LexisNexis®
RISK SOLUTIONS

ANNUAL REPORT

2016 LexisNexis® True Cost of Fraud℠ Study

Remote Channels Continue to Get Hit Hard by Fraud; a Multi-Layered Approach Can Help.

MAY 2016

Table of contents

Introduction 4
Executive Summary 5
Overview 5
Key Findings 5
Recommendations 6
General Fraud Trends 7
Indicators of a Growing Problem 7
Remote Channels Hit Harder 9
Reaction to These Trends 13
What's Being Done about These Trends 15
Large Remote Merchants Solutions Use 15
Less Than Optimal Resource Use 18
Current Solutions Many Not be Ideal 20
The New Way Forward 23
Methodology 25
Appendix 26

Table of figures

Figure 1: Cost per dollar of fraud losses by year (2010 – 2016) 8
Figure 2: Average number total / successful fraud attempts per month (2012 – 2016) 8
Figure 3: Fraud as a percentage cost of annual revenues (2013 – 2016) 9
Figure 4: Cost per dollar of fraud losses per channel by year (2015 – 2016) 9
Figure 5: Percent of successful fraud transactions by debit/credit card (2015 – 2016) 10
Figure 6: Average # total / successful fraud attempts per month by channel 11
Figure 7: Fraud as a percentage cost of annual revenues by merchant type/channel 11
Figure 8: Distribution of fraud methods during past 12 months 12
Figure 9: Percent currently allowing / considering mCommerce 12
Figure 10: Top challenges selling through online/mobile channels 13
Figure 11: Identity verification as top challenge / manual reviews 14
Figure 12: Top-2 box agreement with fraud-related statements 14
Figure 13: Top-2 box agreement with fraud-related statements 15
Figure 14: Percent using automated flagging system or fraud mitigation solution 16
Figure 15: Percent tracking fraud costs / transactions by payment channel / method 17
Figure 16: Fraud mitigation solutions current used by merchants 18
Figure 17: Distribution of fraud mitigation spend 19
Figure 18: Percent transactions flagged for manual review 19
Figure 19: Top challenges among large remote using auto flagging system 20
Figure 20: Most effective fraud mitigation solutions for international fraud 21
Figure 21: Percent false positives transactions 22
Figure 22: Percent false positives by different solution combinations / layering 23
Figure 23: Percent successful fraud attempts with multi-layered solution approach 24
Figure 24: Percent of credit / debit card transactions (2015 – 2016) 26
Figure 25: Percent successful fraud transactions among large remote by online/mobile 26
Figure 26: Fraud mitigation solutions bundled by Large mCommerce 27
Figure 27: Fraud mitigation solutions bundled by Large eCommerce 28

Introduction

The 2016 LexisNexis® True Cost of Fraud℠ Study aims to help merchants grow their business safely, even as signs in the industry point to a growing risk of fraud. The research provides a snapshot of current fraud trends in the United States and spotlights key pain points that merchants should be aware of as they add new payment mechanisms and expand channels into online, mobile, and international sectors.

The study answers a question critical to the entire merchant community: How do I grow my business and manage the cost of fraud while strengthening customer trust and loyalty?

Fraud definition

For the purpose of this study, fraud is defined as the following:

- Fraudulent and / or unauthorized transactions;
- Fraudulent requests for a refund/return and bounced checks; and
- Lost or stolen merchandise, as well as redistribution costs associated with redelivering purchased items (including carrier fraud).

This research covers consumer-facing retail fraud methods and does not include information on insider fraud or employee theft.

Furthermore, LexisNexis Fraud Multiplier℠ is the total amount of costs related to fees, interest, merchandise replacement and redistribution per dollar of fraud for which the merchant is held liable.

Merchant definitions

- Small merchants earn less than $1 million in average annual sales.
- Medium-size merchants earn $1 million to less than $50 million in average in annual sales.
- Large merchants earn $50 million or more in annual sales.
- International merchants operate from the U.S. and do business globally.
- Domestic merchants do not sell merchandise outside the U.S.
- Large eCommerce merchants accept payments through multiple channels but maintain a strong online presence, earning10% to 100% of their revenue from the online channel and earning $50 million or more in annual sales.
- Mobile eCommerce merchants (mCommerce merchants) accept payments through either a mobile browser or mobile application, or bill payments to a customer's mobile carrier. Large mCommerce involves those earning $50 million or more in annual sales.

Executive Summary

Overview

US merchants continue to experience increased fraud losses in 2016, particularly among larger merchants with remote channel transactions. Large eCommerce and mCommerce merchants are challenged on various fronts, including an increased volume of successful fraud attempts, a rise in fraud cost/dollar losses and a bigger bite of fraud costs as a percent of annual revenues. At the same time, these large remote merchants are investing in resources to combat these issues, ranging from adopting multiple fraud mitigation solutions to the use of automated fraud flagging systems. That said, there is frustration with the cost of managing fraud, while still battling the expense of manual reviews and challenges of false positives. In fact, large remote merchants who use an automated flagging system and multiple fraud mitigation solutions still send a sizeable portion of flagged transactions for manual review, suggesting that they don't fully trust their solutions to delineate between legitimate and fraudulent customers. But, perhaps the right combination or layering of solutions aren't being used.

Study findings show that a multi-layered approach that includes identity verification, identity authentication and transaction risk assessment can reduce false positives and the need for manual reviews. While this may not slow the volume of fraud attempts, it can reduce the level of successful fraud transactions and the associated costs of such losses. The following presents key findings and recommendations to help merchants understand and navigate this challenging environment.

Key takeaways in 2016

- Retail fraud continues to rise dramatically as does its cost. The average volume and value of fraudulent transactions has risen sharply since last year. The level of fraud as a percentage of revenues has also inched upwards (1.32% to 1.47%). Each of these contributes to a rise in the LexisNexis Fraud Multiplier℠.
- Larger remote channels are driving the above increases, as they continue to experience the higher share of fraud. These are omnichannel merchants who, on average, experience significantly more fraudulent transactions per month, involving higher ticket items, than physical point-of-sale (POS) only merchants. They also miss more fraudulent transactions than are prevented. As a result, fraud costs as a percentage of annual revenues are much higher for larger remote channel merchants than for other merchants.
- Mobile fraud is the somewhat bigger issue and can be expected to grow. Fraud cost as a percentage of revenues is higher among mCommerce merchants; there is greater concern about the security of allowing mobile transactions; and, there is a significantly high number of lost transactions per month to fraud through mCommerce. All of this will intensity as the mCommerce channel is expected to grow during the next 1 -2 years. While less than one-fifth currently optimize for mobile transactions, a sizeable portion (32%) report considering it in the next 12 months (which could lag based on budgets and priorities).

- Many merchants track fraud costs by either the payment channel (in-store, online, mobile) or payment method (credit / debit card, etc); fewer are tracking by both methods,making the efforts to manage fraud less effective.
- While large remote channel merchants spend on fraud mitigation, some still need to be convinced of solution effectiveness. Nearly two-thirds of Large eCommerce and mCommerce merchants report using an automated system to flag fraud; over three-fourths indicate using a fraud mitigation solution (often multiple). However, nearly half of transactions flagged as potentially fraudulent are ultimately decided by human beings, as these channels spend up to 25% of fraud mitigation budgets on manual reviews. Further, false positive rates and fraud costs continue to grow as these merchants pour money into multiple fraud management tools with seemingly modest success. As a result, their optimism that reduced fraud can increase loyalty and sales is tempered by their frustration that managing fraud costs too much.
- Merchants benefit more when relying on a multi-layered approach to fraud mitigation solutions. Study findings show that those using multiple solutions which layer in identity verification, identity authentication and transaction risk assessment experience fewer false positives and successful fraud attempts than those who don't. In fact, findings show that those who use multiple solutions, but not in a layered approach as noted above, experience similarly higher false positives and successful fraud attempts as those who use very few solutions.
- International remote merchants need more information on which fraud mitigation solutions are best for cross-border transactions. Many don't feel that they've got specialized tools for international fraud prevention, while at the same time they are challenged to readily identify what those solutions would be.

Recommendations

- Remote channel merchants need to increase their tracking of both payment and channel fraud. The omnichannel creates its own complexities and fraudsters are skilled at learning how and where to take advantage of blind spots. They try different fraud methods with different merchants to find out which succeed with whom, such that merchants need to stay focused on all avenues to the sale. Remember, one-size does not fit all.
- Even though most Large eCommerce merchants also operate through the mobile channel, they should track the online and mobile channels separately. While both are remote channels, they have different security approaches and issues. Tracking them together could unknowingly mask over issues specific to only one of these channels, in which case different solutions and technologies would be necessary.
- To effectively combat fraud, remote channel merchants should consider a multi-layered approach, redistributing spend away from excessive manual reviews towards select solution combinations. Fraud emerges from many different facets; no one solution is likely to be the "holy grail" at this point in time. Throwing more resources

at the problem may not be the solution if this doesn't combat fraud from the different facets of identity verification, identity authentication and transaction risk. Therefore, remote merchants should consider some combination of automated transaction scoring/rules and logic filtering, real-time transaction tracking, transaction / customer verification and authentication, geolocation and/or device identification.

- There needs to be more awareness and understanding about the value of investing in a multi-layered approach to fraud mitigation. Survey findings suggest that remote channels may not be using the most effective solutions to address all fraud facets across different channels, yet many are investing in multiple solutions nonetheless. This can create the impression that the cost of managing fraud is an overwhelming battle, while stretching budgets to the limit. But, as findings have shown, the right multi-layered approach can justify upfront costs of the solution investment as greater accuracy yields more positive results on the bottom line.
- Mobile merchants, in particular, need to remain vigilant and open to a wider variety of fraud prevention solutions. Fraud in this channel is only going to grow as more merchants enter this space; more types of mobile transaction methods will emerge beyond the typical browser. As a result, mCommerce merchants may need to rely on different variations of solutions depending on the transaction methods, including Device ID/Fingerprinting, 3-D Secure Tools and Geolocation.
- International merchants who sell through the online and/or mobile channels should complement their multi-layered approach with solutions unique to cross-border issues. They can't necessarily rely on the same solutions to support both domestic and international fraud management. There tends to be a false sense of security through perceiving Card Verification Value (CVV) and PIN/Signature Authentication as being most effective for combatting international fraud; the former can be rendered ineffective with breached card information and the latter is more relevant to the physical POS environment (since remote purchases generally don't require PIN entry).

General fraud trends

General trends indicated a growing problem with retail fraud.

There are indications of increasing fraud challenges for US retailers based on rising fraud costs and volume. One leading indicator is the LexisNexis Fraud Multiplier℠, which is on the rise after a dip in 2015.

On average, US merchants reported an 8% increase over last year in the cost per dollar of fraud losses, from $2.23 to $2.40 (see figure 1). This means that for every dollar of losses, merchants are losing $2.40 based on chargebacks, fees and merchandise replacement.

The LexisNexis Fraud Multiplier℠ is On the Rise

Weighted merchant data

Q: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud cost over the past 12 months.

July 2010 – February 2016, n varies from 145 to 712

Base = Merchants experiencing fraud in the past 12 months

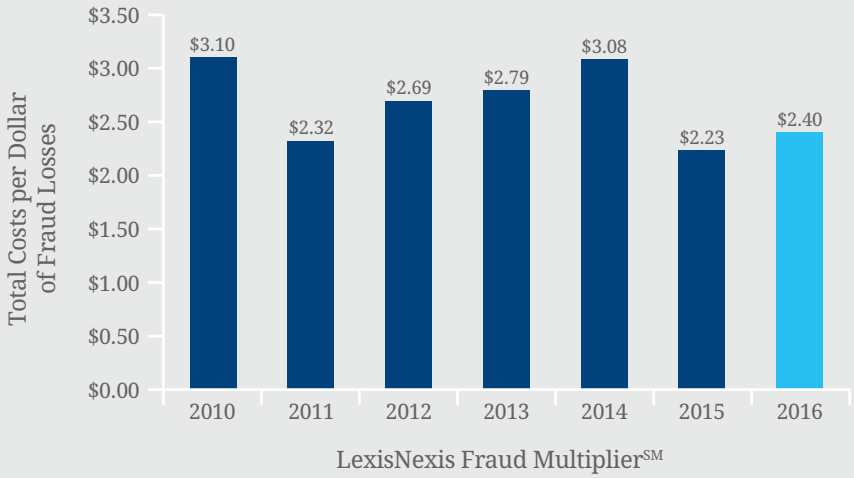


Figure1: Cost per dollar of fraud losses by year (2010 – 2016)

This has been influenced by an increase in the volume of fraudulent transaction attempts, including those which were successful (see figure 2). Since last year, the average number of monthly fraud attempts has spiked by 33%, with just under half (46%) getting past merchants' fraud mitigation efforts. Some of this could reflect late 2015 holiday sales, which would have been top-of-mind for merchants when the survey was fielded in early 2016. Nonetheless, all of this has contributed to a continued increase in the percent of revenues lost to fraud, up 11% over last year from 1.32% to 1.47% (see figure 3).

Average Fraudulent Transactions and Value per Month Have Increased Significantly

Weighted merchant data

Q: In a typical month, approximately how many fraudulent transactions are prevented by your company / successfully completed by fraudsters? What is the average value of successful fraud transactions?

July 2012 – February 2016, n varies from 131 to 1,142

Base = All merchants experiencing specific fraud types

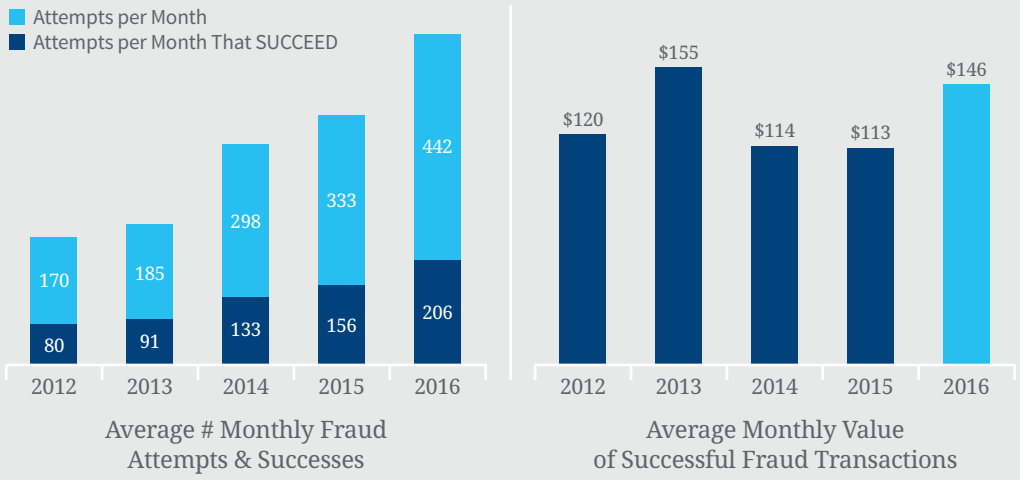


Figure 2: Average number total and successful fraudulent attempts per month; average value successful fraudulent transactions per month (2012 – 2016)

Cost of Fraud as a % of Revenues Keeps Going Up

Weighted merchant data

Q: What is the approximate dollar value of your company's total fraud losses over the past 12 months? Fraud losses as a percent of total annual revenue.

Fraud Costs as a Percentage of Annual Revenues

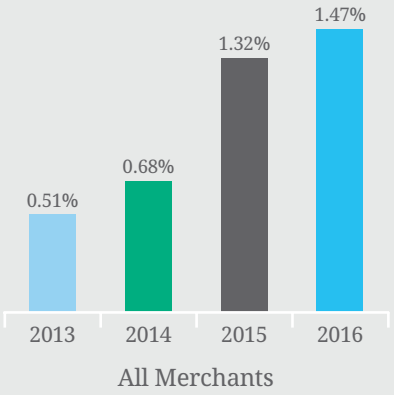


Figure 3: Fraud as a percentage cost of annual revenues (2013 – 2016)

Remote channels are getting hit harder by fraud

Remote channels have experienced a sharper rise in the cost/dollar of fraud losses. Even though physical POS-only merchants have a similar cost/dollar fraud level as remote channel merchants, its year-over-year increase (3%) has been significantly smaller than the sharper 9% - 12% experienced by online and mobile merchants respectively (see figure 4). Further, chargebacks have been higher among remote merchants, which is consistent with assumptions that card-not-present (CNP) makes it easier to anonymously purchase online and leave remote channels with more risk of chargeback liability.

Remote Channels are the Primary Driver of the LexisNexis Fraud Multiplier℠ Increase

Weighted merchant data

Q: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud cost over the past 12 months.

March 2015 – February 2016, n varies from 199 to 320

Base = Merchants experiencing fraud in the past 12 months

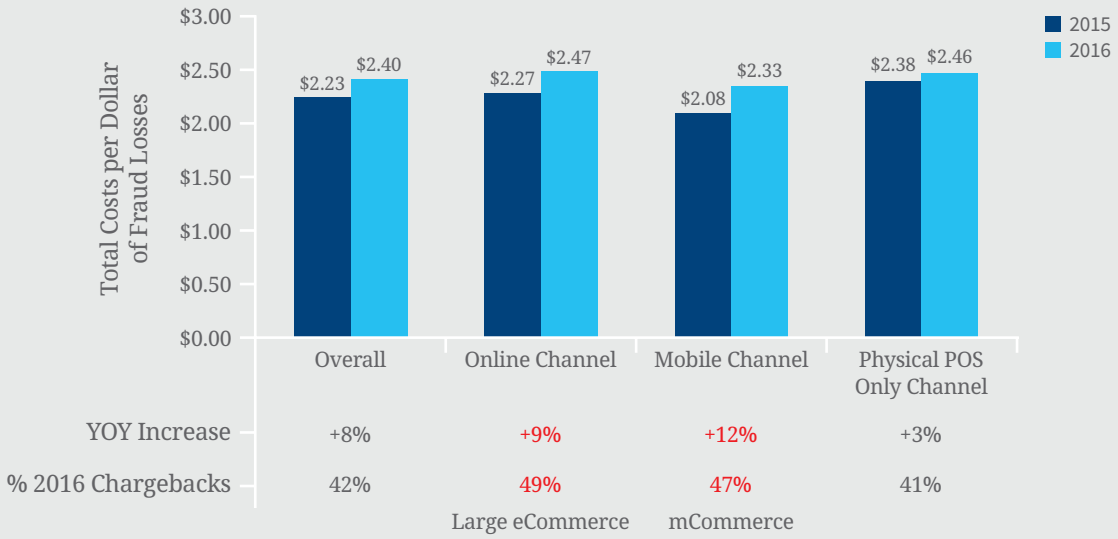


Figure 4: Cost per dollar of fraud losses by year by channel (2015 – 2016)

Remote channels are having to battle fraud from both debit and credit card payment methods.

Debit card fraud has risen across the board, though it has become a larger share of fraud among remote channel merchants than among all merchants (see figure 5). Over the past year, successful remote channel fraud through debit cards has reached levels comparable to credit cards at the same time, credit card fraud has remained fairly constant as a percentage of successful fraud; further, the level of credit and debit card transactions has remained fairly constant as well (see Appendix, figure 24). Therefore, the debit card spike is not about fraudsters switching their focus from one payment method to another. Instead, it signals that fraudsters are seeing this as a weak link in the race to leverage previously breached debit card information.

Successful Fraud Attempts in Remote Channels are Similarly Split Between Debit and Credit Card Payment Methods

Weighted merchant data

Q: Please indicate the distribution of payment methods linked to successful fraud attempts.

March 2015 – February 2016, n varies from 63 to 371

Base = Merchants experiencing fraud in the past 12 months and who track fraud by payment method

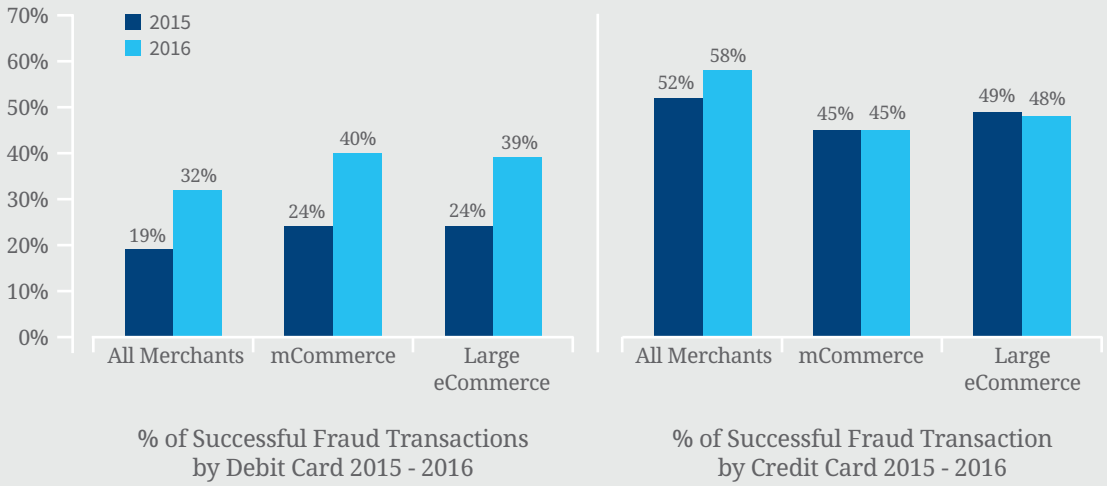


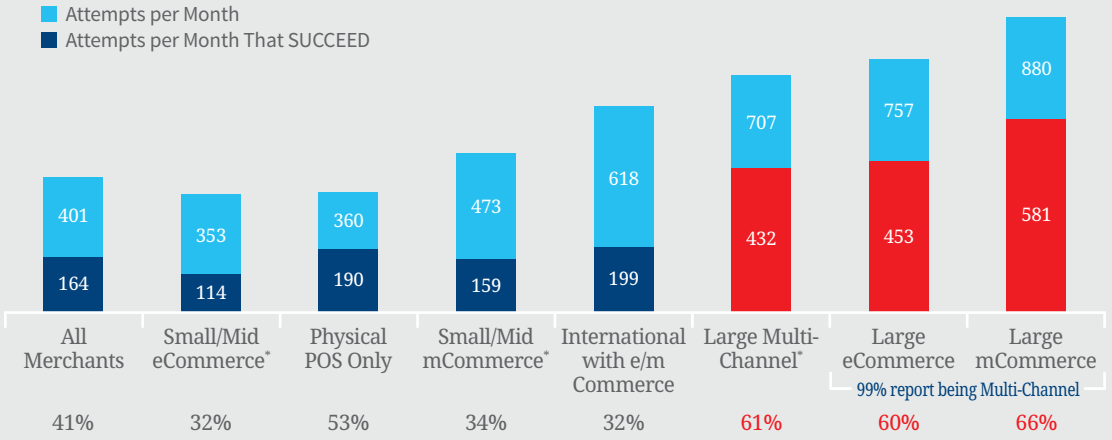
Figure 5: Percent of successful fraud transactions by debit / credit card (2015 – 2016)

Remote channels are getting hit with more successful fraud attempts.

But it's not just remote — larger merchants with multiple channels are experiencing the most fraud volume, particularly mobile (see figure 6). Larger remote channel merchants have a disproportionately higher percentage of successful fraud attempts than smaller remote channel merchants and Physical POS-only merchants. Additionally, the mobile channel as a percent of successful fraud transactions among large remote channel merchants has grown year-over-year from 26% to 35% (see Appendix, figure 25). The assumption that Physical POS adoption of EMV is driving fraudsters remotely appears to be playing out. But, there is more influencing this occurrence.

Large e/mCommerce merchants are multi-channel. This opens up more avenues for attack, particularly where a fraudulent purchase is made remotely and then picked up in-store without the need for card re-swiping.

Larger Remote Channels are Getting Hit with More Successful Fraud Attempts per Month



* Small/Mid = Less than 50M annual revenue; Large = $50M+ annual revenue

Weighted merchant data

Q: In a typical month, approximately how many fraudulent transactions are prevented by your company / successfully completed by fraudsters?

February 2016, n varies from 190 to 1007

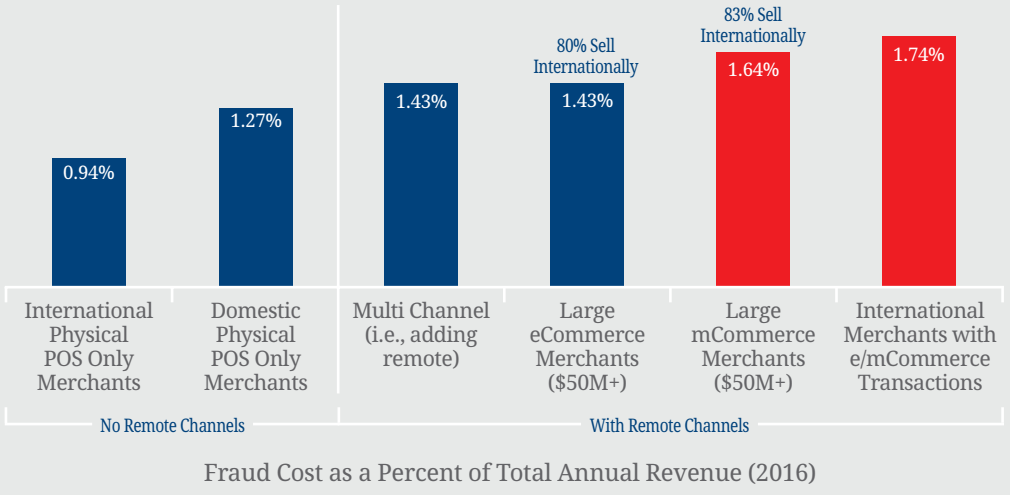
Base = All merchants experiencing specific fraud types

Figure 6: Average number total and successful fraudulent attempts per month by channel (2016)

Remote channels are losing more as a percentage of annual revenues.

Larger remote channels are also getting hit harder on fraud cost, particularly mobile and cross-border transactions which experience 15% - 20% higher fraud costs as a percent of annual revenue than even the average multi-channel merchant (see figure 7). Naturally, remote channels are quicker and easier ways to purchase merchandise outside of the US. And, in the seemingly "borderless" online world, it's not surprising that most Large e/mCommerce merchants are selling merchandise internationally. This makes remote channel challenges even more complex. And as omnichannel retail sales are expected to grow, the risk and cost of remote and cross-border fraud will likely intensify .

Larger Remote Channels with International Sales Indicate Higher Fraud Costs as a Portion of Annual Revenues



* Small/Mid = Less than 50M annual revenue; Large = $50M+ annual revenue

Weighted merchant data

Q: What is the approximate dollar value of your company's total fraud losses over the past 12 months? Fraud losses as a percent of total annual revenue.

February 2016, n varies from 26 to 636

Base = All merchants experiencing >$0 fraud in the past 12 months

Figure 7: Fraud as a percentage cost of annual revenues by merchant type and channel (2016)

Remote channels are battling identity fraud more than others.

Identity theft is more problematic for larger remote channel merchants than for physical channel merchants (see figure 8). The anonymous CNP environment makes identity theft much easier through remote than in-store encounters. Also, fraudsters can take advantage of retailer goodwill of offering online buying convenience and then allowing a return to be made in-store – especially where ID is not required during the return. This continues the trend that larger remote channels are more in the crosshairs of fraudsters at the moment.

Identity Fraud is a Bigger Issue for Remote Channels

Weighted merchant data

Q: Please indicate, to the best of your knowledge, the percentage distribution of the following fraud methods below, as they are attributed to your total annual fraud loss over the past 12 months.

February 2016, n varies from 100 to 337

Base = Large e/mCommerce, International with e/mCommerce and Physical POS-only merchants experiencing fraud

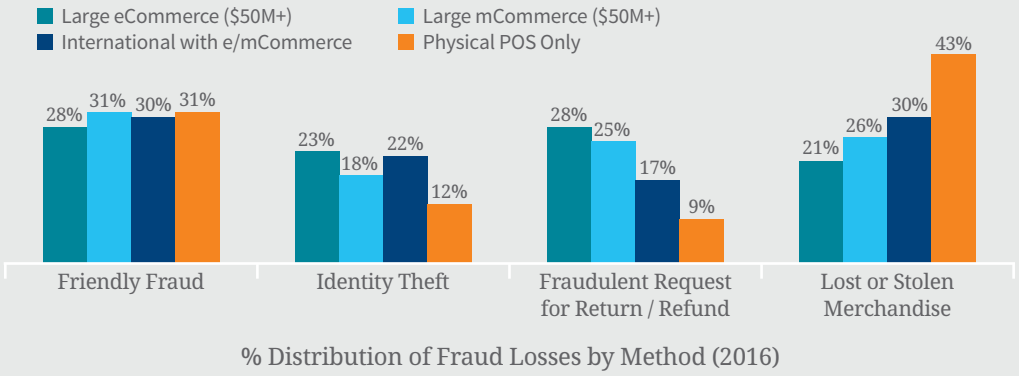


Figure 8: Distribution of fraud methods during past 12 months (2016)

These challenges will likely continue, particularly in the mobile channel.

mCommerce could grow significantly over the next 1-2 years, which would add to the issues cited previously. Current mCommerce merchants tend to be larger in terms of annual revenues ($50M+) and are already conducting eCommerce and international transactions. Growth within the next 1-2 years will likely be fueled by mid-sized merchants who already conduct eCommerce but are seeking the next step (see figure 9). This means that the remote channel base will grow for fraudsters, giving them a fresh supply of new merchants to target.

mCommerce Expected to grow in the Near-Term

*Not all who say "likely in next 12 months" may actually be able to do so in that timeline. Budgets and other unforeseen factors could delay adoption

Weighted merchant data

Q: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment channels currently accepted by your company. Is your company considering accepting payments by mobile device over the next 12 months?

February 2016, n varies from 14 to 1007

Base = All merchants

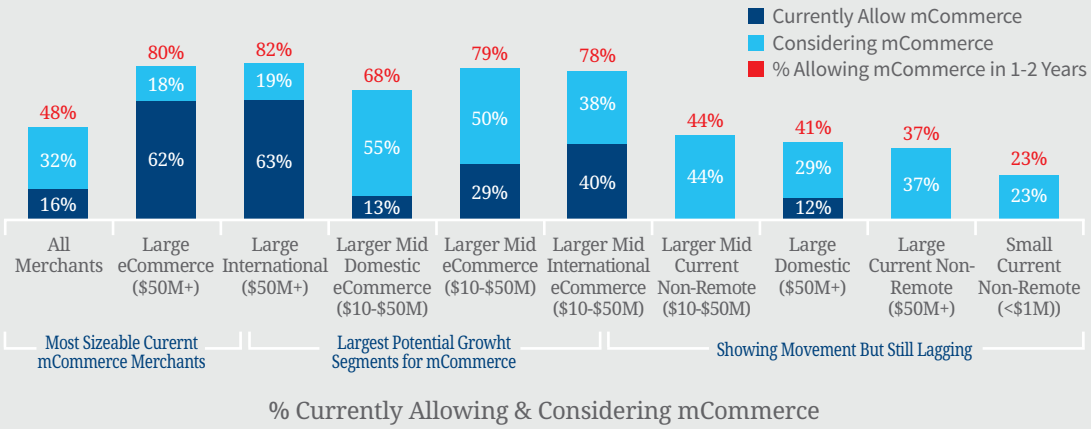


Figure 9: Percent currently allowing and considering mCommerce (2016)

Reaction to these trends

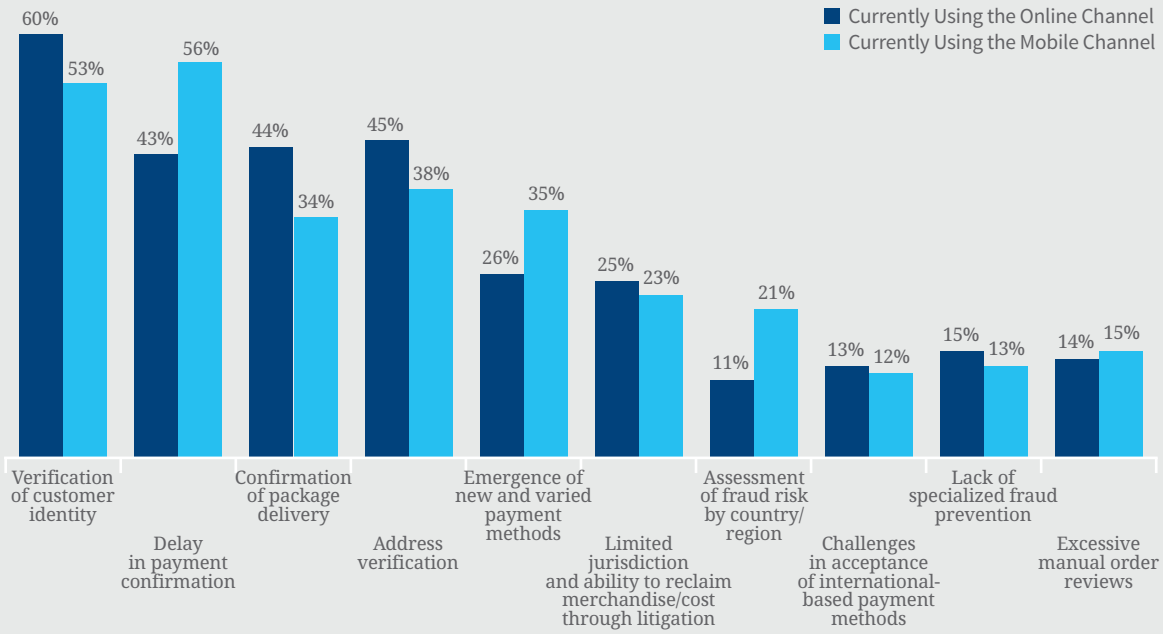
Online and mobile channel merchants worry about catching the bad guys without alienating the good ones.

Since identity theft is more prevalent in CNP transactions, remote channel merchants are more challenged with determining if the customer is fraudulent or not. The wrong decision can lead to declining a legitimate customer and losing the lifetime value that would have come with his / her future purchases.

But that's not the only way to lose a customer. Delayed transaction confirmation can cause friction for customers, causing them to abandon a merchant's website before transaction completion. That alone can make customers avoid merchants in the future. But, if the customer leaves the website before confirmation, yet gets charged for the transaction, this can result in chargebacks to the retailer – along with the potentially lost future business. Therefore, remote channel merchants struggle between concerns about lessening customer friction while needing to ensure that the person is in fact valid.

Being remote also means the absence of a physical hand-off of merchandise with the customer. Therefore, it's not always clear if the merchandise has been delivered to a legitimate location. Not having delivery confirmation (i.e., not getting signature upon delivery) can weaken merchants' defenses against chargebacks, especially in the case of friendly fraud.

Ability to Quickly Distinguish & Confirm Fraud is a Challenge for Remote Merchants



Weighted merchant data

Q: Please rank the top 3 challenges related to fraud faced by your company when selling merchandise to customers in the Online / Mobile Channels.

February 2016, n = 620 Online & 304 Mobile

Base = Merchants selling through the online or mobile channels

Figure 10: Top challenges when selling merchandise through the online / mobile channels (2016)

Challenges with verifying customer identity can increase the perceived need for more manual reviews among remote channel merchants.

Among online and mobile channel merchants who ranked verification of customer identity as their #1 challenge, the average percent of flagged transactions sent for manual review (51% - 58%) is significantly above the average (42%) (see figure 11). This would suggest that remote channel merchants don't entirely trust their fraud mitigation solutions to make the distinction between authentic customers and criminals.

Average % of Flagged Transactions Sent for Manual Review

Weighted merchant data

Q: Please rank the top 3 challenges related to fraud faced by your company when selling merchandise to customers in the Online / Mobile Channels. You indicated that a percentage of the transactions your company flags are flagged by automated system. Of this percentage, what proportion are sent for manual review?"

February 2016, n = 100 for Online, 49 for Mobile & 439 for All Merchants

Base = Merchants selling through the online or mobile channels who ranked "Verification of customer identity" as their top challenge and who use an automated system to flag potentially fraudulent transactions

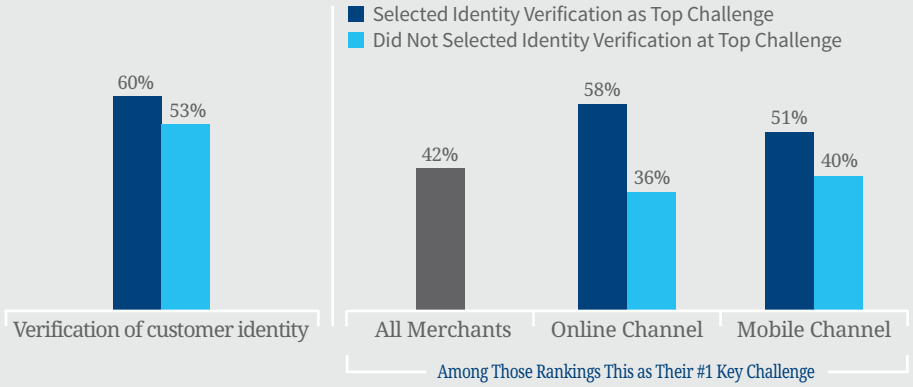


Figure 11: Identity verification as the top challenge when selling merchandise through the online / mobile channels by % of transactions flagged for manual review (2016)

Larger remote channel merchants are concerned about fraud management costs overall and mobile security in particular.

Larger remote channel merchants clearly understand that managing fraud and knowing more about the customer and transaction can have a combined effect of increased sales and loyalty. However, a sizable portion also feel that the cost of controlling fraud is too high (see figure 12). That said, the losses associated with fraud, including lost customers due to false positives, could prove significantly more costly over time than solution investments to mitigate such issues in the first place.

Perceived Benefits of Managing Fraud Are Somewhat Muted by Concerns about its Cost among Large Remote Channel Merchants

Weighted merchant data

Q: Using a 5-point scale, where "5" is "agree completely" and "1" is "do not agree at all", please rate the extent to which you agree or disagree with the statements below.

February 2016, n = 102 for Large mCommerce, 136 for Large eCommerce & 113 for Large International with e/mCommerce

Base = All Large mCommerce, Large eCommerce and Large International with e/mCommerce

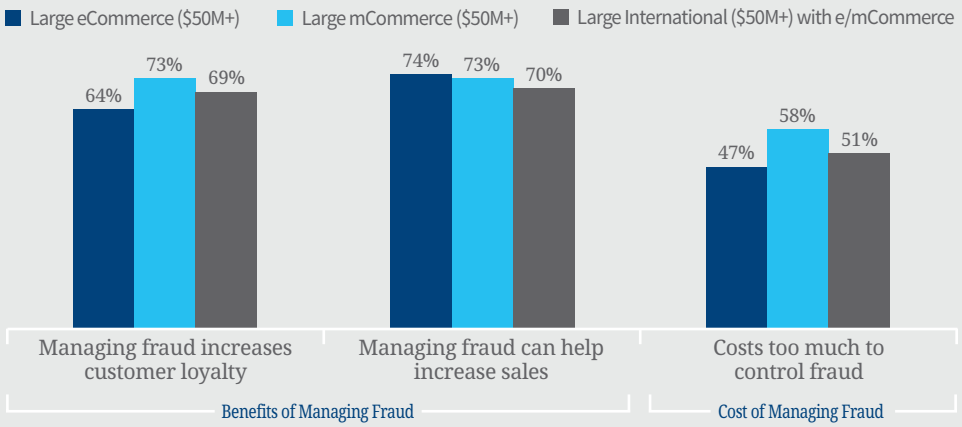


Figure 12: Top-2 Box (4 or 5 on 5-point scale) agreeing with fraud-related statements (2016)

But it is the mobile channel that causes the most concern. Larger participants in remote / international channels are still not sold on the security and risk management of the mobile channel and payment method. Nearly all concede that mobile adds significant risk to their business. At the same time, perceived benefits are modest (see figure 13), suggesting that online merchants are embracing the mobile channel based on a cautious competitive need rather than a whole-hearted desire for customer convenience or adding an additional sales channel.

Significant Concerns about Mobile Channel Security Outweighs Perceived Benefits of Allowing it as a Payment Channel

Weighted merchant data

Q: Using a 5-point scale, where "5" is "agree completely" and "1" is "do not agree at all", please rate the extent to which you agree or disagree with the statements below.

February 2016, n = 102 for Large mCommerce, 136 for Large eCommerce & 113 for Large International with e/mCommerce

Base = All Large mCommerce, Large eCommerce and Large International with e/mCommerce

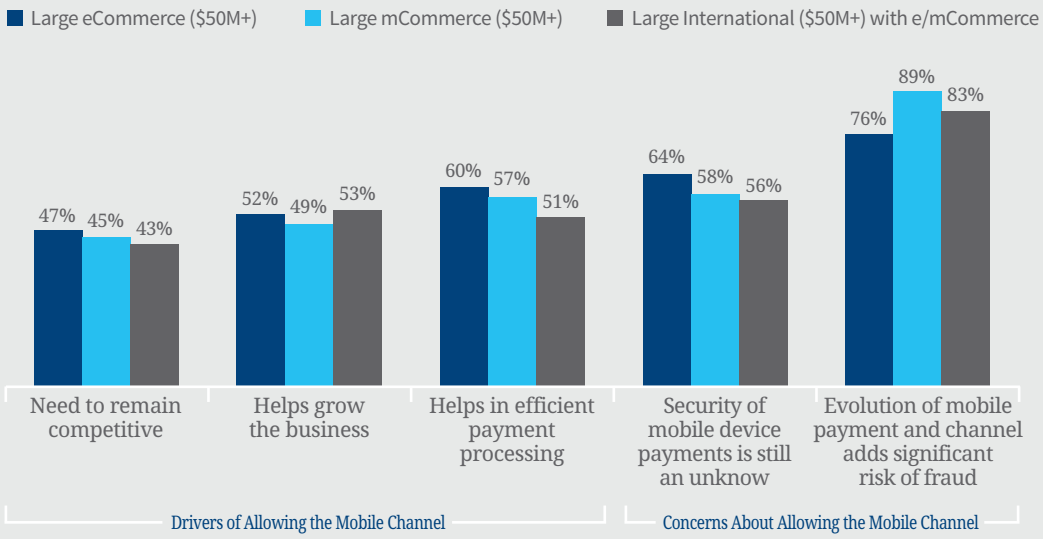


Figure 13: Top-2 Box (4 or 5 on 5-point scale) agreeing with fraud-related statements (2016)

What's being done about these growing fraud issues?

As larger remote merchants are getting hit harder by fraud, they are more likely to invest in solutions that help combat it.

As described earlier, larger eCommerce and mCommerce merchants are handling higher volumes of transactions, making manual fraud checking impractical. As multi-channel merchants, there is also a need to invest in solutions that can support fraud management within particular retail channels. As a result, they are more likely than others to invest in a system that automatically flags suspicious transactions, as well as to combine that with multiple fraud mitigation solutions – with Large mCommerce merchants leading the pack (average 5.8; see figure 14).

The card-not-present challenge continues to keep online and mobile merchants engaged with solutions. The number of solutions purchased tends to vary with the degree and type of concerns. Address and identity verification are top issues

regardless of how many solutions are used by a merchant. But, as concerns emerge around assessing fraud by country, the emergence and variety of payment methods and delays with transaction confirmation, then the number of solutions used by merchants tends to grow. For large mCommerce, the lack of fraud prevention tools for international orders tends to be a top issue as well – further underscoring the unique concerns with this channel.

Larger Remote Channel Merchants Use More Fraud Mitigation Tools & Solutions

*Small/Mid = Less than 50M annual revenue; Large = $50M+ annual revenue

Weighted merchant data

Q: Does your company use an automated system to flag potentially fraudulent transactions? Which of the following best describes your awareness and use of the fraud solutions listed below? Number of solutions being used.

February 2016, n varies from 102 to 1,007

Base = All merchants

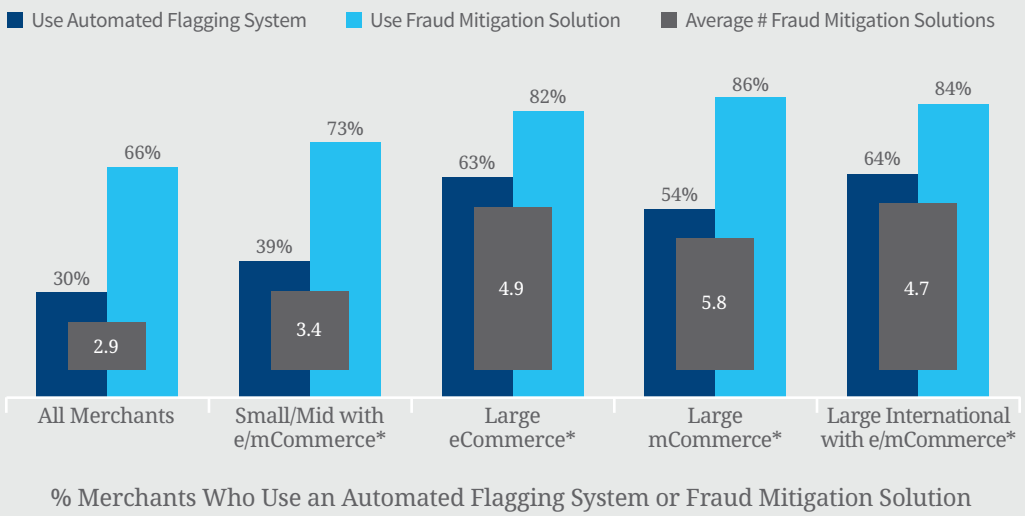


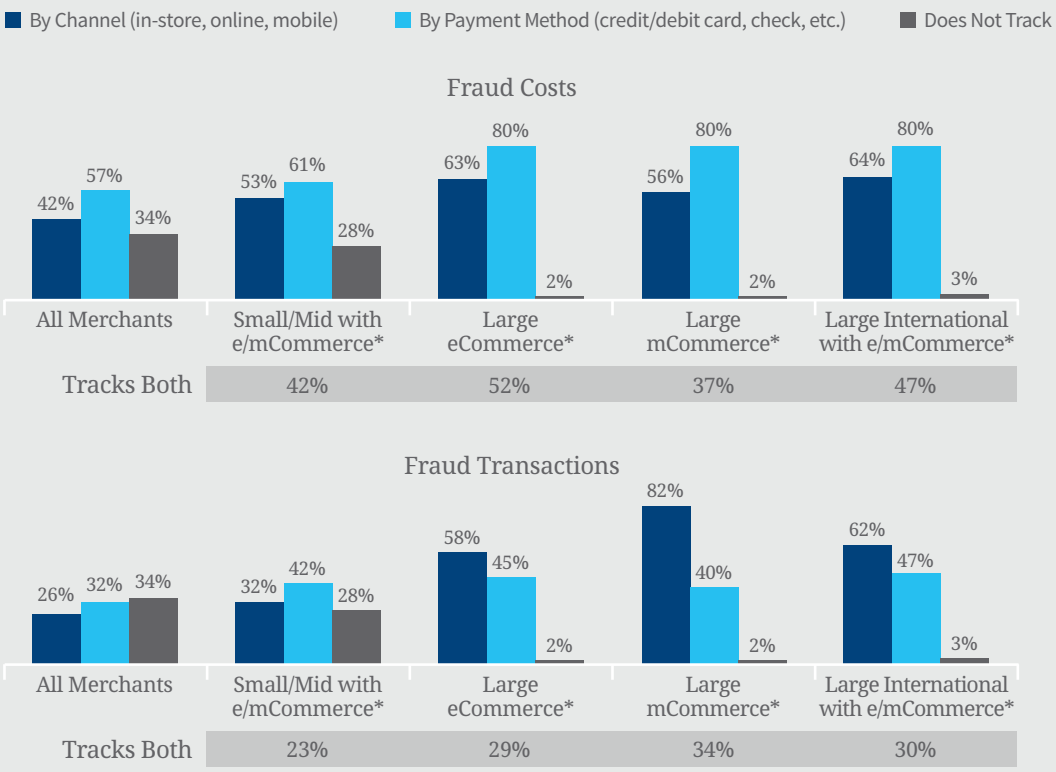
Figure 14: Percent using an automated flagging system or fraud mitigation solution (2016)

The application of fraud mitigation resources may be less than optimal.

Large remote channel merchants may not be tracking fraud to the fullest extent. Large eCommerce and mCommerce merchants are more likely than smaller remote channel merchants to take further steps beyond fraud mitigation solutions; they are also more likely to track where fraud originates. However, such tracking is not always done on consistent measures. Larger remote / international channel merchants are more likely to track fraud costs by payment method, while tracking fraudulent transactions by channel. Fewer are tracking fraud costs and transactions by both channel and payment method (see figure 15).

Since the omnichannel is more complex to manage, the lack of tracking fraud costs and transactions by both channel and payment methods can lessen the overall effectiveness of managing fraud in this environment.

Larger Remote Channel Merchants Track Fraud by Channel or Payment Method, but Less Often by Both



*Small/Mid = Less than 50M annual revenue; Large = $50M+ annual revenue

Weighted merchant data

Q: Does your company track the cost of fraudulent transactions by payment channels or methods? Track successful fraud by payment channels or methods?

February 2016, n varies from 102 to 1,007

Base = All merchants

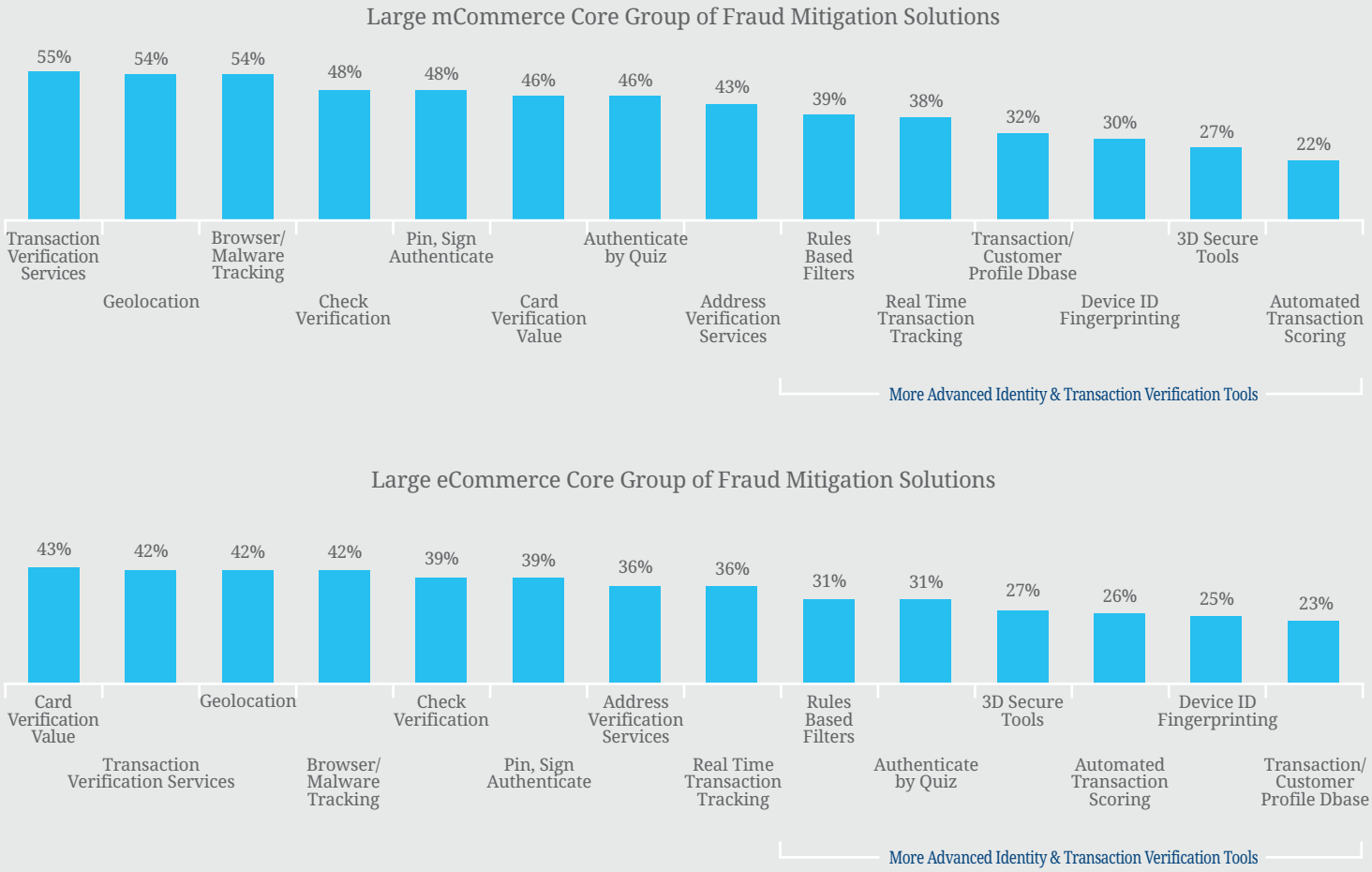
Figure 15: Percent tracking fraud costs and transactions by payment channel and method (2016)

Large remote channel merchants use many solutions together, but not always ones involving advanced identity and transaction verification tools.

As mentioned earlier, larger remote channel merchants use 5 – 6 fraud mitigation solutions on average (see figure 14). For Large eCommerce and mCommerce merchants, there tends to be a similar core group that is bundled together (see figure 16 and Appendix, figures 26 & 27). While there is some bundling of more advanced identity and transaction verification solutions with the core group, most Large e/mCommerce merchants are not using them.

And, while some of the core solutions can help manage fraud across different channels, others may be less relevant to particular ones. For example, Check Verification and Pin/Signature are more useful to physical POS transactions; Card Verification (CVV) can be less effective in the remote channel once a person's data has been breached; AVS can be less effective when seeking to verify a foreign address (not always compatible or easy to trace).

Fraud Mitigation Solutions Used by Large m/eCommerce



Weighted merchant data

Q: Which of the following fraud solutions does your company use? February 2016, n = 102 for Large mCommerce, 136 for Large eCommerce Base = All Large mCommerce and Large eCommerce

Figure 16: Fraud mitigation solutions currently used by merchants (2016)

While larger remote channel merchants spend on fraud mitigation solutions, they also continue spending on manual resources as well.

International merchants spend a significant amount on manual reviews. And, while large remote channel merchants spend nearly half of mitigation budgets on solutions, they have a sizeable portion that is apportioned to manual reviews and physical security (for their brick and mortar operations) (see figure 17). Plus, it's not just those who lack an automated flagging system that deal with manual reviews; a

sizeable portion of transactions that are flagged by merchants using an automated flagging system are in fact sent for manual review (see figure 18). In the more complex omnichannel environment, this adds more time and cost to fraud mitigation processes.

Distribution of Fraud Mitigation Costs by Percent of Spend

Weighted merchant data

Q: What is the percentage distribution of mitigation costs across the following areas in the past 12 months?

February 2016, n = 101 for Large mCommerce, 134 for Large eCommerce, 376 for International

Base = Merchants who spend >$0 on fraud mitigation

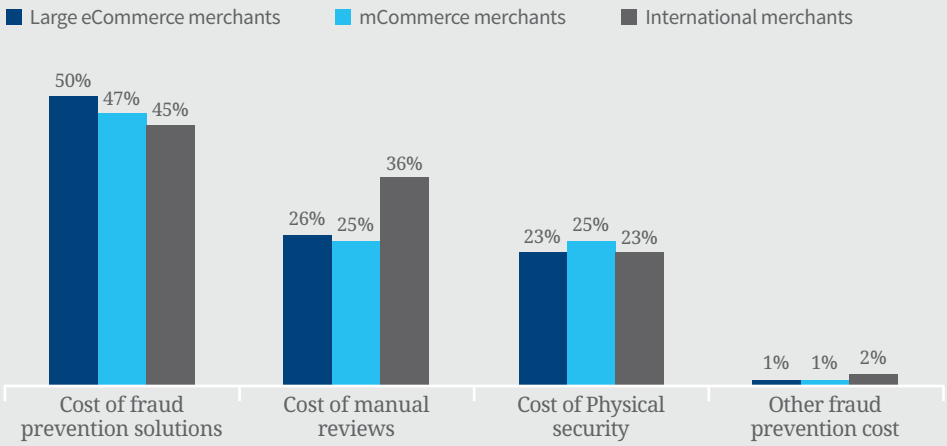


Figure 17: Distribution of fraud mitigation spend (2016)

Large remote merchants are sending a sizeable portion of auto flagged transactions for manual review.

Flagged Transactions from Remote Channel Merchants

Weighted merchant data

Q: Of all the transactions your company flagged as potentially fraudulent in the past 12 months, what percentage was flagged by your automated system?

Of this (…), what proportion are sent for manual review?

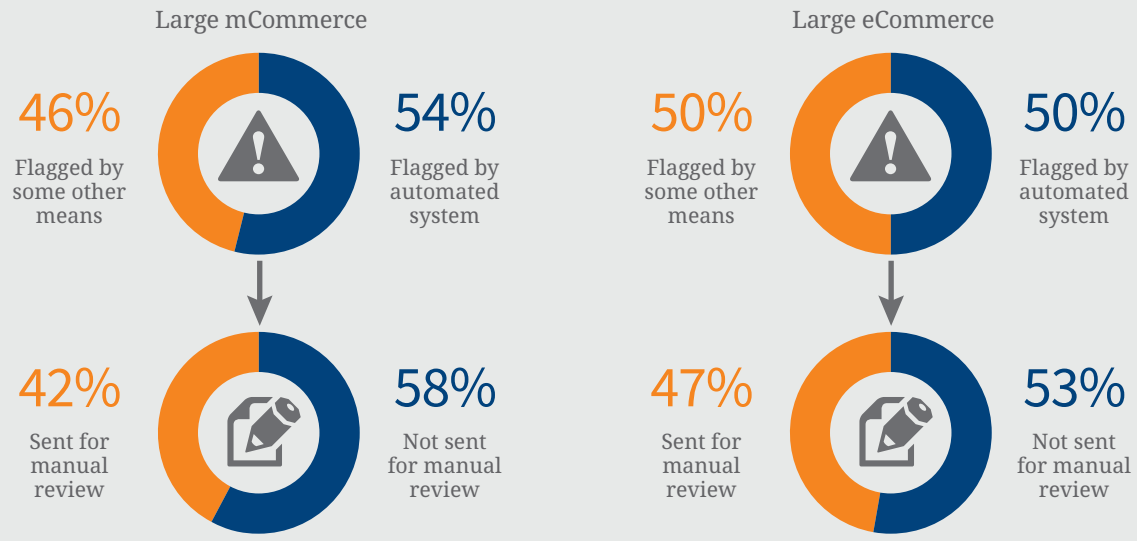


Figure 18: Percent of transactions flagged by automated system that are sent for manual review (2016)

The current solutions may not be ideal.

Manual reviews and false positives remain issues even with significant efforts by large remote channel merchants.

For domestic sales, excessive manual reviews are a top challenge among large remote channel merchants who use an automated flagging system (see figure 19). This type of system does what it says – it flags potentially fraudulent transactions. But, it doesn't necessarily give that extra step towards understanding the underlying reasons for potential fraud, including identity verification. In fact, it can create more work as merchants are naturally sensitive about declining legitimate transactions while catching the bad guys.

With remote international sales, excessive manual reviews remain a problem while other unique cross-border issues emerge as well (see figure 19). There is concern among both Large e/mCommerce merchants about new and varied payment methods in diverse international settings, where each country and region has its own laws and customs. Merchants don't feel as if they have the right specialized tools to manage cross-border fraud.

Further, Large mCommerce merchants have particularly stronger concerns about identity verification once its transactions cross the border (44% selling internationally versus 30% domestic). And, those excessive manual reviews remain a pain point. Part of the problem could lie in the solutions being used to manage fraud, particularly internationally.

Top Challenges of Large Remote Channel Merchants with Automated Flagging Systems

Weighted merchant data

Q: Please rank the top 3 challenges related to fraud faced by your company when selling merchandise to customers in the US. Please rank the top 3 challenges related to fraud faced by your company when selling merchandise to customers outside of the US

February 2016, n = 73 / 60 for Large mCommerce, 95 / 79 for Large eCommerce

Base = Large e/mCommerce merchants who use an automated flagging system and sell merchandise in or outside of the US

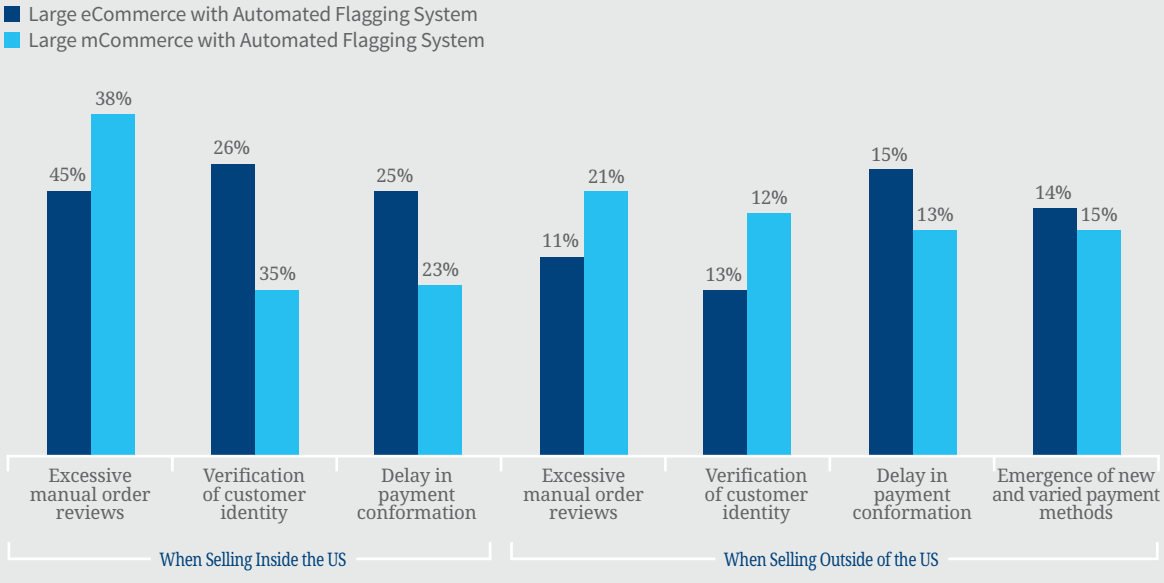
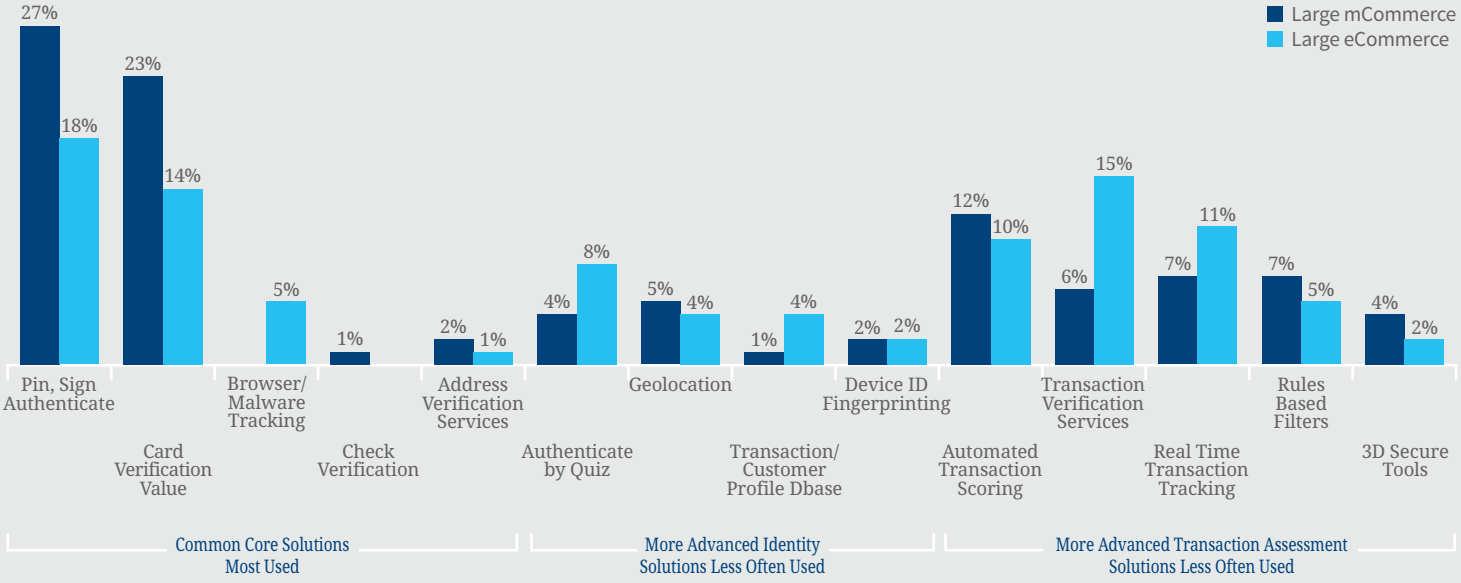


Figure 19: Top challenges among large remote even when they have an automated flagging system (2016)

But, there is little consensus around which solutions are most effective for controlling fraud internationally (see figure 20).

Further awareness and understanding is needed around the solutions that are best suited to support international fraud. Where limited consensus emerges, it is often with some of the same solutions used for domestic fraud management but which are not necessarily as effective for remote channels (PIN/Signature Authentication) or which can be tricked by fraudsters (CVV once card data is breached). Few remote merchants who sell internationally mentioned (or use) the more sophisticated identity and transaction assessment solutions which can address blind spots about purchasers from other countries.

Limited Consensus on Most Effective Solutions For Controlling International Fraud



Weighted merchant data

Q: Which of the following solutions is most effective in controlling fraud when selling outside of the US?

February 2016, n = 102 Large mCommerce, 136 for Large eCommerce

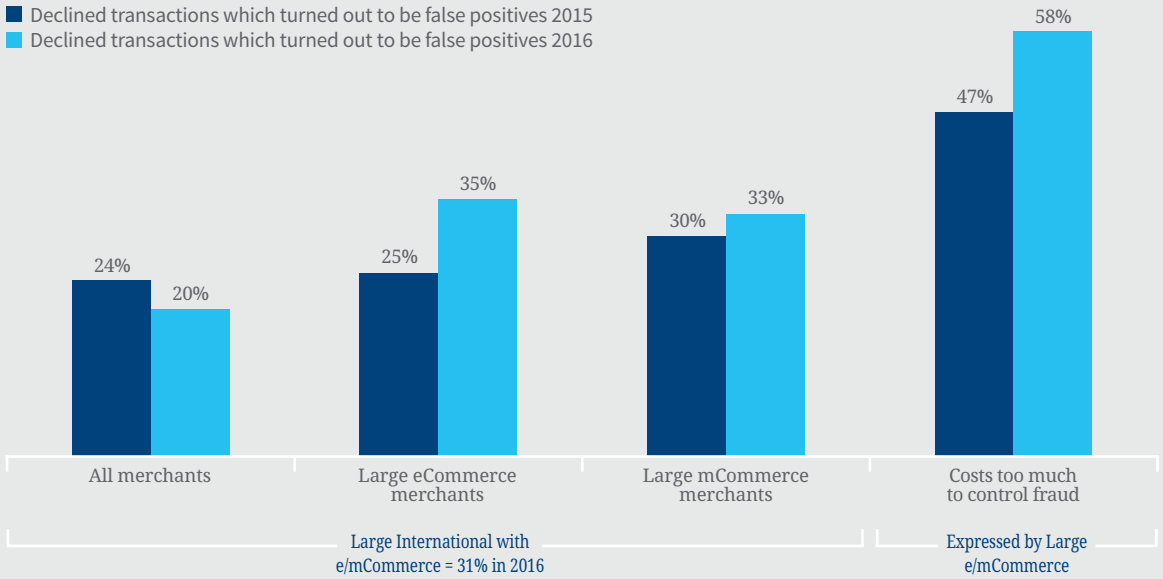
Base = Large e/mCommerce which conduct transactions outside of the US

Figure 20: Fraud mitigation solutions selected as most effective for controlling international fraud (2016)

So, with all of the efforts of fraud mitigation solutions, manual reviews and automated flagging systems, remote channel merchants still battle false positives.

In fact, false positives have increased for Large e/mCommerce merchants, even though they use more solutions and automated flagging systems than others (see figure 21). After all of these efforts, it's understandable that many remote channel merchants express concerns about the cost of managing fraud. Perhaps the more effective solutions are not being used.

False Positives Continue to Increase for Large e/mCommerce



Weighted merchant data

Q: What percentage of declined transactions turned out to be false positives?

February 2016, n = 102 Large mCommerce, 136 for Large eCommerce

Base = Large e/mCommerce

Figure 21: Percent of false positive transactions (2016)

The new way forward for combatting retail fraud.

It's not just about the number of solutions, but rather the right ones based on layering identity and transaction-based protection.

Survey findings show that remote channel merchants who invest in multiple solutions involving a multi-layered approach of advanced identity and transaction verification / authentication realize lower false positive rates than others (see figure 22).

On the other hand, remote channel merchants who invest in more solutions, but not a multi-layered approach as described above, experience similarly higher false positive rates as those who are using fewer solutions overall.

Percent of False Positives Declines with a Multi-Layered Approach

Weighted merchant data

Q: Which of the following fraud solutions does your company use? What percentage of declined transactions turned out to be false positives?

February 2016, n varies from 29 to 84 depending on combination

Base = Remote channel merchants

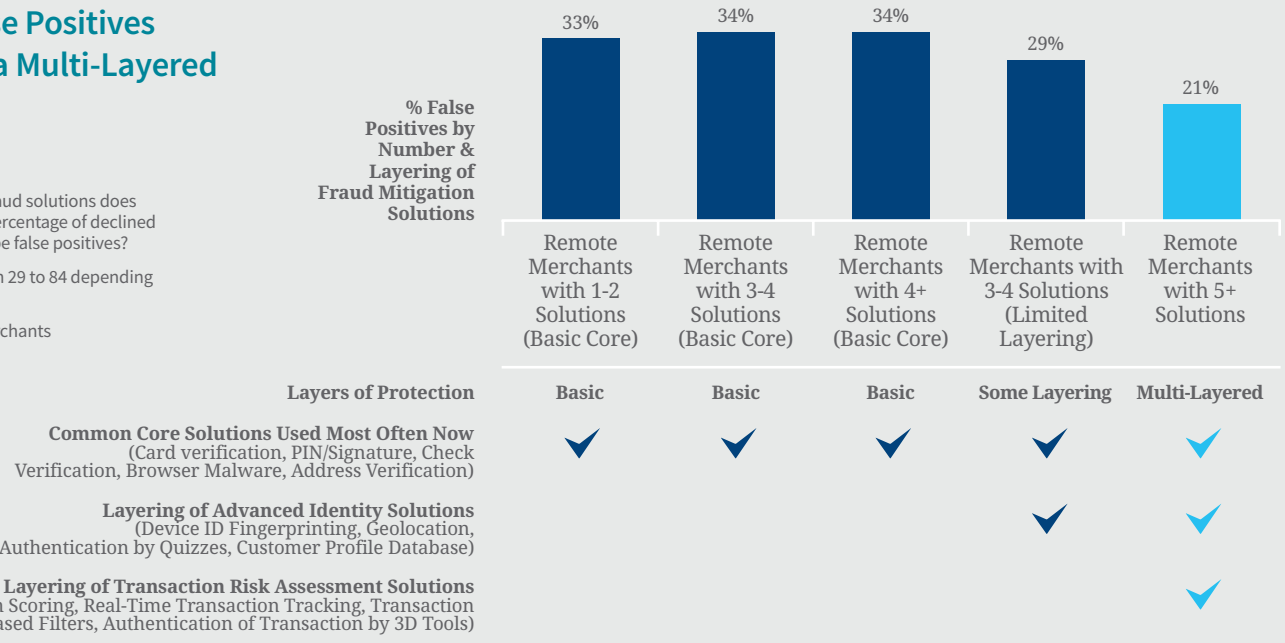


Figure 22: Percent of false positives based on multi-laying of specific types of fraud mitigation solutions (2016)

And, a multi-layered approach can reduce the amount of successful fraud attempts.

Large remote channel participants using a multi-layered approach report sizably fewer successful fraud attempts than all large remote merchants (see figure 23). This would make sense given that a multi-layered approach means managing fraud from different threat perspectives, including the identity of the person (are they real), the authentication of their information (is it right, does it make sense) and the risk of the transaction (just because it's a higher ticket price, it may not be fraud).

Percent of Successful Fraud Attempts Declines with a Multi-Layered Solution Approach

Weighted merchant data

Q: In a typical month, approximately how many fraudulent transactions are prevented by your company? In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

February 2016, n = 102 Large mCommerce, 136 for Large eCommerce, 84 for Large Remote with Multi-Layered Approach

Base = Large e/mCommerce

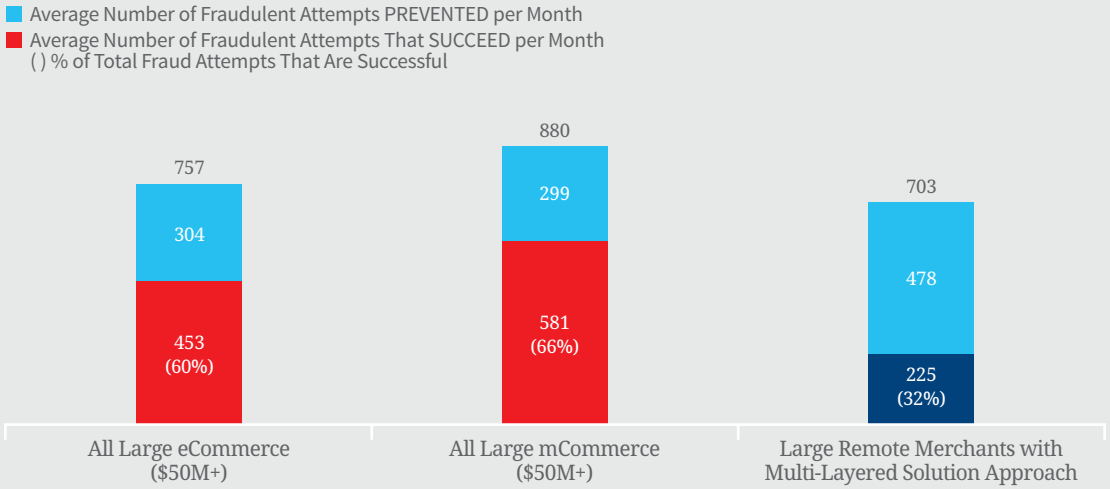


Figure 23: Percent of successful / prevented / total fraud attempts per month with multi-layered approach (2016)

LexisNexis® Risk Solutions can help.

LexisNexis® Risk Solutions provides powerful identity verification, identity authentication and transaction scoring tools to combat fraud. These solutions can help:

- Increase sales
- Reduce manual reviews
- Minimize fraud and chargebacks

LexisNexis® Risk Solutions leverages the largest, broadest, deepest, and most reliable repository of identity information available. With more than 45 billion records from over 13,000 sources and more than 3 million record updates per day, nothing else comes close. Combining unmatched information assets with unique data linking, and advanced analytics, LexisNexis® Risk Solutions helps uncover the information you need for a complete picture of individuals and companies you do business with.

Customer-Focused Solutions Relevant to Remote Channel Needs Include:

Identity Verification

- Validate name, address and phone information
- Reconcile name variations, duplicates, multiple addresses, and myriad other inconsistencies and linkages
- Perform global identity checks with seamless integration and reporting capabilities

Transaction Risk Scoring

- Identify risks associated with bill-to and ship-to identities with a single numeric risk score
- Quickly detect fraud patterns and isolate high-risk transactions
- Resolve false-positive and Address Verification Systems failure

Manual Research Support

- Access billions of data records on consumers and businesses
- Discover linkages between people, businesses and assets
- Leverage specialized tools for due diligence, account management and compliance

Identity Authentication

- Authenticate identities on the spot using knowledge-based quizzes
- Dynamically adjust security level to suit risk scenario
- Receive real-time pass/fail results

Methodology

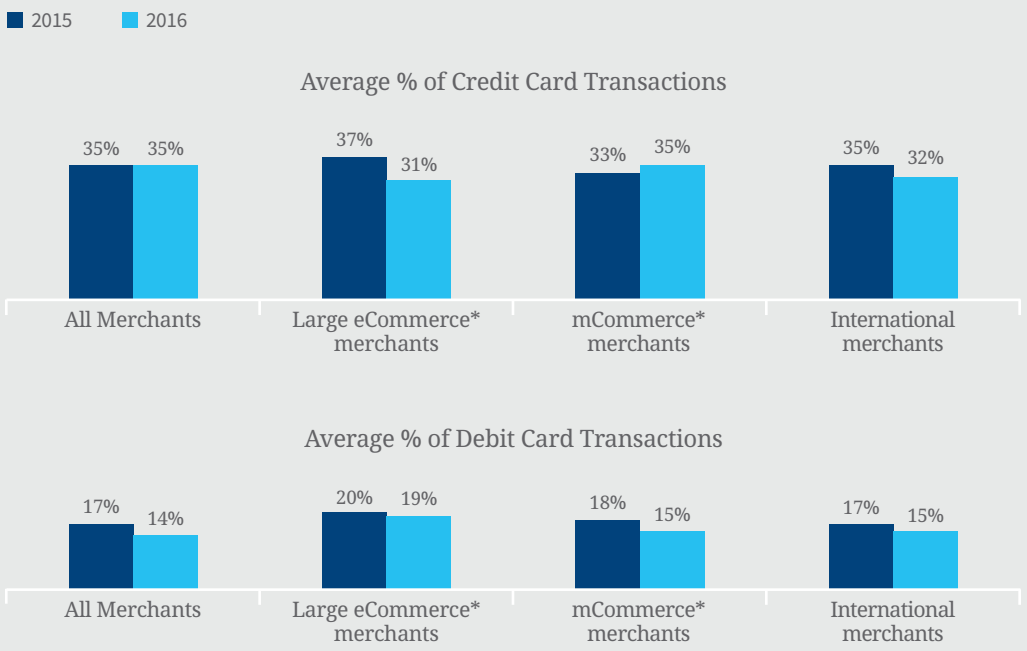
In 2016, LexisNexis retained KS&R, a global market research firm, to conduct the eighth annual comprehensive research study on U.S. retail merchant fraud.

The methodology of this study comprised U.S. Retailers as follows:

- A comprehensive survey of 1,007 risk and fraud executives in retail organizations, deployed during January-February 2016.
- All surveys were conducted online via a US business panel. LexisNexis was not identified as the sponsor of the study.
- Respondents represented retail businesses across all channels, company sizes, industry segments, and payment methods in order to be consistent with previous study waves.
- The overall margin of sampling error at the Total Level (All Merchants) is +/- 3.1% at the 95 percent confidence level. The sampling error is larger for subsets of respondents.
- Data reflects the US Merchant population based on weighting to U.S. Economic Census. Weighting to representativeness was based on two dimensions, consistent with previous waves, including
    - Size of merchant by number of employees; and
    - Industry segment.

Appendix

Level of Credit & Debit Card Transactions Has Remained Fairly Constant



Weighted merchant data

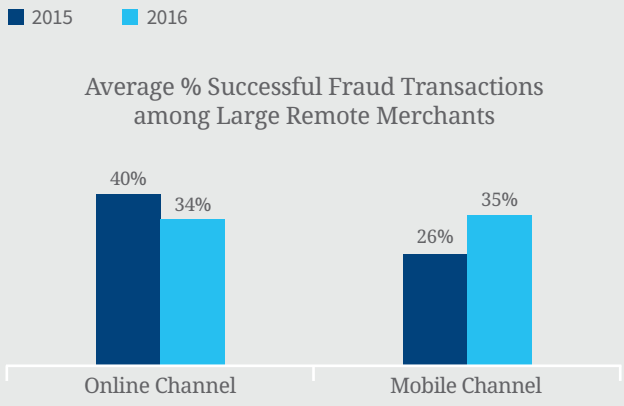
Q: Please indicate the percentage of transactions completed over the past 12 months for each of the following payment methods currently accepted by your company.

March 2015 – February 2016, n varies from 92 to 1,007

Base = All merchants

Figure 24: Percent of credit and debit card transactions (2015 – 2016)

The Mobile Channel as a Percent of All Successful Fraud Transactions Has Grown Since Last Year



Weighted merchant data

Q: Please indicate distribution of successful fraudulent transactions linked to the following channels.

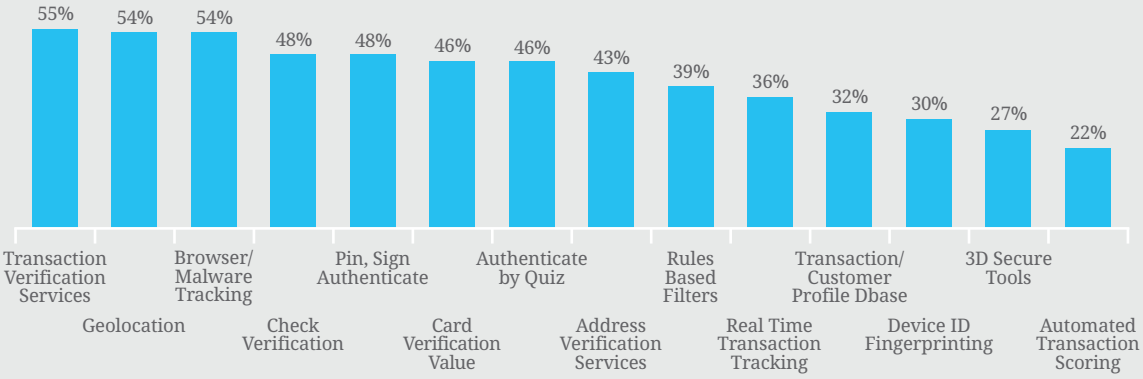
March 2015 – February 2016, n varies from 92 to 136

Base = Large eCommerce and Large mCommerce merchants

Figure 25: Percent of successful fraud transacti ons among large remote merchants linked to the online and mobile channel s (2015 – 2016)

Large mCommerce tends to Bundle a Core Set of Solutions

Large mCommerce Core Group of Fraud Mitigation Solutions



If Using One of the Core, Then Typically Also Using the Other Core Solutions . . .

Transaction Verification Services			✓	✓	✓	✓		✓
Geolocation			✓	✓	✓	✓	✓	✓
Browser / Malware Tracking	✓	✓		✓	✓	✓	✓	✓
Check Verification	✓	✓	✓		✓	✓	✓	✓
Pin, Sign Authentication	✓	✓	✓	✓		✓	✓	✓
Card Verification Value	✓	✓	✓	✓	✓		✓	✓
Authenticati on by Quiz		✓		✓	✓	✓		✓
Address Verification Services	✓	✓	✓	✓	✓	✓	✓	

These other advanced identity and transaction assessment / authentication may get bundled with the core by some in various combinations.

However, a majority of Large mCommerce are not using these types of fraud management / mitigation solutions.

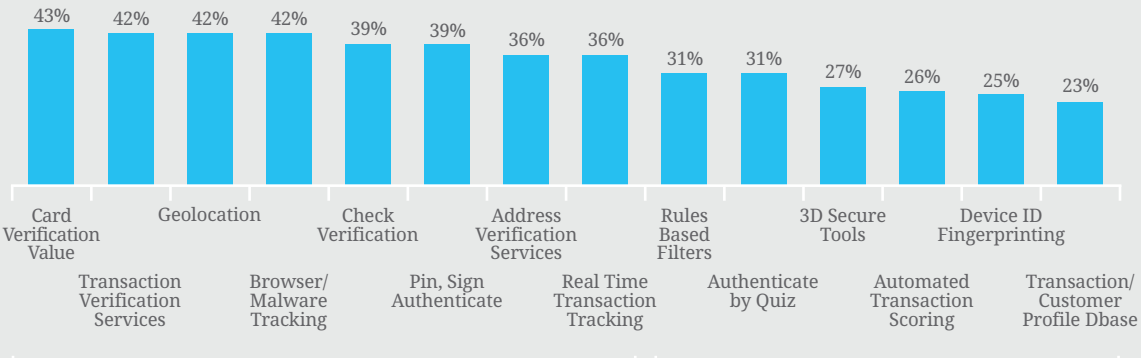
Weighted merchant data

Q: Which of the following fraud solutions does your company use? February 2016, n = 102 for Large mCommerce Base = All Large mCommerce

Figure 26: Fraud mitigation solutions bundled by Large mCommerce (2016)

Large eCommerce tends to Bundle a Core Set of Solutions

Large eCommerce Core Group of Fraud Mitigation Solutions



If Using One of the Core, Then Typically Also Using the Other Core Solutions . . .

Card Verification Value		✓	✓	✓	✓	✓	✓	✓
Transaction Verification Services	✓			✓	✓	✓	✓	
Geolocation				✓	✓	✓	✓	✓
Browser / Malware Tracking	✓	✓	✓		✓	✓	✓	✓
Check Verification	✓	✓	✓	✓		✓	✓	✓
Pin, Sign Authentication	✓	✓	✓	✓	✓	✓	✓	✓
Address Verification Services	✓			✓	✓	✓		✓
Real Time Transaction Tracking			✓		✓	✓	✓	

These other advanced identity and transaction assessment / authentication may get bundled with the core by some in various combinations.

However, a majority of Large eCommerce are not using these types of fraud management / mitigation solutions.

Weighted merchant data

Q: Which of the following fraud solutions does your company use? February 2016, n = 136 for Large eCommerce Base = All Large eCommerce

Figure 27: Fraud mitigation solutions bundled by Large eCommerce Merchants (2016)

For more information on LexisNexis® Retail Solutions

Call: 800.869.0751

Visit: lexisnexis.com/retail

About LexisNexis Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group, plc, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

About KS&R, Inc.

KS&R is a multi-award winning supplier of global market research. The firm works closely with clients in a range of industries to improve market position and increase returns on marketing investments. The views expressed by KS&R are not necessarily those of LexisNexis® Risk Solutions. The opinions expressed in this paper are those of survey respondents and do not necessarily reflect the positions of LexisNexis® Risk Solutions.

NXR11397-00-0516-EN-US