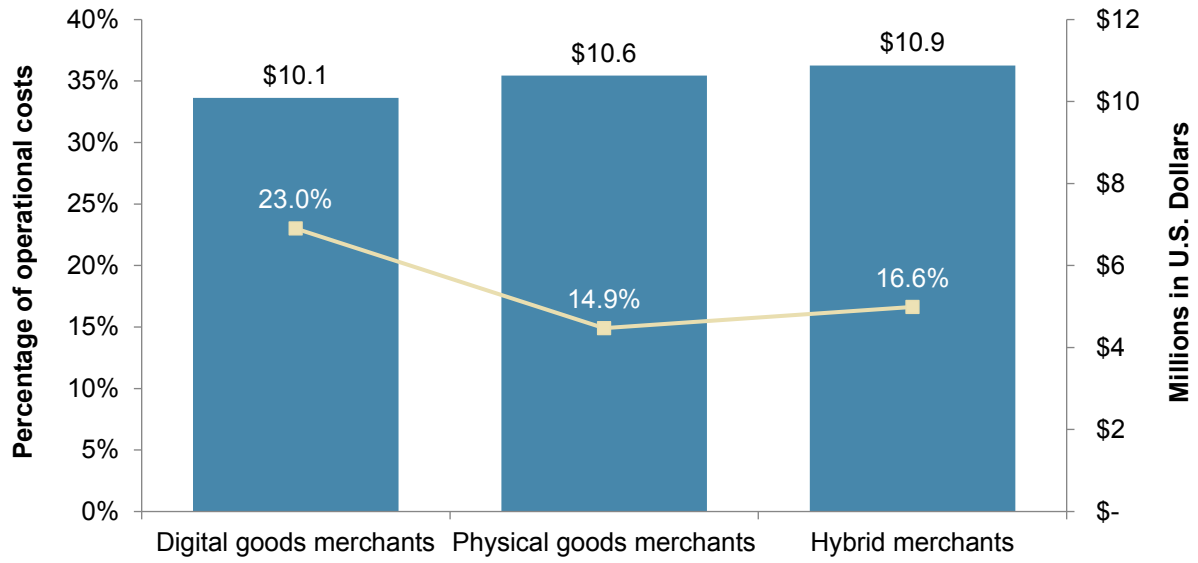


Giving up 8.6% of total revenue in 2016, digital merchants have the highest proportional cost of fraud. In addition, they spend the greatest percentage of their operational costs on fraud management, at 23% (see Figure 7). One reason for these higher rates resides in their stringent limitations in how they manage fraud due to their product and delivery models. With physical goods a merchant receives a physical address, which is highly useful for determining the risk of the transaction. For instance, some addresses can immediately be flagged as fraudulent if they have previously been used to commit fraud. Digital goods do not need a shipping address to be processed. Another limitation of digital goods is that the transactions are expected to be processed immediately. Unlike physical goods, which require time to reach the customer, digital goods can be sent instantly.

Hybrid merchants encounter unique obstacles when it comes to fraud, losing 8.1% of their revenue to fraud in 2015 and spending 16.6% of their operational costs on fraud management. Some hybrid merchants may start off as physical goods merchants, but expand their business to include the sale of digital goods such as gift cards. Regardless of how these merchants entered the market, managing fraud involving both digital goods and physical goods is an obvious challenge. Without the ability to specialize in identifying and managing fraud related to a single type of good (and delivery method), hybrid goods merchants can face high costs in mitigating fraud schemes involving both physical and digital goods.

Digital Goods Merchants Invest Nearly a Quarter of Operational Cost in Fraud

Figure 7: Fraud Management Expenditures in Total Costs and Percentage of Operational Costs, by Merchant Segment



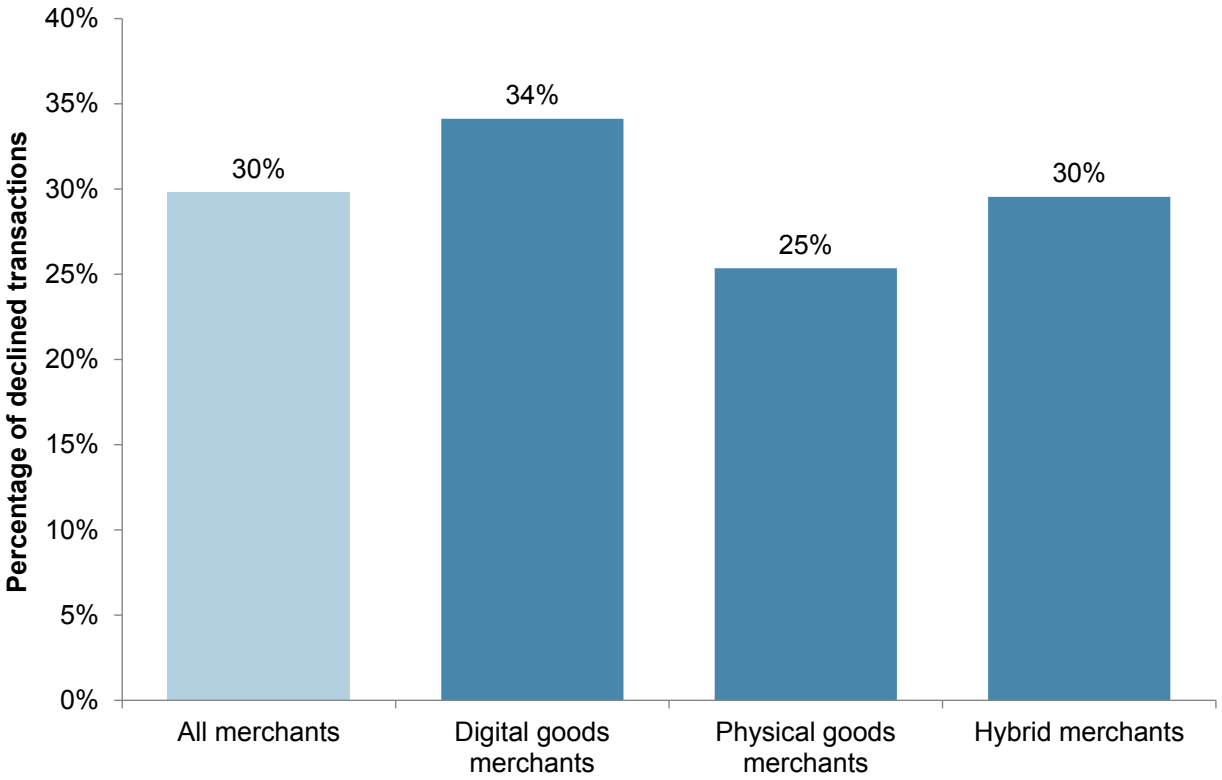
PRESERVING THE CUSTOMER EXPERIENCE

False-Positive Declines: The Epitome of Checkout Friction

Arguably worse than experiencing fraud is losing the transaction and the customer because overly sensitive controls are blocking legitimate shopping activity. A staggering 30% of all declined transactions are later determined to have been mistakes (See Figure 8). This percentage is likely understated, as it is impossible to determine the fraud status of all declined transactions, especially if the customer gives up without making contact.

1 in 3 Declines Is a False Positive

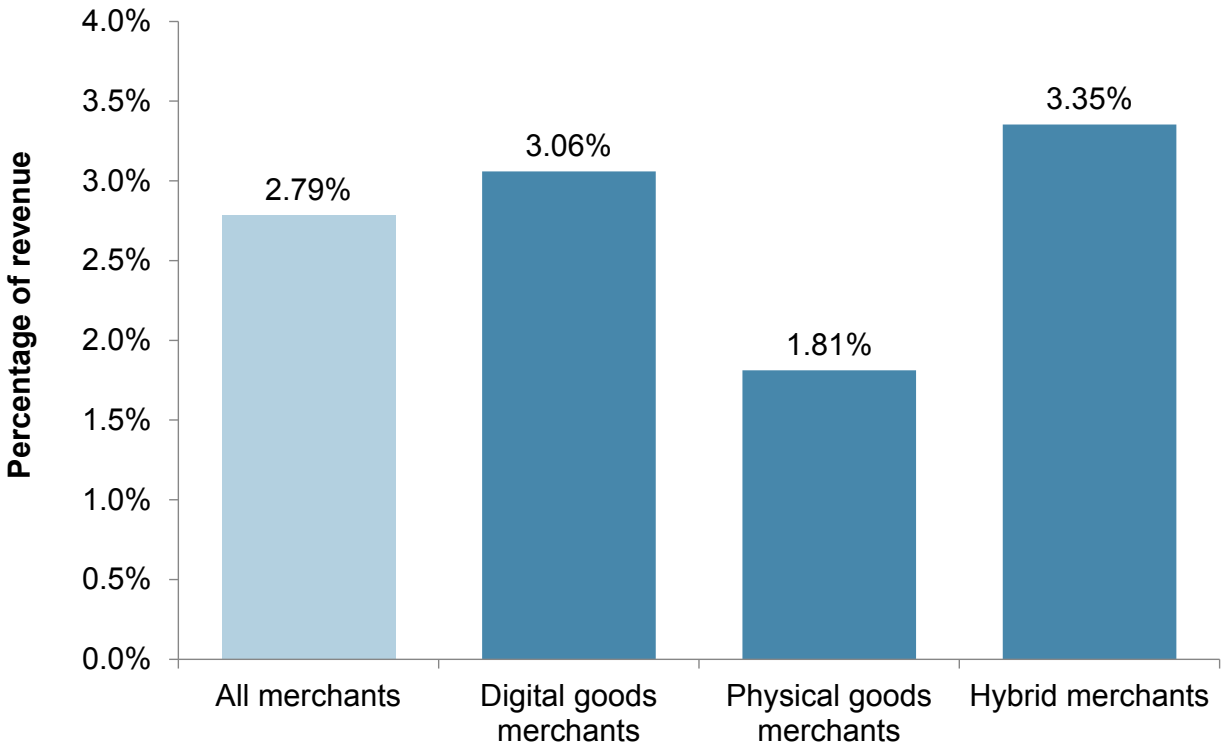
Figure 8: Percentage of Declined Transactions Found to Be False Positives



Dollars lost to false-positive declines eclipse the amount of chargebacks by more than 5 to 1. The average percentage of revenue lost to false positives is 2.79% for all merchants (compared with 0.52% lost to chargebacks), with physical goods merchants experiencing the lowest false-positive losses, at 1.81%, and hybrid merchants facing the highest, at 3.35%. Furthermore, there may be a multiplier effect from the losses to false-positive transactions, as this inconvenience undoubtedly affects customer loyalty and the long-term value of that relationship. Clearly, fraud prevention can be a double-edged sword, as being overly cautious or using the wrong metrics can result in sizable losses. (see Figure 9)

Roughly 3% of Sales Revenue Is Lost to False Positives

Figure 9: Losses From False-Positive Declines as a Percentage of Revenue



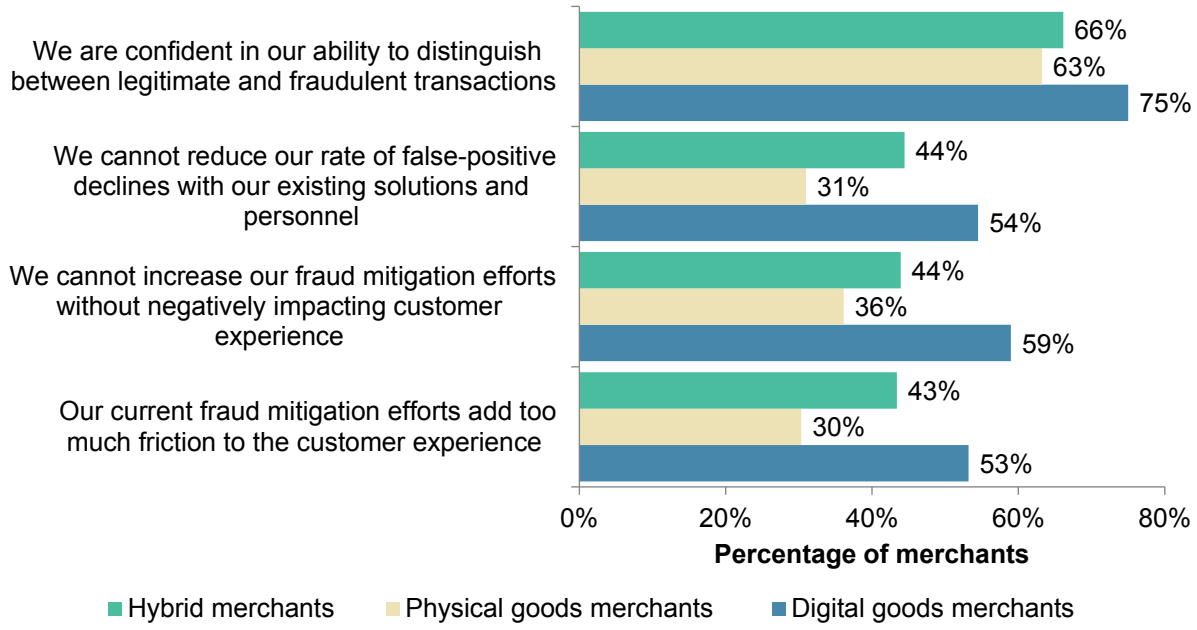
New Threats Risk Increasing the Rate of False Positives

Merchants express plenty of confidence in their ability to combat fraud at the present moment. But although they believe they have a handle on current fraud tactics, they feel they have reached a delicate balance in terms of weighing fraud prevention against customer experience friction. While this may represent equilibrium at present, it also signals that merchants are constrained from ramping up controls at a time when rapidly changing fraud trends require the flexibility to adapt.

> "There is an overarching trend that the scale of attacks that are occurring are becoming much larger. My hypothesis is that fraudsters are doing larger, more spread out attacks to see what (will go) through. They are undertaking $50,000 attacks to try and steal a million dollars. Economies of scale to do a large spread of attacks. Makes sense as organizations may catch some of it, but you can't get all of it."
>
> - Senior Executive, Digital Goods Merchant

Merchants Believe They Are Controlling Fraud as Best They Can Without Affecting Customer Experience

Figure 10: Merchant Attitudes About Their Current Fraud Practices



Merchants already face high losses from false-positive declines, and roughly one-third to one-half of merchants believe that they cannot further reduce their false-positive rates with existing solutions. Digital goods merchants are the most likely to report that they are not only unable to further reduce false positives, they're also negatively affecting the customer experience as a result of the fraud controls they are using (see Figure 10). This is another set of factors that make identifying best practices, leveraging tools that are optimized for new fraud trends, and cost-effective outsourcing imperative for digital goods merchants.

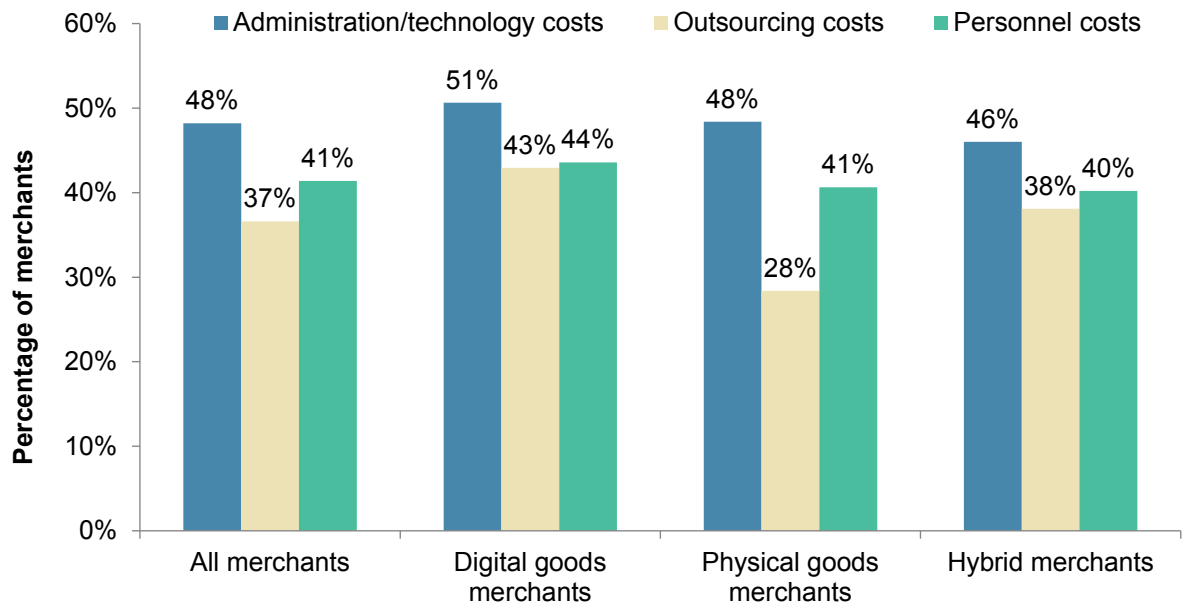
FRAUD MANAGEMENT: FINDING THE RIGHT APPROACH

Effective fraud management requires trade-offs, not only between convenience and security for the customer, but also in the types of solutions used. There are two main areas of investment and management for merchants seeking to tackle fraud on their own: 1) people to identify, respond to, and resolve fraud situations (leveraged by 41% of all merchants), and 2) technology to automate those processes (leveraged by 48% of all merchants). For many merchants, managing fraud risk and its aftermath are tasks best left to third-party specialists — 37% of merchants outsource these tasks. (See Figure 11.)

> "What we do is automated and we tend to be super conservative. So security is so embedded in everything we do. While I would assume at some point we're gonna have an incident, we do whatever we possibly can to minimize those threats and let them go to one our competitors."
>
> - Co-founder, Digital Goods Merchant

Outsourcing Appeals Most to Digital Goods Merchants

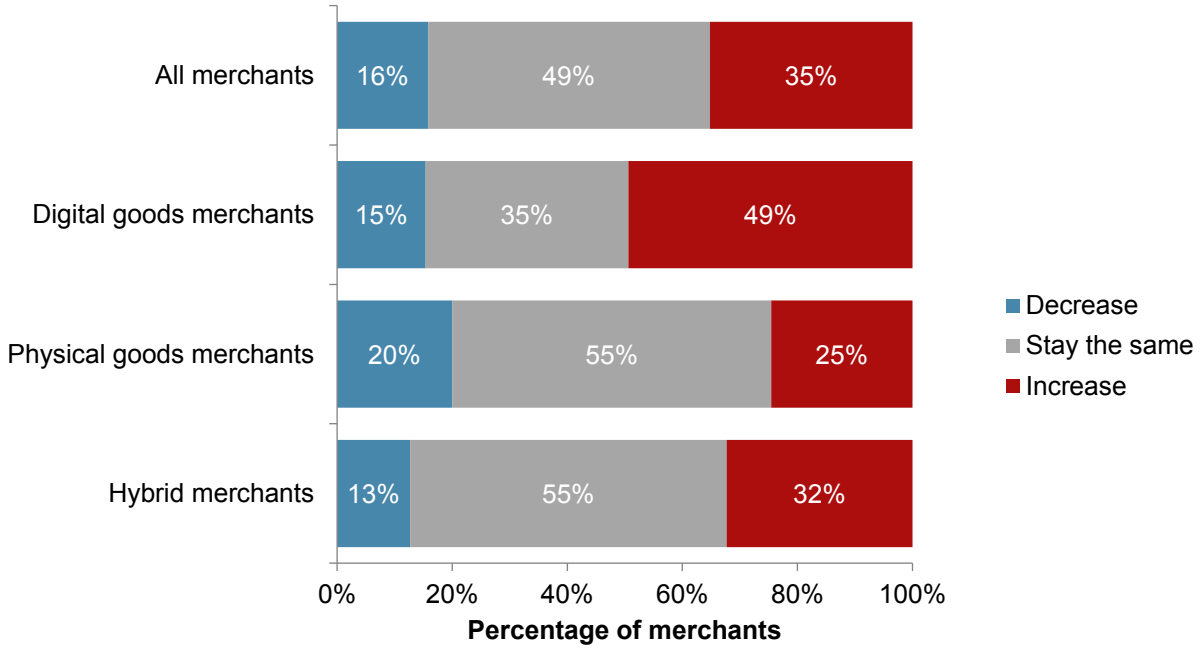
Figure 11: Fraud Mitigation Expenditures Applicable to Each Merchant Segment



Digital goods merchants face some of the most significant fraud risks as their businesses grow, which in turn influences their investments. The ease with which criminals can resell digital goods on the Internet, compared with the logistics needed to acquire and resell physical goods, makes these merchants a prime target. Further still, with no need to physically collect goods, fraudsters can make better use of channel-specific fraud tools like bots to attempt to steal massive volumes of transactions in short periods of time. These stolen virtual goods can then be fenced with far greater ease than physical goods, thereby easing the logistical challenge for fraudsters. The complexity in managing fraud due to these types of inherent risks facing digital goods merchants is evidenced by the 49% of this segment that is planning to increase fraud expenditures over the next 12 months, compared to 55% of physical goods merchants who are maintaining their current fraud expenditures (see Figure 12).

More Than Half of Digital Goods Merchants Plan to Boost Fraud Spending

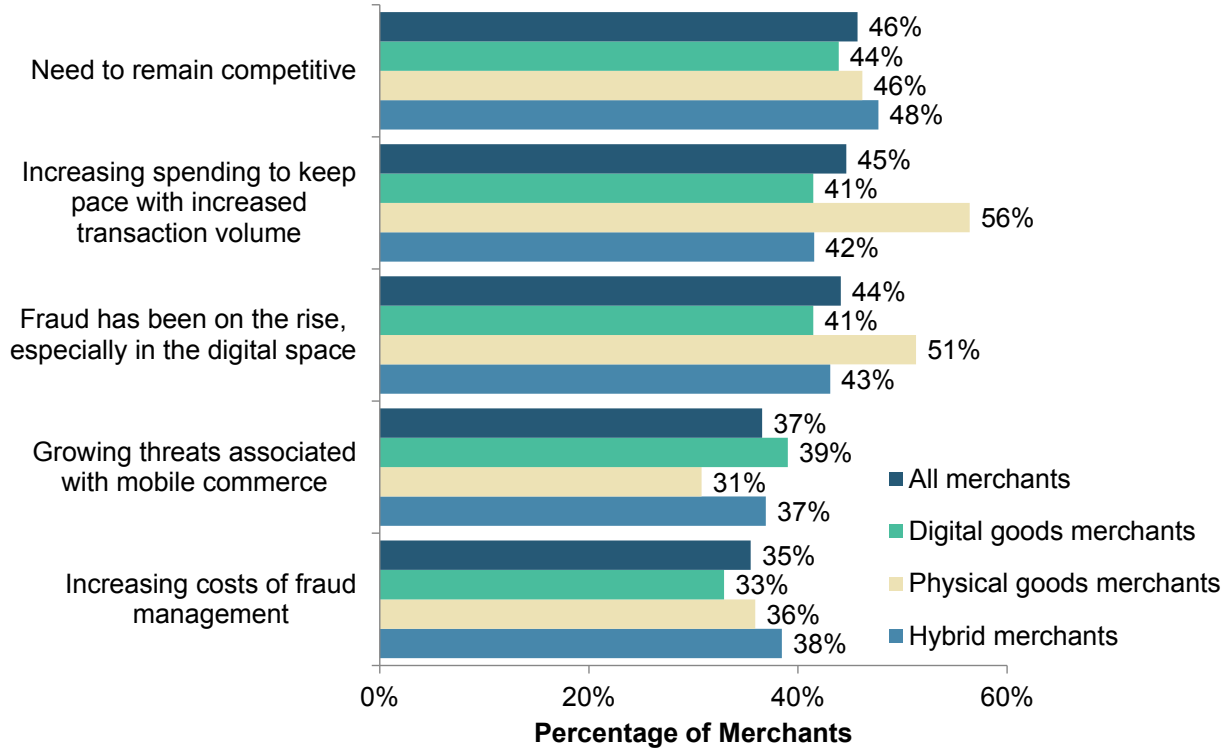
Figure 12: Expectations About Change in Fraud Expenditures Over the Next 12 Months



Regardless of how they manage fraud risk — whether internally or through outsourcing — merchants that plan to increase fraud-related expenditures said the top driver is the need to remain competitive (see Figure 13). This means stemming the fraud losses and enabling more legitimate transactions to increase profitability, without eroding the customer experience. The second driver cited was the need to keep up in a high-growth market where transaction volumes continue to grow. The third driver was the need to stem the risk of CNP fraud, which is expected to rise at twice the rate of POS card fraud by 2019 and which will be bolstered by increasing data breaches involving compromised CNP data.[4]

Spending Increases Driven by a Variety of Concerns

Figure 13: Expectations About Change in Fraud Expenditures Over the Next 12 Months



[4] 2016 Data Breach Fraud Impact Report, Javelin Strategy & Research, June 2016

Throwing People at the Problem

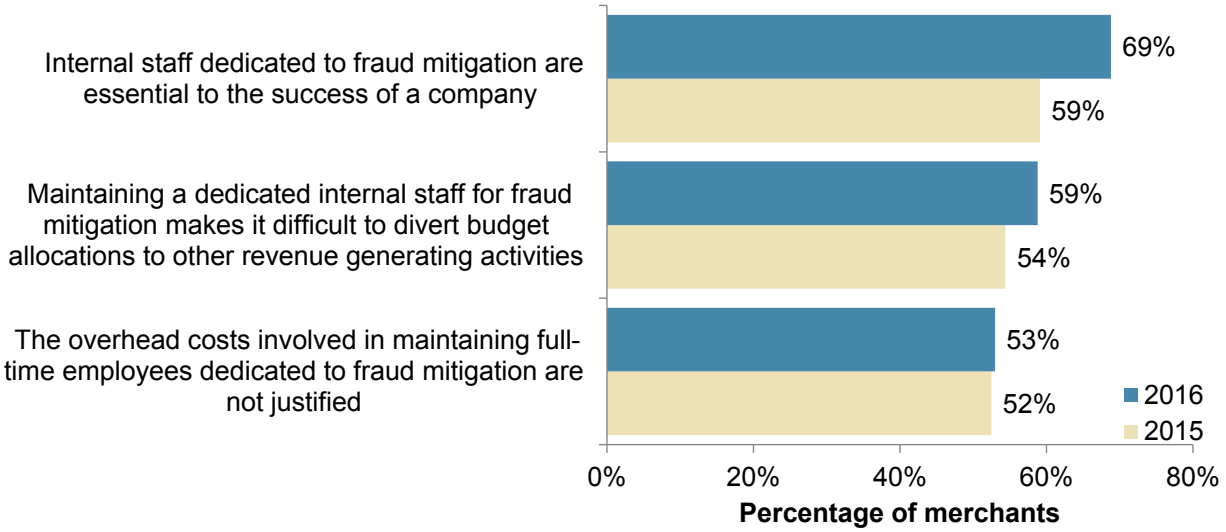
Technology is only part of the equation in managing fraud. Having the right people also matters, though identifying and cultivating a fraud team can come at a considerable cost. Sixty-nine percent of merchants believe that internal fraud mitigation resources are essential to their business, up from 59% last year. However, finding, hiring and training fraud staff is challenging and expensive, leading 53% of merchants to indicate that maintaining staff dedicated to fraud mitigation is not justified. In finding and hiring the right people, some merchants incur opportunity costs, indicating that while a fraud management staff is essential to their business, they can't necessarily afford it. A significant challenge for 59% of merchants is the lack of flexibility their fraud budget gives them to make investments in other parts of their business, particularly revenue-generating services. (See Figure 14.)

> "It's people always and technology first. If you don't have the right people then the technology is useless. I've seen it time and time again – you have great tech, but the wrong people."
>
> - Senior Executive, Digital Goods Merchant

Training fraud management staff is critical because criminals take advantage of merchants that are unaware of new fraud schemes. Despite the evolving nature of fraud, 65% of merchants considered staff training for fraud mitigation to be very expensive, almost unchanged from last year (see Figure 15). Since effective fraud mitigation is considered by most merchants to be critical to the success of their

Internal Fraud Staff are Increasingly Viewed as Essential, but Reducing Growth Opportunities

Figure 14: Attitudes About Training Staff in Fraud Management (2015–2016)



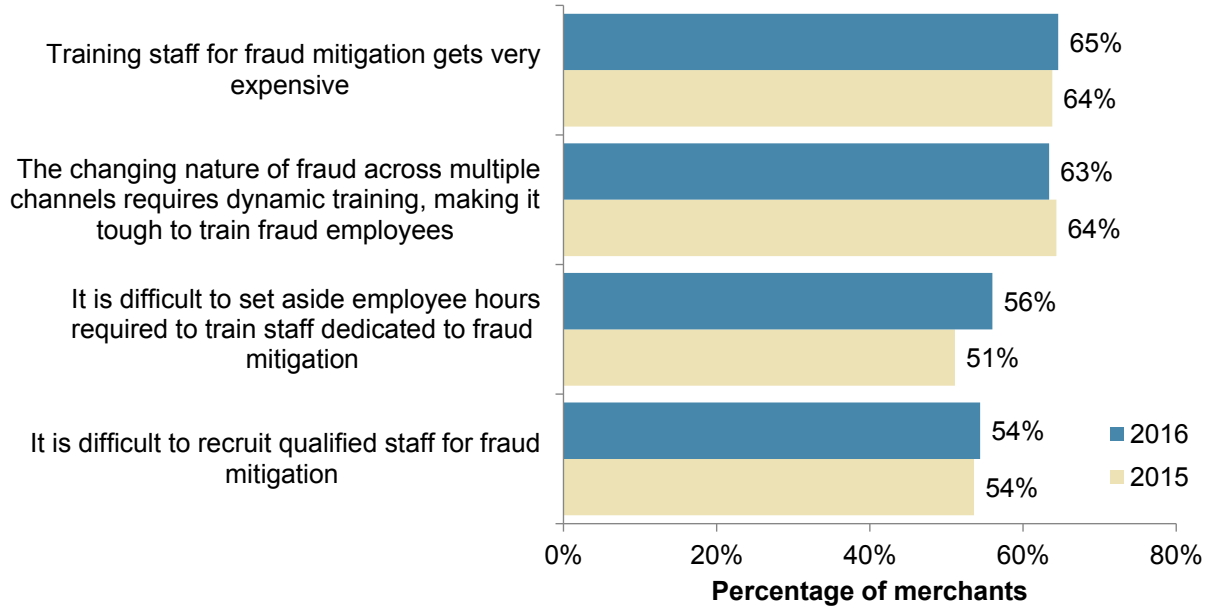
business, this disconnect indicates that merchants may not feel that they are getting the most out of their investments in fraud management. This could be a function of failing to adapt quickly enough to realize the benefit of training, as 63% of merchants indicated that it is difficult to keep their employees up to date on emerging schemes.

Between growing transaction and fraud volumes, 56% say fraud mitigation training time is difficult to set aside. Training time means taking staff away from alert queues and research to identify fraudulent transactions, further slowing merchants down on a problem they already feel behind on.

The actual costs related to salary and benefits, when confronted with a limited pool of qualified candidates, are likely another factor driving dissatisfaction in fraud management investments. More than half (54%) of merchants also indicated that it is difficult to recruit qualified staff to mitigate fraud (see Figure 15). The competition is fierce for skilled workers in a recovering economy. Furthermore, good fraud analysts must possess certain qualifications, including analytical skills, expertise in payments and fraud matters, interviewing skills, and critical thinking. In most cases, good customer service representatives are graded on their ability to quickly solve an issue to a customer's satisfaction, which fraudsters use to their advantage.

Rapidly Changing Fraud Poses Training Challenges

Figure 15: Attitudes About Fraud Management Staff (2015–2016)



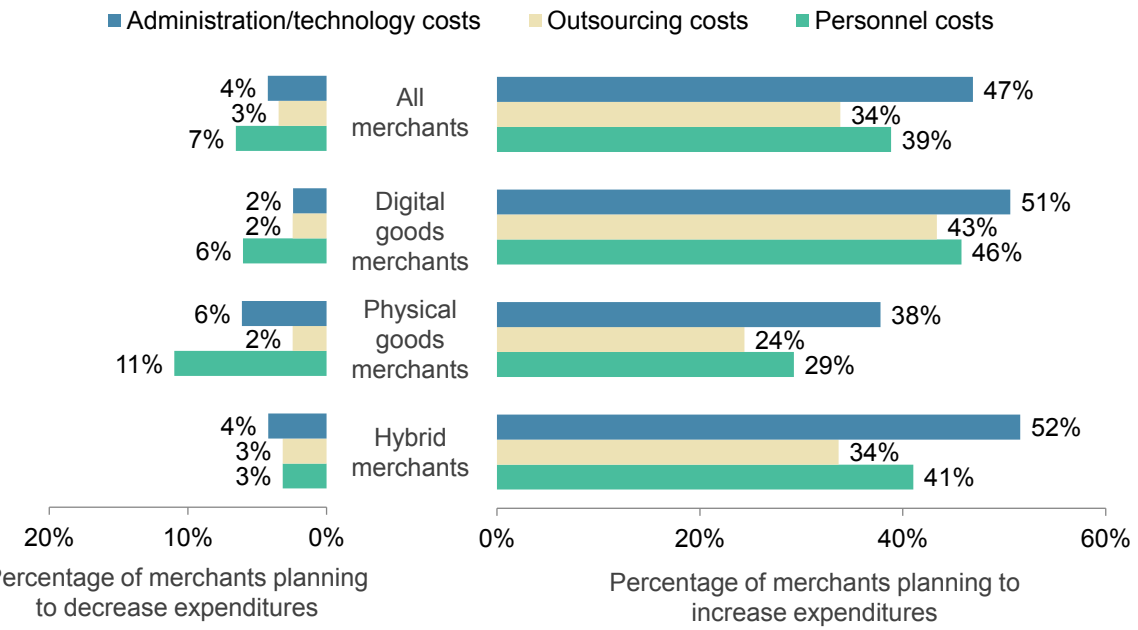
Technology Solutions: The Old Gods and the New

Technology investments are critical to effectively managing fraud, interconnecting the customer information with the payment risk and the delivery of the goods. This begins with the process of enrolling and authenticating customers during their initial interactions with the merchant. Merchants can leverage internal and external data sources to feed a risk engine that assesses the likelihood of fraud in a purchase. More importantly, they enable a workflow for the fraud team to review and adjudicate high-risk transactions. This is a complex process as technology management requires understanding the landscape of solutions and determining which pieces of technology meet the business needs. The solutions need to be integrated and managed over time, which requires technology resources to build out and maintain the applications. Risk engines require regular tuning based on real-time feedback from changing fraud schemes, which require data analysis resources.

Digital merchants are leading the pack across the board when it comes to a planned increase in fraud-related expenditures over the next year — including investments in people, technology, and outsourcing (see Figure 16). Yet more than any other area, this is where more digital goods merchants are committed to increasing their technology spend (51%). Physical goods merchants have more time, sometimes up to

Digital Goods Merchants Are Most Aggressive About Increasing Spending in All Areas of Fraud Management

Figure 16: Merchants to Increase/Decrease Fraud Management Expenditures



24 hours, to make a decision about a customer's order before shipping it out the door. Digital merchants need to make that decision in milliseconds while the customer, or criminal, is waiting to download the product.

Physical merchants have standard data feeds to verify the delivery address and understand the level of risk associated with known drop sites used by fraudsters to collect their ill-gotten gains. Digital goods merchants, on the other hand, are limited to relying on channel-oriented data, such as device and session information. Much of this data are relatively recent, compared with physical address information, and need to be ranked by risk and fed into the processing stream before authorization. Digital merchants are thereby required to increase their fraud technology spending to access and integrate new solutions that have to work together in real time.

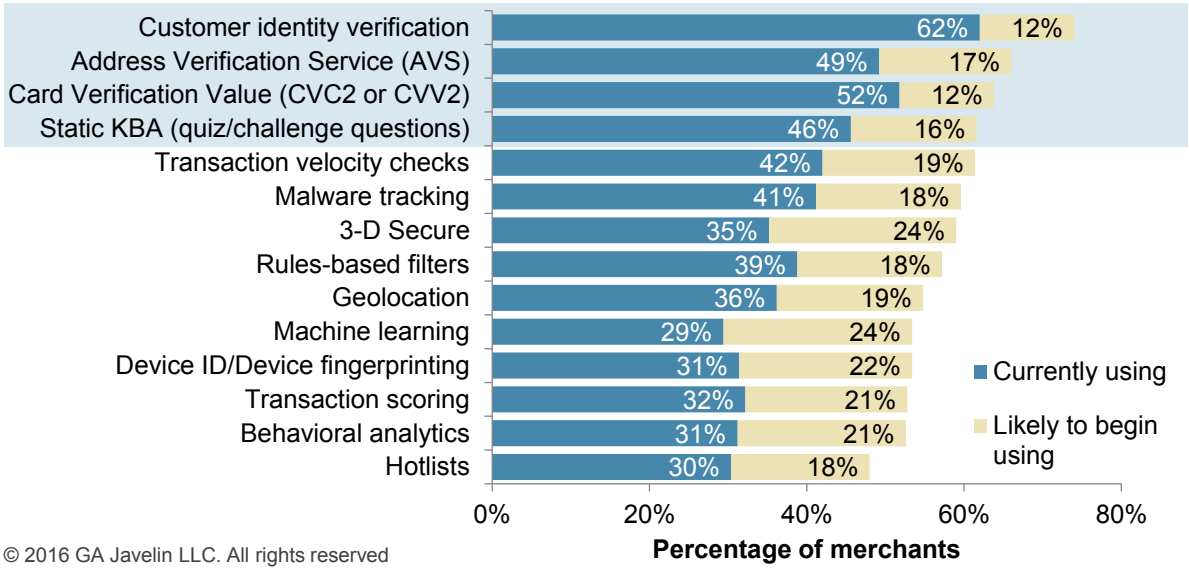
> "We're not spending any more as the system we have scales. But will that be a true statement for everyone out there. The more material number is that some companies may take some very large fraud hits. If they are public companies it could affect perception."
>
> - Senior Executive, Digital Goods Merchant

Among the different fraud mitigation solutions available today, the four most frequently used by merchants are based on validating static data elements (see Figure 17), which are easily sidestepped by fraudsters:

- Address verification service (AVS) and card verification value (CVV2/CVC2/CID) are card-oriented solutions that rely on data elements that can be gleaned by fraudsters online, via

Validation of Static Data Elements Tops Fraud Solution Use

Figure 17: Use of Security Solutions, With Expectation of Adoption in the Next 12 Months



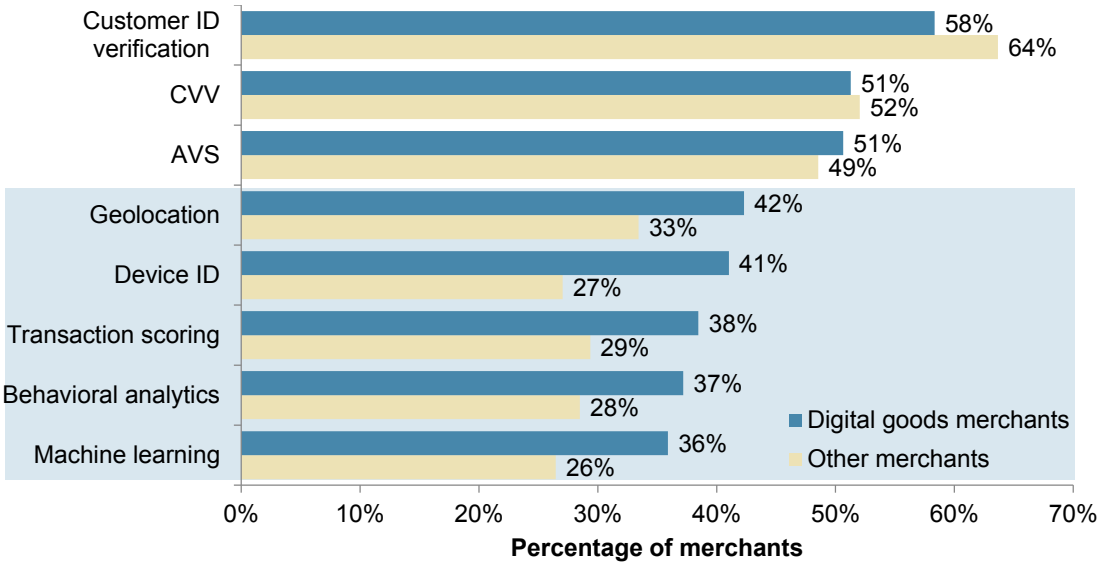
malware or a data breach — the address of the cardholder or a three- or four-digit value printed on a card and entered during CNP transactions. Customer identity verification is the process of checking that the personally identifiable information (PII) provided by the customer is accurate, which may be ineffective for mitigating fraud involving digital goods where physical addresses are less of a factor.

- Static knowledge-based authentication (KBA) involves asking customers to add answers to questions they choose, which it can be of limited security value as demonstrated by the 20% of Google users who had "pizza" as the answer to the question "What is your favorite food?"[5]
- Superior from a security perspective, dynamic KBA can leverage public and nonpublic data sets for information that is more difficult for a criminal to access based on research. Unfortunately, as the questions may go back over a long period of time, the answers may be difficult for customers to recall, negatively affecting the customer experience by contributing to false positives and lost transactions.

Digital merchants are adopting next-generation tools faster than physical merchants (see Figure 18). This is not surprising as physical merchants are shipping goods to a physical address, whereas digital goods merchants are shipping data to a device — so it helps them to understand that device as much as possible. E-commerce merchants, and digital goods merchants especially, are investing in systems that analyze data from a consumer's device, online session, and

Digital Goods Merchants Turn to Lower Friction, Real-Time Tools

Figure 18: Use of Solutions by Digital Goods Merchants, Other Merchants



[5] https://techcrunch.com/2015/05/21/google-study-shows-security-questions-arent-all-that-secure/, accessed September 20, 2016

transaction behavior to build a profile of the customer. New customer behavior data are fed into transaction scoring, behavioral analytics, and machine learning systems to calculate risk scores in milliseconds.

Digital goods merchants are often early adopters of systems that manage multiple data inputs and complex calculations. This is a practical necessity because digital goods merchants have very little time to make a decision on a customer's transaction before delivering the goods. And the more data a merchant collects the better place it's in to manage the chargeback process. Creating connections between chargeback processing and customer activity can reveal that a customer used the same IP address for the transaction in question and for legitimate purchases in the past, for example. As these technologies become more widely used, though, criminals will increasingly challenge them, spurring the need for new solutions and additional investments from merchants.

> "The integration on the website grabs the order information, uses the IP address and uses that for the order to confirm location vs. order address. There are rules in place to approve, review, or decline the order – it all happens in seconds. It's effective, but I'm not going to say it's foolproof."
>
> - Co-founder,
> Physical Goods Merchant

Outsourcing Fraud Management

In a perfect world, fraud management would not be an expense for merchants. But the reality is that merchants have a choice between building and managing fraud expertise and solutions internally or working with a third-party service provider. In-house fraud and technology management gives merchants more control over their resources and investments. On the other hand, the value of outsourcing is reducing the cost fluctuations associated with fraud management and losses, and allowing merchants to invest in differentiating their business from the competition. Yet not all e-commerce merchants will benefit equally. To reach the decision on whether or not to outsource, merchants must consider all the financial and opportunity costs involved and particular to their business.

Merchants are of two minds on the necessity of an internal fraud team and the significant challenges it presents — with more than half viewing it as necessary and a similar proportion considering the investment as too great (see Figure 14). This is not surprising as hiring the right people and integrating the right technology are only the first steps. Merchants must subsequently maintain and upgrade their technology and processes over time, and respond to new and evolving fraud threats.

While physical goods merchants are easing their investments in fraud mitigation, digital goods merchants are racing to invest in new technologies to

keep ahead of fraudsters. Digital goods merchants are in the best place to take advantage of outsourcing their fraud management. Third-party service providers can scale their technology investments and human resources in ways that are difficult for an individual merchant. Service providers can also leverage the experiences of all the merchants they serve for the benefit of each — this is the power of consortium data. If a criminal targets one merchant with a fraud scheme, the knowledge of the device, IP address, or shipping address can be used to stop a transaction when it is attempted at another merchant.

Outsourcing fraud and technology operations creates scale that can accommodate fluctuations in transaction and fraud volume. It is much easier for a merchant to scale the fee to a third-party service provider when transaction volumes rise and fall than to hire and manage trained staff — this can include the ebb and flow associated with the holidays or the expected growth in CNP fraud (see *The Changing Nature of Fraud* section, pg. 10). Staying abreast of the latest software, analytic models, and rules is challenging. That is in addition to determining the efficacy of new data and authentication solutions that continue to come into the market, and performing the software integrations and ongoing technical management. Fraud management outsourcing can level the playing field so merchants can compete on their unique value propositions.

CONCLUSION

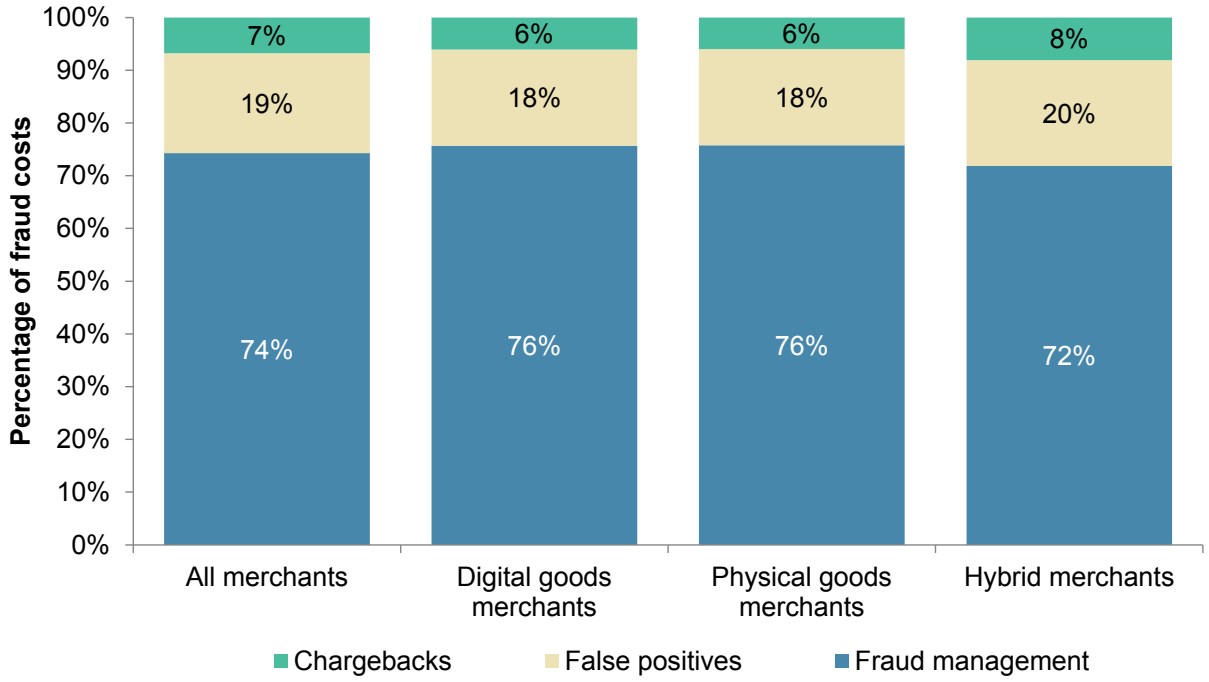
A rebounding economy, new products and services, and greater convenience are accelerating growth in online transactions. Merchants with a presence in the digital channel stand to benefit immensely from this trend, but it also brings tremendous risks. Forced by EMV closing opportunities for fraud at the point of sale, fraud is increasingly moving online. To detect and mitigate this threat, merchants must navigate a complex web of solutions to find the right approach — one that does not sacrifice profitability and erode customer experience for the sake of security.

In light of the increasing risk, digital and hybrid merchants are expanding their technology investments. When the costs of these planned technology investments are considered alongside the expected growth in expenditures for fraud management staff, outsourcing some or all fraud management can be a viable alternative that enables merchants to focus more on their go-to-market strategies. For those e-commerce merchants that invest in digital data and analytics, they will reap the rewards of improved customer experience, reduced chargebacks, and lower fraud staffing levels. Given the dynamic nature of fraud, regardless of the path that merchants choose to mitigate fraud, there will be new trends that test their organization and capabilities for years to come.

APPENDIX

Majority of Fraud Costs Spent on Management

Figure 19: Breakdown of Fraud Cost Types as a Percentage of Total Costs



METHODOLOGY

In June 2016, 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 500 e-commerce merchants earning $1 million or more annually, falling into key merchant segments:

- 156 merchants selling only digital goods
- 155 merchants selling only physical goods
- 189 hybrid merchants, selling both types of goods

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

ABOUT JAVELIN STRATEGY & RESEARCH

Javelin Strategy & Research, a Greenwich Associates LLC company, is a research-based consulting firm that advises its clients to make smarter business decisions in a digital financial world. Our analysts offer unbiased, actionable insights and unearth opportunities that help financial institutions, government entities, payment companies, merchants, and other technology providers sustainably increase profits.

Authors: Al Pascual, Research Director and Head of Fraud & Security
Kyle Marchini, Analyst
Sarah Miller, Senior Analyst – Custom Research & Operations
Mike Urban, Senior Advisor

Publication Date: October 2016

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 Portland, Vesta's operations span the Americas, Europe and Asia. For more information, visit trustvesta.com.