Annual Report

2014 LexisNexis® True Cost of Fraud℠ mCommerce

Merchants Struggle To Contain Rising Mobile Fraud Costs

January 2015

LexisNexis®

Risk Solutions
Retail

Table of contents

Table of figures

Introduction

The 2014 LexisNexis® True Cost of Fraud mCommerce Study provides insight into the mCommerce fraud challenges faced by merchants, financial institutions and consumers. This study establishes the cost of fraud for mCommerce merchants, and presents an analysis of these merchants' perceptions of the risks and benefits associated with mobile payments. The goal of this study is to inform mCommerce merchants on how to mitigate fraud and its associated costs by wisely choosing and employing the necessary fraud technology solutions.

Fraud definition

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

- Fraudulent and/or unauthorized transactions
- Fraudulent requests for a refund/return; bounced checks
- 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.

Merchant definitions

- Small merchants earn less than $1 million on average in annual sales.
- Medium-sized merchants earn between $1 million to less than $50 million on average in annual sales.
- Large merchants earn $50 million or more in annual sales.
- Large eCommerce merchants accept payments through multiple channels but maintain a strong online presence, earning 10% 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.

Overview

As merchants rush to meet customer demand for accepting mobile payments, fraudsters are similarly shifting their focus. For the 15% of merchants accepting mCommerce payments in 2014, mobile transactions accounted for only 14% of the total transaction volume, but 21% of the volume of fraudulent transactions. mCommerce merchants are currently counterbalancing the astronomical costs associated with mobile fraud (the LexisNexis Fraud Multiplier℠ cost for this channel is $3.34 per dollar of fraud losses) simply due to the low volume of payments accepted via mCommerce. However, discrepancies between mCommerce merchants' biggest fraud pain-points and the solutions they use to combat them indicate that mCommerce merchants are poorly prepared for the growing prevalence of mobile fraud.

Executive summary

Key findings

mCommerce adoption soars to 15% of all merchants. This is more than double the percentage that accepted the channel last year, indicating that the rate of adoption may be increasing as the consumer smartphone and tablet markets mature. Customer convenience is the top reason for adopting the channel, with more than 4 in 5 mCommerce merchants listing this as their primary reason for accepting mobile payments.

More mobile fraud is occurring than should be expected given the respective proportion of mobile transactions. While mobile payments account for only 14% of mCommerce merchants' transactions, this segment of merchants attributes 21% of fraud to mobile transactions. This disproportionate amount of fraud is indicative of the risk inherent in these types of transactions, and mCommerce merchants are aware of this, as 60% say that the evolution of mobile payments represents a significant fraud risk for merchants.

The costs associated with mobile channel fraud are more than three times the initial losses. At $3.34 per dollar of fraud losses, the LexisNexis Fraud Multiplier cost for fraudulent mobile transactions is the highest of any channel. Furthermore, the Fraud Multiplier cost for mobile transactions has increased 18% since 2013, even while the Fraud Multiplier cost for online transactions has decreased 15%. One reason for this uptick in the mobile channel Fraud Multiplier cost is that more physical goods are being sold over the channel, compared with digital goods which dominated its early history.

Despite high costs for mobile fraud, mCommerce merchants still keep overall fraud costs low. This is due to the low percentage of total volume attributed to mobile transactions. Since mCommerce merchants accept payments through the widest variety of channels (4.5 compared with 2.6 for all merchants and 3.9 for eCommerce), the cost distribution is balanced by a mix of low- and high-cost channels.

The mobile web browser remains the most prevalent mCommerce payment-acceptance channel, and the popularity of bill to phone is fast-growing. While mCommerce adoption saw tremendous growth in 2014, there was no significant change in the proportion of mCommerce merchants accepting payments through the mobile browser (67%) or app (49%). The proportion of mCommerce merchants allowing consumers to bill to the mobile phone carrier increased two-thirds over the past year to 35%.

The burden of tracking mobile fraud rests with merchants, as FIs have no reason to track this separately from online channel fraud. Executives in the financial industry agree that there is not enough difference between mobile and online channel transactions to necessitate their tracking these channels separately for fraud. Because most transactions through either channel are CNP transactions, and the liabilities are the same for each channel, FIs treat these transactions the same.

mCommerce merchants suffer disproportionately from international fraud. While internationally-originating payments make up a similar proportion of the total volume of transactions for mCommerce merchants as large eCommerce, mCommerce merchants incur a 20% higher proportion of international fraud than do large eCommerce merchants. Neglecting to use an array of available fraud prevention solutions may be the reason international fraud is slipping by for mCommerce merchants, as the solutions they rate as being most effective at preventing international fraud are not among those they are most likely to actually use.

Recommendations

Track mobile fraud separately from online fraud. This is the only way to accurately assess the need for fraud solutions designed for mobile transactions. As the percentage of fraudulent mobile transactions among all fraud is disproportionate to the percentage of all mobile transactions, it is clear that mCommerce comes with additional risk compared to other payment channels. Only when a merchant is able to disaggregate data by fraud channel will it be able to know where fraud is moving and whether or not solutions are working.

Mitigate high-cost mobile fraud by leveraging solutions optimized for the channel. Among mCommerce merchants, 15% cite a lack of specialized mobile and online fraud solutions as a top fraud challenge, yet use rates are low for online and mobile-oriented fraud prevention solutions such as device identification and geolocation. Supplementing or replacing solutions geared to only prevent fraud on certain types of payments with solutions designed to authenticate mobile transactions can effectively reduce the rate of high-cost mobile fraud.

Review and align priorities for the implementation of fraud prevention solutions, especially if selling internationally. mCommerce merchants consistently display a disconnect between the fraud they encounter and their awareness and use of solutions. In addition to the specific challenges of mobile transactions, mCommerce merchants experience a high proportion of international fraud, yet they are not likely to use the solutions they believe are most effective for preventing fraudulent internationally-originating transactions. Reviewing the dominant fraud types and surveying the marketplace for the most appropriate solutions are in order.

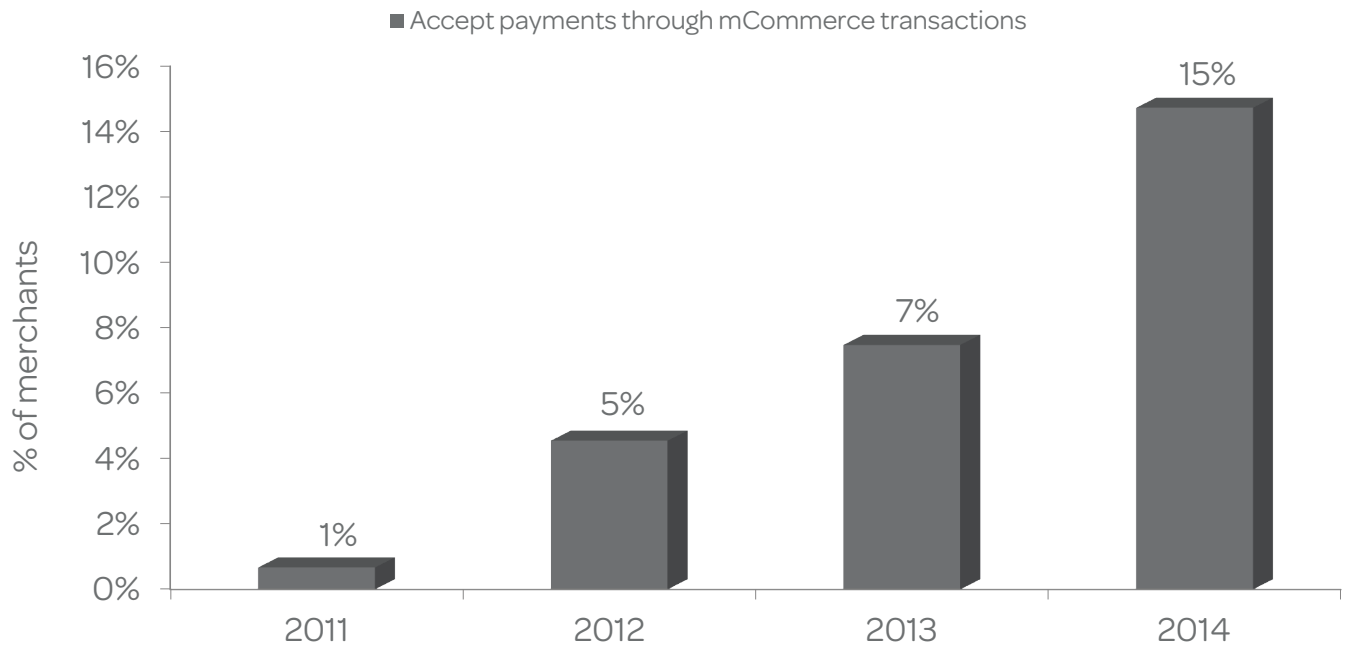
mCommerce adoption

mCommerce channel adoption is skyrocketing as merchants take advantage of the pervasiveness of mobile devices. According to a recent Javelin study, 69% of consumers own a smartphone and 53% own a tablet in 2014.[1] As customers get savvy with technology, they look for accessible and convenient tools for making purchases. Most merchants feel the need to better engage with customers and provide them a hassle-free experience to stay competitive.

Nearly 1 in 4 of all merchants (23%) believes the evolution of mobile payments will have a moderate to significant impact on their overall business strategy (see Appendix, Figure 19). It is of little surprise, then, to see a shift in focus to the opportunities facilitated by mobile payments and to see rapid growth of mCommerce over the past three years (from 1% of merchants accepting these mobile payments in 2011 to 15% in 2014) (See Figure 1).

mCommerce Acceptance More Than Doubles in 2014

Figure 1.Adoption of mCommerce Transactions by Year



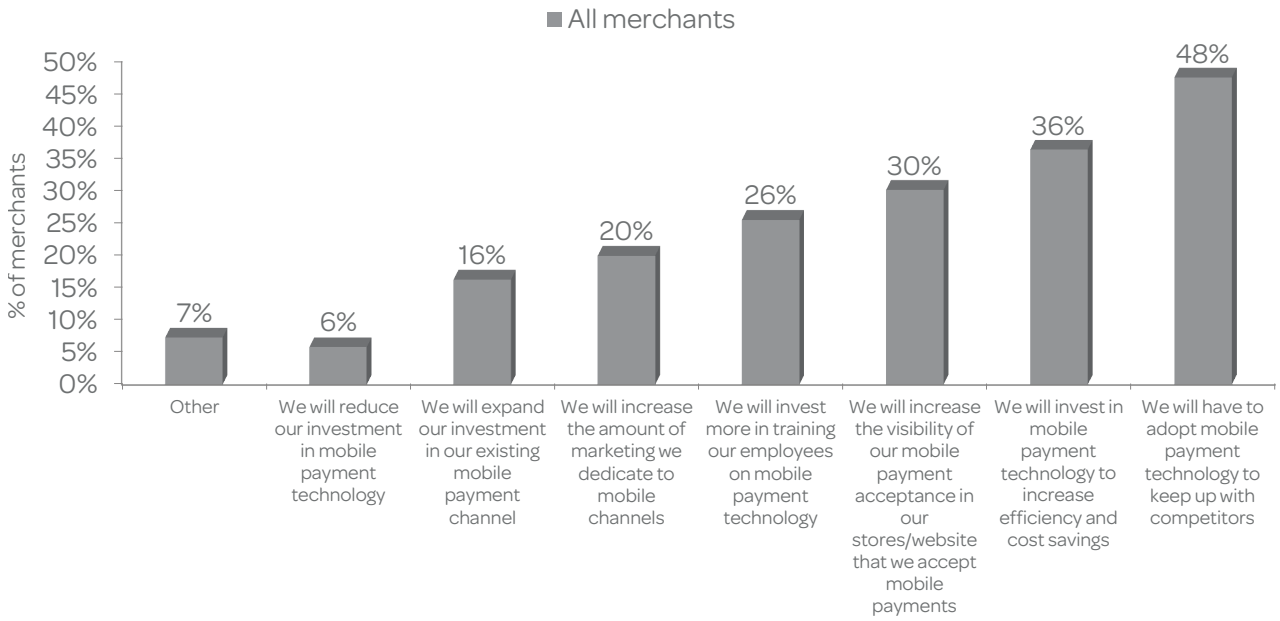
Q. Which of the following mobile payment channels do you currently accept?

March 2014, n varies 1,005 to 1,142
Base: All merchants by year.

Merchants who expect mobile payment technology to have an impact on their overall business strategy outline a variety of steps for taking full advantage. Nearly half (48%) believe that adopting mobile payments is necessary to stay competitive, and over 1 in 3 (36%) plan on investing in this technology to increase efficiency and savings. To ensure a smooth rollout of the channel, 30% of merchants are looking to increase visibility of mobile payment acceptance at their stores and website. Over 1 in 4 (26%) plan on training employees on mobile payment technology, and 1 in 5 merchants plans on increasing marketing efforts dedicated to mobile channels (See Figure 2).

Merchants Plan to Invest In and Increase the Visibility of Mobile Payment Systems

Figure 2. Ways Mobile Payment Technology Will Affect Merchants' Business Strategies



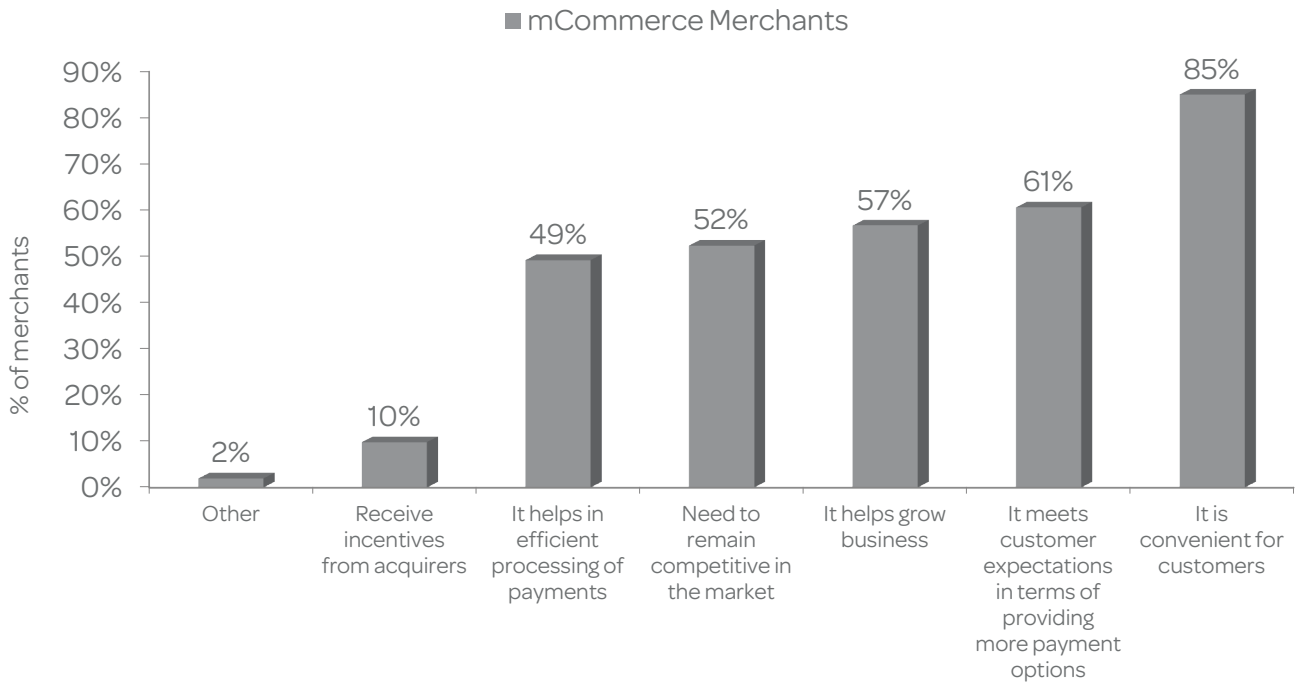
Q. How do you expect emerging mobile payment systems to impact your overall business strategy?

March 2014, n = 612
Base: Merchants who expect mobile to influence their overall business strategy

mCommerce merchants clearly agree that they can no longer afford to dismiss mobile payments if they wish to win over customers and stay competitive. Among the reasons mCommerce merchants gave for accepting mobile payments, the top two pertain to satisfying customer demands (see Figure 3): 85% cited customer convenience as their primary reason and 61% percent cited customer expectations of more payment options.

mCommerce Merchants Name Customer Convenience as the Primary Reason for Adoption

Figure 3. Reasons for Adopting Mobile Payments



Q. You indicated that your company currently accepts payments via mobile device. What were some of the reasons for adopting this payment channel?

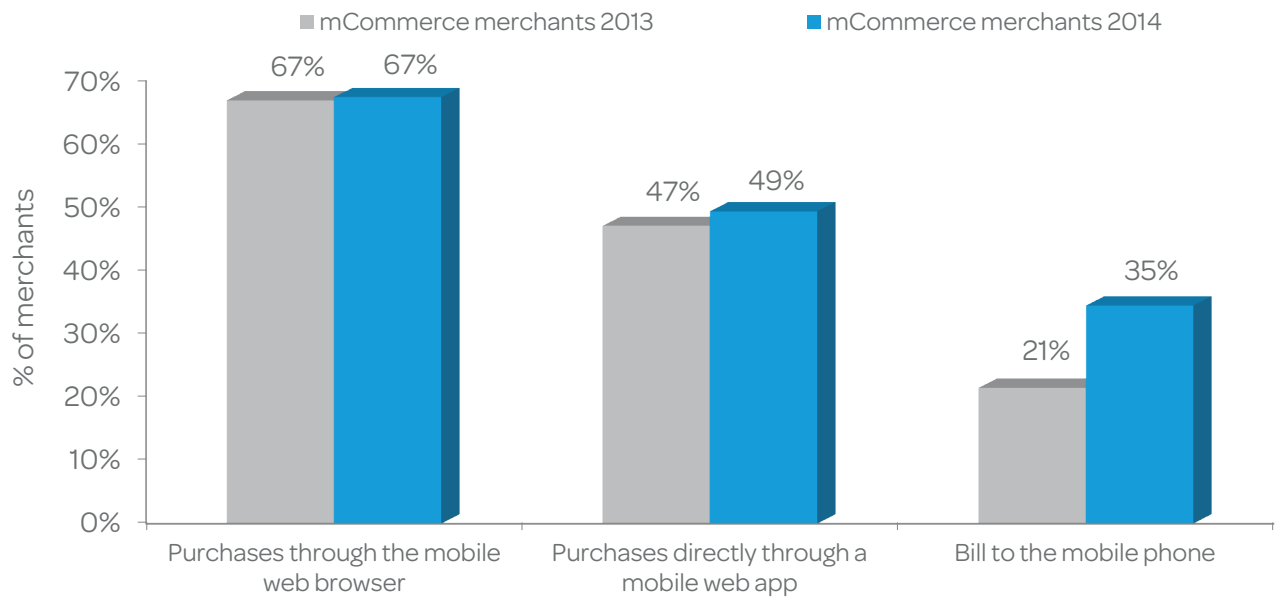
March 2014, n = 255
Base: mCommerce merchants

Mobile browser remains preferred over mobile app, while bill-to-phone acceptance soars

Since last year, little has changed among mCommerce merchants' preference between the mobile browser and mobile app. The mobile web browser is still the most prevalent mobile payment channel among mCommerce merchants, with 67% acceptance for the past two years, while adoption of the mobile app also remains relatively stagnant (see Figure 4).

Bill to Mobile Phone Is Fast-Growing Among mCommerce Merchants

Figure 4.mCommerce Channel Acceptance, 2013–2014



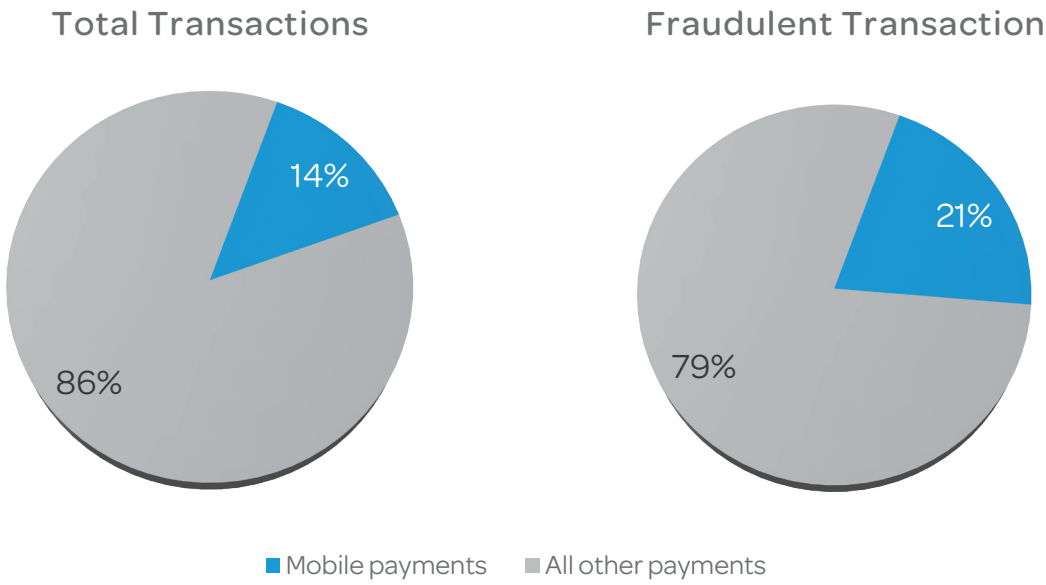
Q. Which of the following mobile payment channels do you currently accept?

March 2014, n = 242, 255
Base: mCommerce merchants by year

It is important to keep the growth of mobile payments in perspective. The proportion of mobile transactions is still low for the average mCommerce merchant: A mere 14% of all transactions are mobile transactions in 2014. However, a disproportionate amount of fraud is attributed to mobile transactions compared with the overall volume of transactions, making up about a fifth (21%) of all fraudulent transactions. The volume of mCommerce transactions will continue to grow, as merchants facilitate the adoption of mobile payment technology to meet customer demands, as witnessed by the dramatic growth in the acceptance of bill-to-phone payments by mCommerce merchants, from 21% in 2013 to 35% in 2014 (see Figure 4). However, merchants must implement a mobile fraud-mitigation strategy to balance the proportion of mobile fraud.

Mobile Fraud Is Disproportionate to the Volume of Mobile Transactions

Figure 5.Volume of Mobile Transactions in Total Transactions and Fraudulent Transactions



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. Q. Please indicate the percentage distribution, to the best of your knowledge, of the payment channels used to commit fraud against your company.

March 2014, n = 123, 255
Base: All mCommerce merchants, mCommerce merchants experiencing > $0 fraud in the past 12 months.

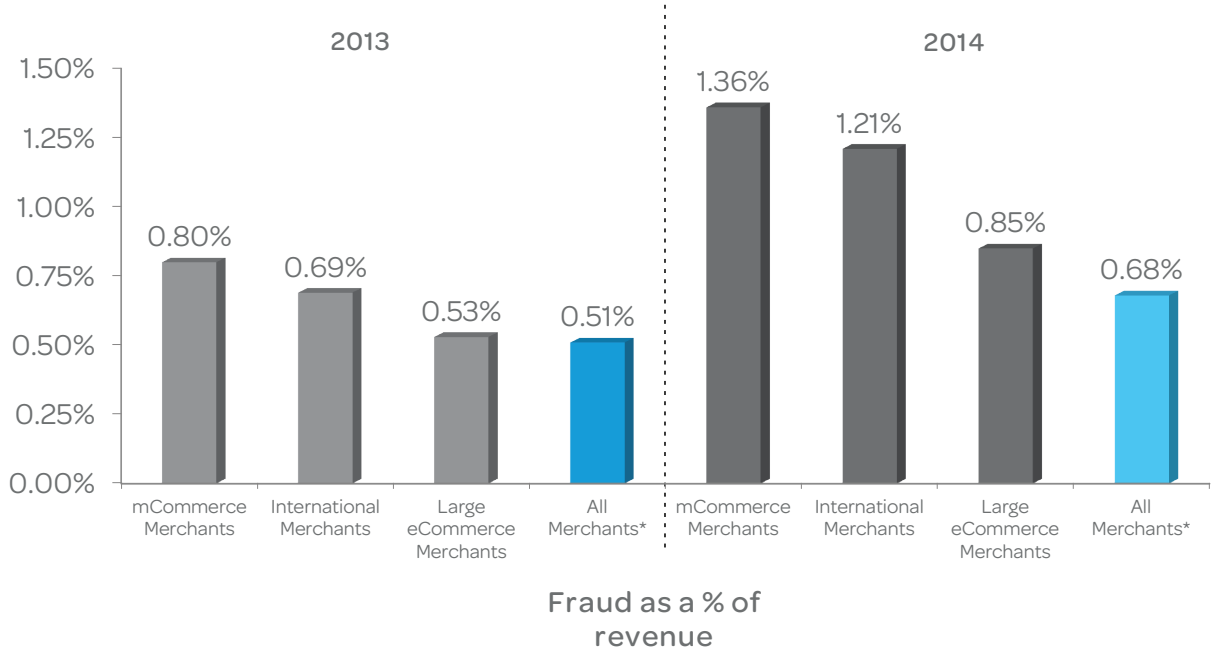
mCommerce fraud overview

Fraud as a percentage of revenue increases sharply

As merchants increasingly adopt mobile payment technology to meet customer demands and keep up with competition, they also have to deal with the consequences of a relatively new but popular mode of payment. mCommerce merchants lost a significantly higher proportion of revenue to fraud than all merchants and large eCommerce merchants for the past two years. This segment of merchants experienced a steep increase over the past year as the percentage of revenue lost to fraud increased 70%, from 0.80% in 2013 to 1.36% in 2014 (See Figure 6). This is primarily due to the proliferation of breached credentials resulting from the numerous data breaches experienced by merchants in the past few years.[2] This, along with fraudsters' increased proficiency in getting unauthorized transactions approved, will keep merchants on their toes in combating fraud.

For the Past Two Years, mCommerce Merchants Lose the Most Revenue to Fraud

Figure 6.Fraud as a Percentage of Revenue for Merchant Segments by Year



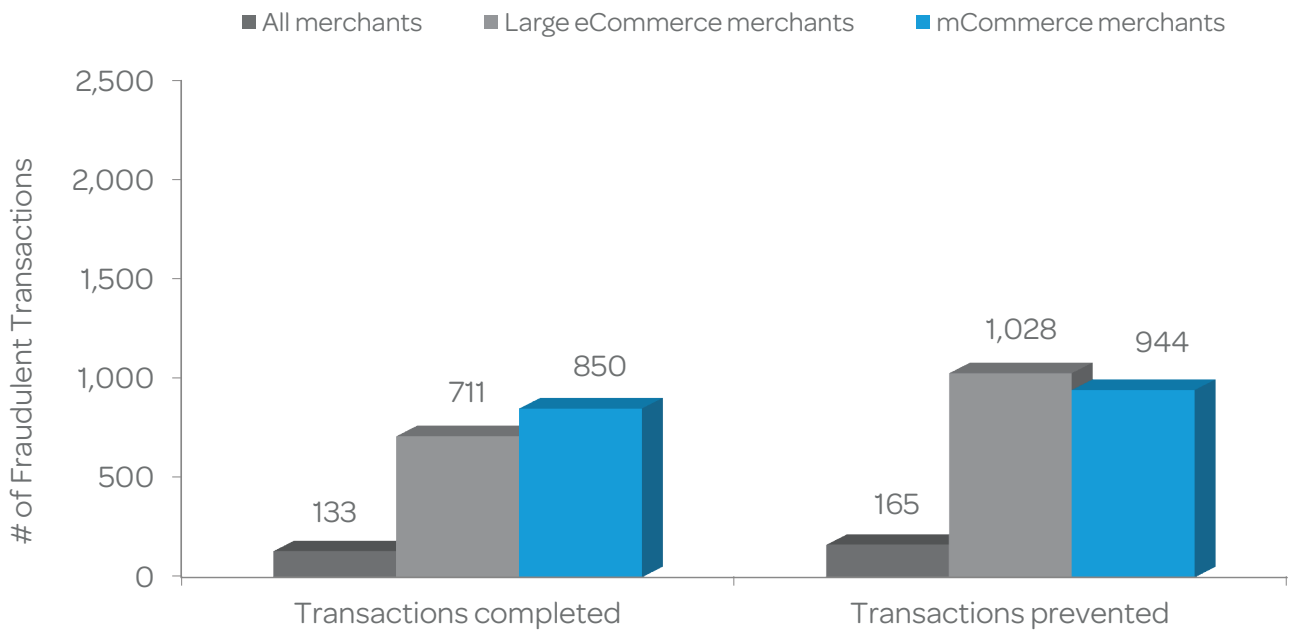
Q: What is the approximate dollar value of your company's total fraud losses over the past 12 months? Fraud losses as a percent of total annual revenue.

May 2013 – March 2014, n = varies 111 - 1,142
Base: All merchants, Large eCommerce Merchants, International Merchants, mCommerce Merchants

The reason for mCommerce merchants' higher losses to fraud is simple: They experience a higher volume of fraudulent transactions. Despite preventing 53% of fraud attempts against them, they report a significantly higher number of successful fraudulent transactions compared with all merchants (850 successful fraudulent transactions vs. 133 reported by all merchants) (See Figure 7). This should be expected given the multitude of payment channels accepted by mCommerce merchants. This segment accepts payments through an average of 4.5 channels, significantly more than the 2.6 channels supported by all merchants and marginally higher than the 3.9 supported by large eCommerce merchants. While supporting multiple channels offers the greatest convenience to consumers, it also presents fraudsters with the widest variety of attack vectors. If any of these channels is not adequately protected, fraudsters' chance of success increases.

mCommerce Merchants Are Under Assault by Fraudsters, With 850 Successful Fraudulent Transactions per Month

Figure 7.Number of Prevented and Successful Fraudulent Transactions per Month by Merchant Segment

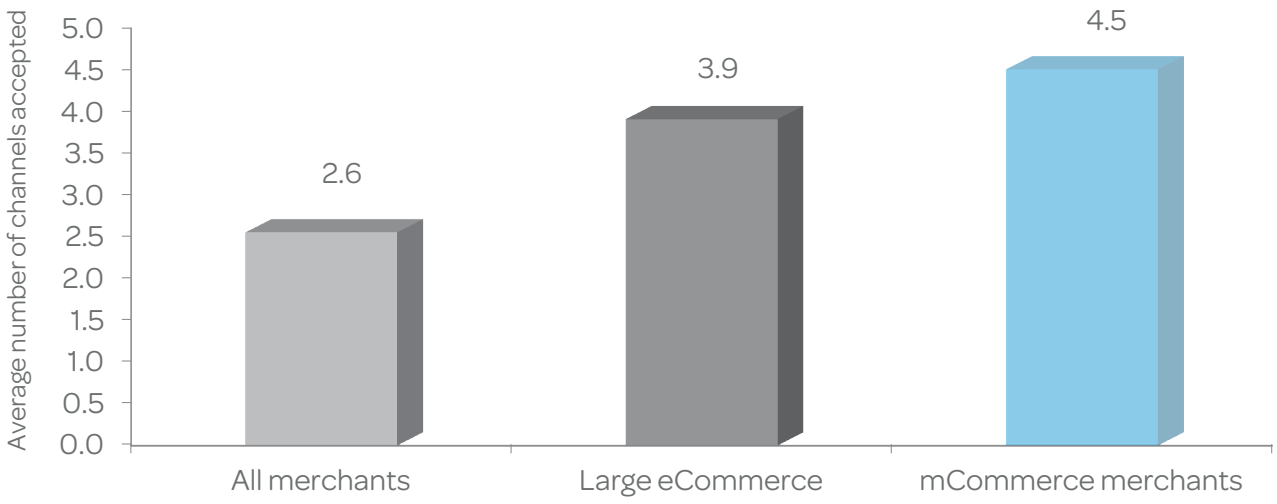


Q: In a typical month, approximately how many fraudulent transactions are successfully completed at your company? Q: In a typical month, approximately how many fraudulent transactions are successfully prevented at your company?

March 2014, n varies 100 to 1,142
Base: All merchants, large eCommerce merchants, mCommerce merchants

mCommerce Merchants Accept Payments through the Most Channels on Average, Benefiting Customers and Fraudsters Alike

Figure 8.Mean Number of Channels Accepted by Merchant Segment



Q. Does your company currently accept payments through any of the following channels? Mean number of channels shown.

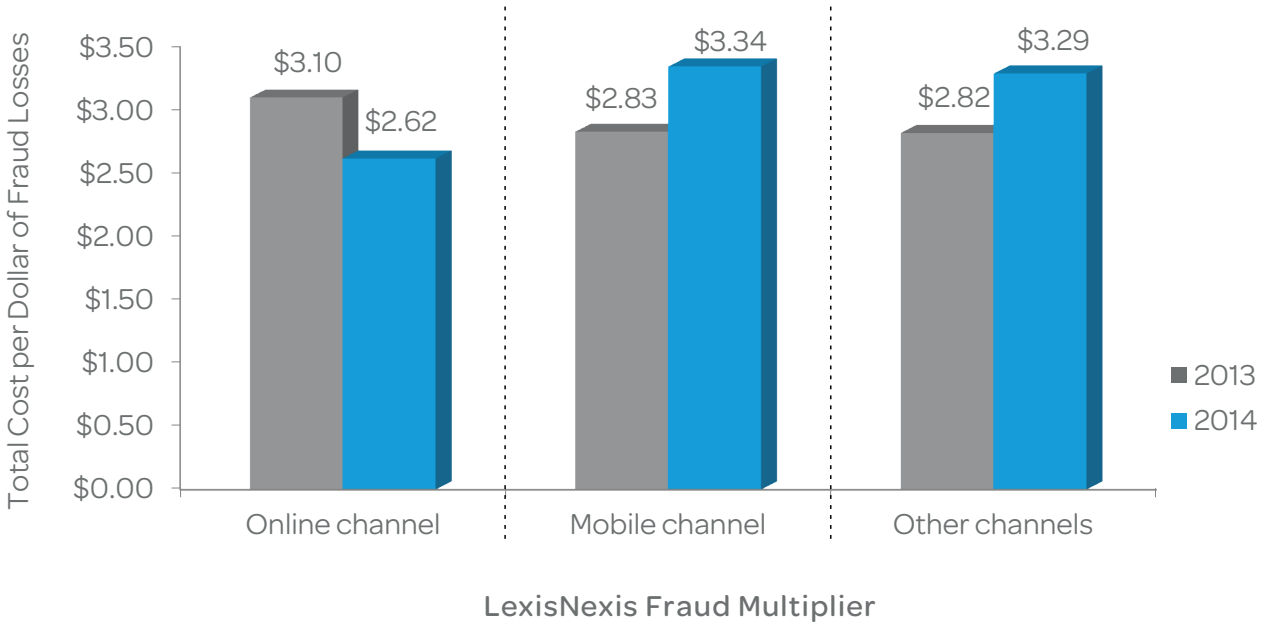
March 2014, n = 1,142, 255, 111
Base: All merchants, large eCommerce merchants, mCommerce merchants

Mobile channel fraud multiplier cost increased dramatically as online channel multiplier declined

While merchants are finding greater success in managing the costs associated with fraudulent online transactions this year (spending only $2.62 per dollar of fraud in 2014, compared with $3.10 in 2013) (See Figure 9), they are unable to manage costs for mobile fraud as successfully. The overall mobile channel LexisNexis Fraud Multiplier cost grew from $2.83 in 2013 to $3.34 in 2014.This isn't surprising given that mCommerce is still in its infancy compared with eCommerce and merchants have yet to adapt their fraud mitigation strategies to mobile-specific challenges, rather than taking a one-size-fits-all approach.

Merchants Pay More per Dollar of Mobile Fraud

Figure 9.LexisNexis Fraud Multiplier Cost by Payment Channel, 2013–2014



Weighted merchant data

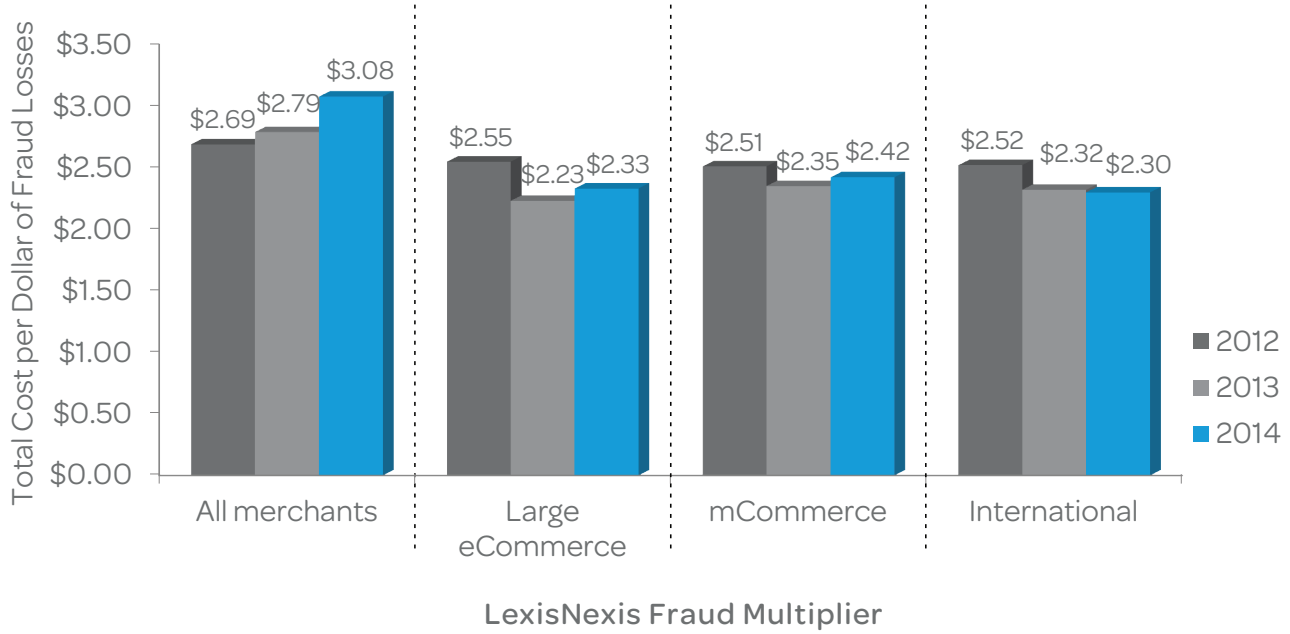
Q: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud costs over the past 12 months.

March 2014, n varies 74 to 181
Base: Merchants experiencing fraud through specific channels in the past 12 months

mCommerce merchants may bear the brunt of higher fraud losses because they are attacked on multiple fronts (see Fraud as a Percentage Of Revenue Section, pg.13), but the LexisNexis Fraud Multiplier cost for mCommerce merchants has been fairly stable, at $2.51 in 2012, $2.35 in 2013, and $2.42 in 2014 (See Figure 10). This stability is due to the fact that mCommerce merchants encompass a wide variety of merchants who benefit from accepting several other channels, thus helping them distribute their costs from overall fraud losses over all channels. Moreover, only 14% of the total transactions completed at mCommerce merchants were mobile transactions, partly mitigating the contribution that the high mobile channel Fraud Multiplier cost has on mCommerce merchants' bottom line.

mCommerce Merchants' Overall Fraud Costs per Dollar of Losses Are Lower Than for All Merchants

Figure 10.LexisNexis Fraud Multiplier Cost Across All Channels Accepted by Merchant Segment



Weighted merchant data

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

July 2012– March 2014, n varies 41 to 712
Base = Merchants experiencing >$0 fraud in the past 12 months by segment

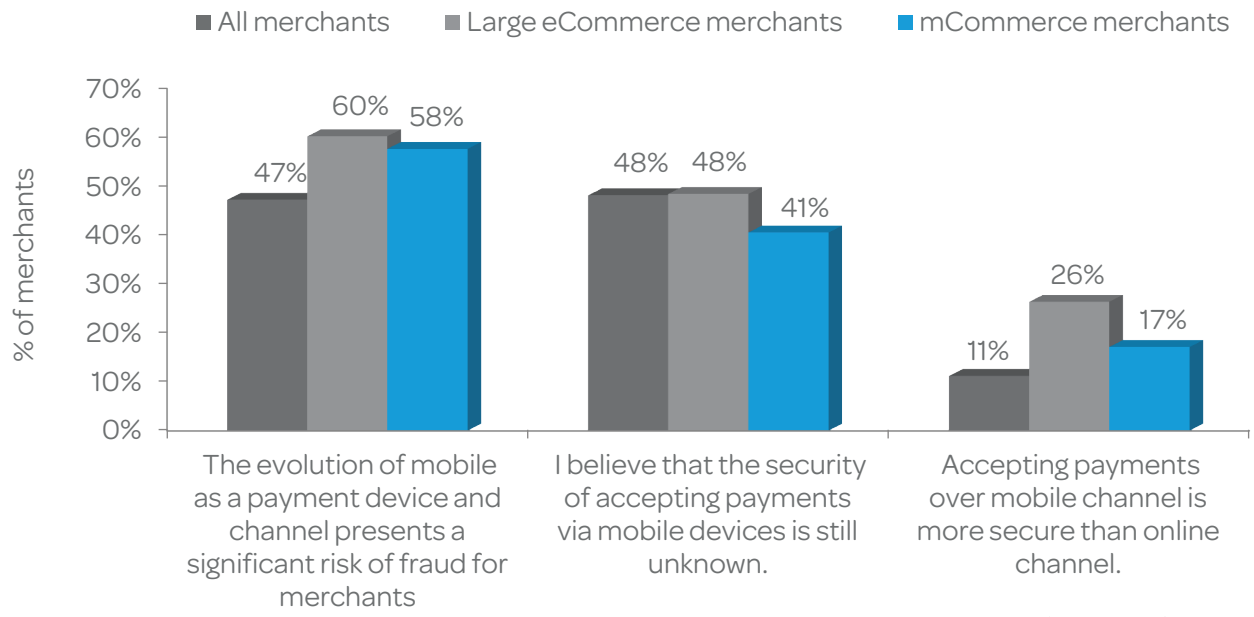
Mobile payments prompt concern over fraud, but data thought to be secure

In the wake of their fraud losses and costs, mCommerce merchants are more likely than all merchants to believe that mobile payments pose a significant fraud risk to merchants (61% vs. 47%). However, a smaller percentage — though still significantly higher than all merchants — believes that accepting mobile payments is more secure than accepting payments through the online channel (26% vs. 11%).

While these responses may seem contradictory, they could actually indicate that merchants perceive a difference between fraud risk and data security risk pertaining to mobile payments. Regarding fraud, merchants still need to implement mobile fraud-specific solutions to control fraud risk. Since mobile payments are still emerging and evolving, they are not yet as large a target for data compromise as the point-of-sale or online channels. There is promise that this will continue as mobile payment solutions such as Apple Pay and broader tokenization schemes from payment industry groups will effectively render mobile payment data unusable for would-be thieves.[3,4]

mCommerce Merchants Perceive a Significant Fraud Risk from Mobile Channel Payments

Figure 11.Attitudes Toward Mobile Payments Security



Q. On a scale of 1 to 5, please indicate the extent to which you agree or disagree with each statement listed below.

March 2014, n varies 111 to 1,142
Base: All merchants, large eCommerce merchants, mCommerce merchants

Financial institution perspectives

Tracking fraud channels remains a merchant's burden

Good communication over payments fraud is the basis for a powerful partnership between merchants and financial institutions. When it comes to tracking mCommerce fraud, there is a significant disconnect between these parties. Over half of mCommerce merchants track fraud by payment acceptance channel, and they find that a disproportionate number of fraudulent transactions are mobile transactions (See Figure 5). Financial institutions, on the other hand, generally do not track mobile channel fraud separately from the online channel.

The reasons FI executives cite for not tracking mobile fraud are twofold: Mobile channel payments are not big enough yet, and they are not significantly different from online channel payments to make tracking separate channels worthwhile. While the first reason may soon be invalidated by the burgeoning volume of mCommerce, that the liability for fraudulent CNP transactions resides with the merchant regardless of the device on which the transaction originated means that mobile and online fraud are not meaningfully different to the FI. This leaves the onus for preventing and detecting mobile fraud primarily to merchants.

Intermediate parties confound FIs' advanced analytic aspirations

Whether or not FIs eventually find it in their interest to track mobile fraud, some payment types often used through the mobile device are confounding their ability to achieve optimal granularity on some of the key variables they do track. Alternative payments used for online and mobile transactions, including Amazon and PayPal, are often linked to bank-issued cards or DDA accounts, but the payment provider may withhold some transaction details (e.g., location of transaction, items purchased). This withheld data represents important inputs into FIs' fraud detection models, limiting their ability to identify suspicious activity using alternative payment methods, further shifting the burden to merchants and alternative payment providers.

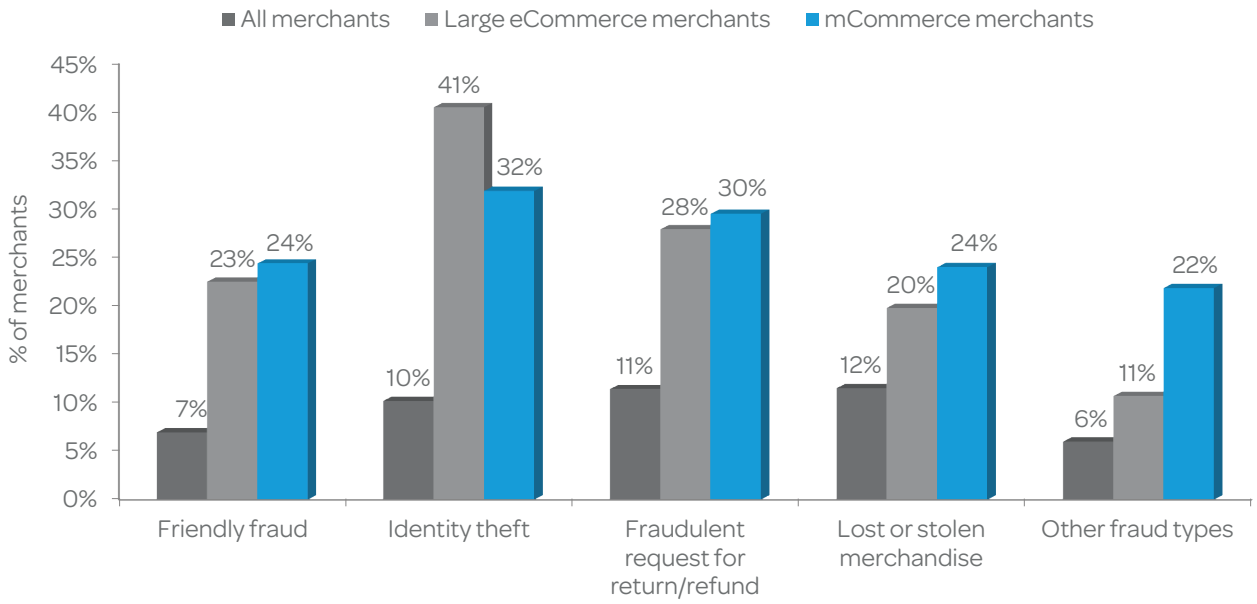
The specific impact of different fraud types

Customer identification and verification are essential to fraud mitigation for merchants. At the same time, customer experience — among the top reasons for accepting mobile transactions — depends on low-friction identity verification and authentication solutions. mCommerce merchants need to balance effectiveness with optimization for the mobile device.

In 2014, mCommerce merchants attributed 24% of fraudulent transactions to friendly fraud (See Figure 12). This will continue to be a challenge until merchants can more closely tie the legitimate customer to his or her device, making transactions irrefutable. Despite the promise that mobile channels hold for improved authentication, a failure to deploy effective solutions has also allowed fraudsters to misuse stolen customer payment information (see mCommerce Merchants and Fraud Prevention section, pg. 29).

mCommerce Merchants Experience More of Every Fraud Type Compared With All Merchants on Average

Figure12.Distribution of Fraud Types by Merchant Segment



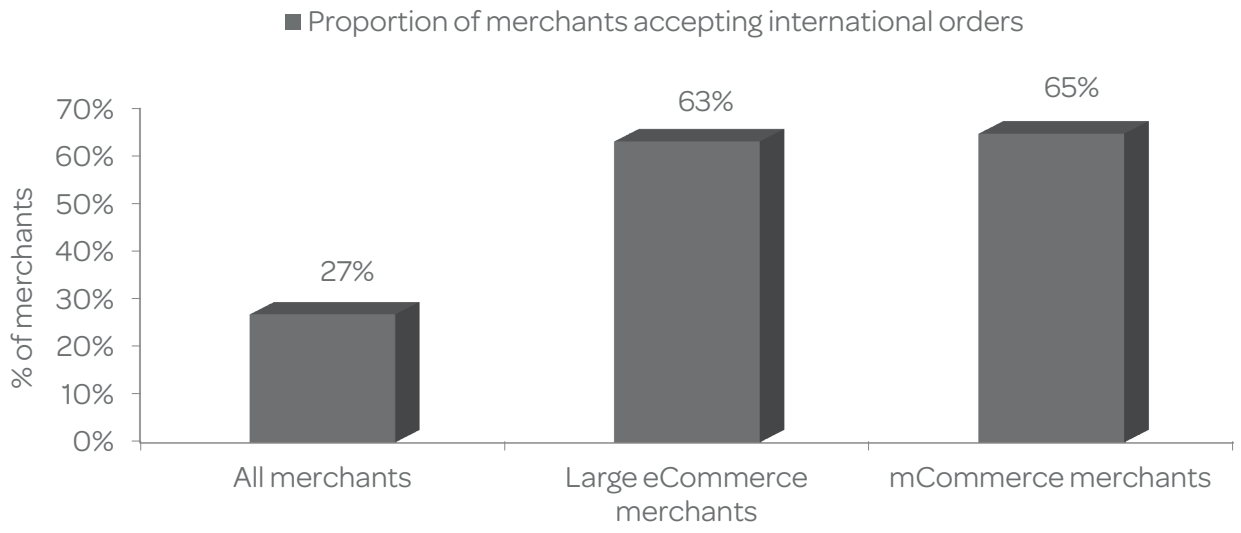
Q. Please indicate whether the incidence of each of the following fraud types has increased, decreased, or stayed the same over the past 12 months, for your company. "Increased" responses shown.

March 2014, n = 1,142, 255, 111
Base: All merchants, large eCommerce Merchants, mCommerce merchants

mCommerce merchants are just as likely to accept international orders as large eCommerce merchants, showing that they are not shying away from the challenges associated with international trade (See Figure 13). Yet as they must stretch their fraud mitigation capabilities further than other merchant segments, they are experiencing more of a challenging circumstance in dealing with international fraud.

mCommerce Merchants Most Likely to Accept International Orders

Figure 13.International Order Acceptance by Merchant Type



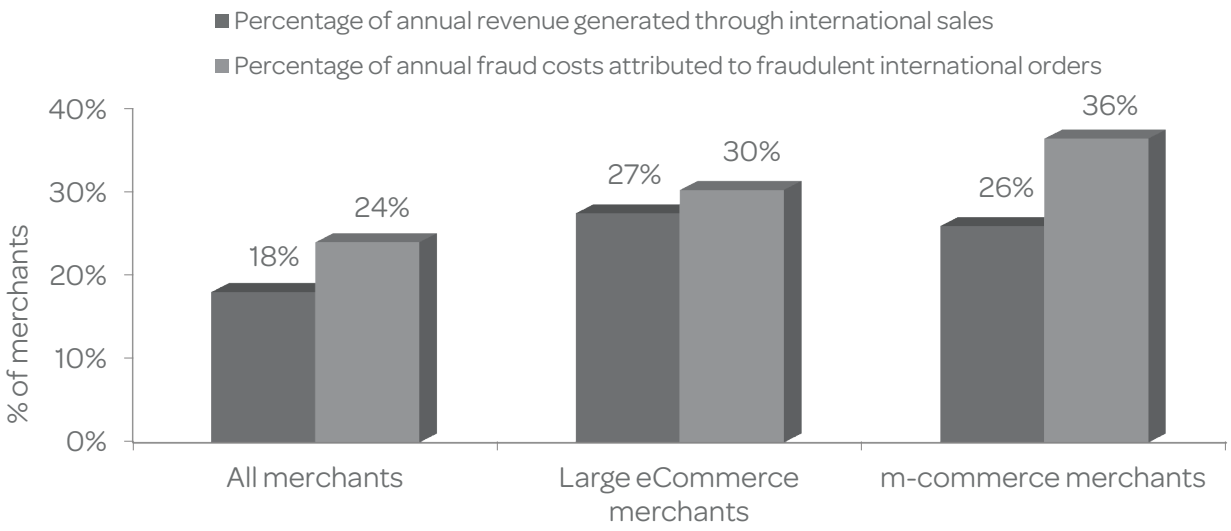
Q. Does your company currently sell merchandise to customers outside of the domestic US?

March 2014, n = 1,142, 255, 111
Base: All merchants, large eCommerce Merchants, mCommerce merchants

While mCommerce merchants receive a similar proportion of transactions from international sales as large eCommerce merchants (26% and 27% respectively), they experience a 20% higher proportion of fraudulent transactions originating internationally (See Figure 14). Clearly, mCommerce merchants face a higher risk of international fraud compared with other merchants, which makes it imperative for them to leverage more effective fraud solutions for both customer and device verification.

mCommerce Merchants' Proportion of Revenue from International Sales Comparable to Large eCommerce Merchants, But Suffer Disproportionate Fraud from Them

Figure 14.Percentage of Revenue and Fraud Costs Related to International Sales by Segment



Q. Please indicate the percent of annual revenue generated through domestic compared to international sales in the last 12 months. International sales shown.
Q. Please indicate, to the best of your knowledge, the percent of fraud costs generated through domestic orders compared to international orders in the last 12 months. Fraudulent international orders shown.

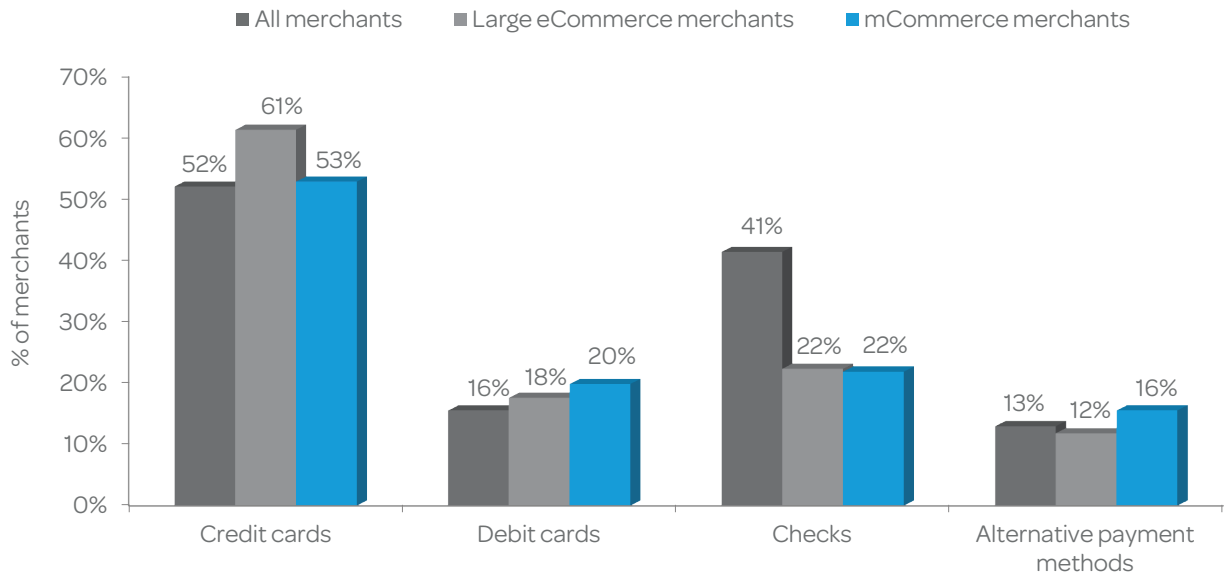
March 2014, n varies 65 to 307
Base: All merchants, large eCommerce merchants and mCommerce merchants accepting international orders

Impact of different payment methods

Fraudulent credit card transactions make up the highest volume of fraudulent transactions for mCommerce merchants accepting credit cards, the same as what other merchants are experiencing. However, compared with other merchant segments, mCommerce merchants implicate debit cards and alternative payments in a greater proportion of fraudulent transactions. This may have to do with the younger demographic primarily responsible for mCommerce purchases, as this group also tends to use debit cards and alternative payments more heavily as a result of their tech savvy and relative lack of credit-maturity.[5]

Credit Cards Attributable in 53% of Fraud Cases for mCommerce Merchants Who Accept Them

Figure 15.Proportion of Fraudulent Transactions Attributed to Payment Methods



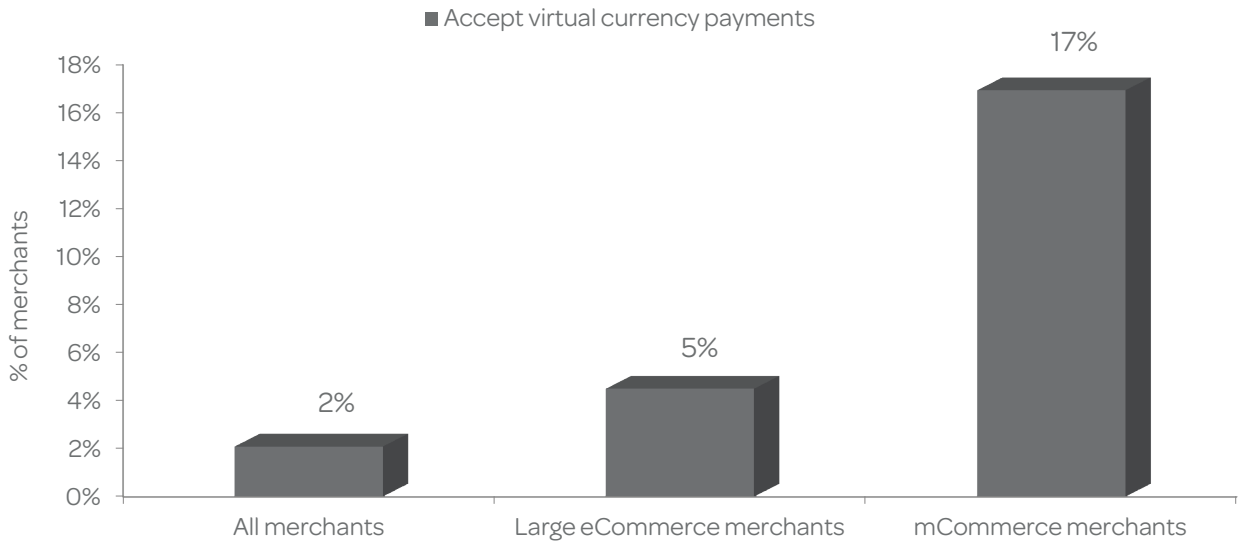
Q. Please indicate the percentage distribution, to the best of your knowledge, of the payment methods used to commit fraud against your company.

March 2014, n varies 31 to 341
Base: All merchants, large eCommerce merchants, mCommerce merchants experiencing > $0 fraud by specific payment types

mCommerce merchants are more than three times as likely to accept virtual currency as large eCommerce merchants (See Figure 16). One of the most highly-touted advantages of using virtual currencies is that this payment method does not require merchants to verify customer identities, potentially reducing the risk for both merchants and consumers.[6] Although virtual currency makes up only 10% of the transaction volume for mCommerce merchants who accept it, 26% of those who accept it say fraud using this payment method increased in the past 12 months, suggesting that no payment method is without risk.

mCommerce Merchants Are More Than 8 Times as Likely to Accept Virtual Currency Than All Merchants

Figure 16. Virtual Currency Acceptance by Merchant Type



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. Virtual currency shown.

March 2014, n = 1,142, 255, 111
Base: All merchants, large eCommerce Merchants, mCommerce merchants

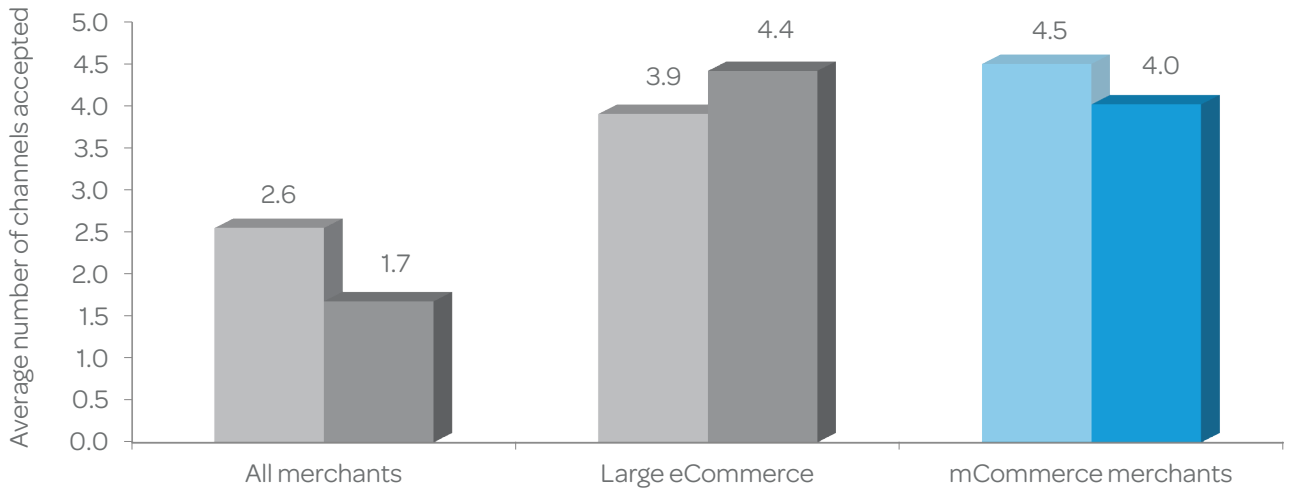
mCommerce merchants and fraud prevention

mCommerce merchants are playing a higher-stakes game than other merchant segments when it comes to fighting fraud. mCommerce merchants are more likely to accept payments through a higher number of channels compared with all merchants and large eCommerce merchants. Accepting payments through more channels means that mCommerce merchants are forced to fend off attacks on all sides. It is no wonder that mCommerce merchants are more likely than all merchants to believe that fraud is inevitable (56% vs. 49%) (see Appendix, Figure 22), since they are stretched thin to fight fraud on multiple fronts.

With the exception of some analytic solutions, fraud prevention solutions are best-suited to only a single channel or payment method. Thus, it makes sense that the more channels through which a merchant accepts payments, the greater the number of fraud prevention solutions it should employ. The lower number of solutions per channel employed by mCommerce merchants suggests that they are not defending themselves quite as well as large eCommerce merchants (though both are still better protected than all merchants). This makes sense, as mCommerce merchants lament the limited availability of mobile-specific solutions. Lack of effective prevention tools for online and mobile channels is the second-most-cited fraud prevention challenge for mCommerce merchants (15% of mCommerce merchants said this was their top challenge for preventing mobile fraud, representing a 44% increase over 2013) (see Appendix, Figure 21).

mCommerce Merchants Must Fight Fraud on More Fronts, But Use Slightly Fewer Fraud Prevention Solutions Than Large eCommerce Merchants

Figure 17.Number of Payment Channels Supported by Merchant Segment



Q. Does your company currently accept payments through any of the following channels? Mean number of channels shown.
Q: Which of the following best describes your awareness and use of the fraud solutions listed below? My company currently uses the solution.

March 2014, n = 1,142, 255, 111
Base: All merchants, large eCommerce merchants, mCommerce merchants

Yet while mCommerce merchants bemoan the dearth of mobile-specific fraud solutions, they are neglecting to use the ones that do exist. Device fingerprinting, for instance, is among the best-suited solutions for mobile device authentication. Device identification can be used with both mCommerce card transactions and alternative payments, along with the benefit of being invisible to the consumer (adding no friction to the checkout process). Yet this solution is used by only 14% of mCommerce merchants (See FIgure 18).

Card verification values (CVV), on the other hand, are designed only to prevent CNP fraud, add friction to the customer experience, and are prone to misuse. CVV requires additional data entry, which is cumbersome on a mobile keypad, and even then this credential is relatively ineffective since it is liable to be compromised through malware or online data breaches along with the card numbers. 3D Secure, on the other hand, is a supplemental authentication protocol that leverages the cardholder's relationship with the issuer to verify their identity during an online transaction. This solution does not rely on easily compromised static data, yet is used by just over half as many merchants as CVV.

While the obvious recommendation is to shift to using solutions that are more effective and generate less friction for mCommerce channels, mCommerce merchants indicate that cost may be prohibitive. Twenty-seven percent of mCommerce merchants believe that it costs too much to control fraud. This is a significantly higher proportion than of all merchants, who also lose a lower percentage of revenue to fraud and incur lower fraud-related costs per dollar of losses.

mCommerce Merchants Are Overly Reliant on Card-Specific Solutions, Neglecting Mobile-Specific Solutions

Figure 18.Use of Fraud Prevention Solutions by mCommerce Merchants

Q. Which of the following best describes your awareness and use of the fraud solutions listed below? Current users.

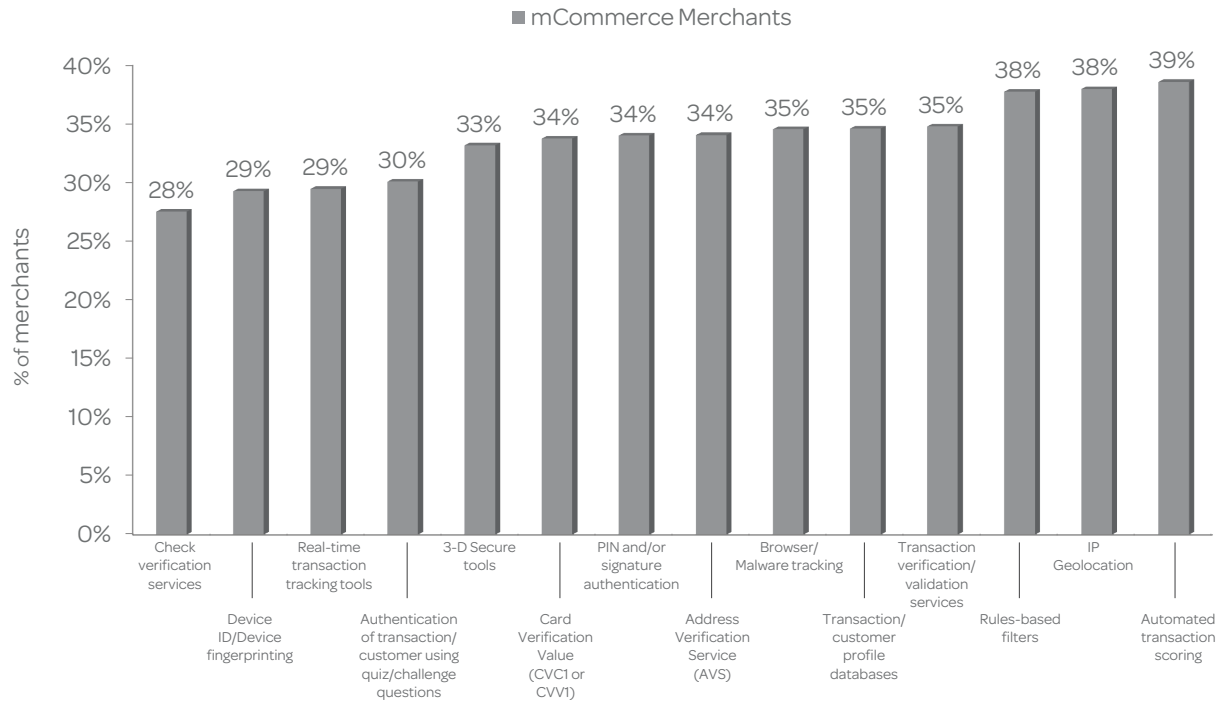
March 2014, n = 255
Base: mCommerce merchants

Mobile transactions, global threats

Mitigating international fraud has been particularly challenging for mCommerce merchants, who suffer a disproportionate amount of international fraud compared with the volume of transactions originating internationally. Interestingly, mCommerce merchants who are aware of various fraud prevention solutions do not show vast differences in their perceptions of the effectiveness of these solutions against international fraud. However, the solutions mCommerce merchants are most likely to perceive as effective against international fraud (automated transaction scoring [39%], IP geolocation [38%], and rules-based filters [38%]) are among the least likely to be in current use by mCommerce merchants (17%, 19%, and 24% use these solutions, respectively). (See Figures 18 and 19) This fact beckons merchants to assess their fraud pain points and adjust their use of solutions to those best-suited to their needs.

mCommerce Merchants Differentiate Very Little Among Technology Solutions When Evaluating Their Effectiveness at Preventing International Fraud

Figure 19.Perceived Effectiveness of Fraud Technology Solutions for Preventing International Fraud

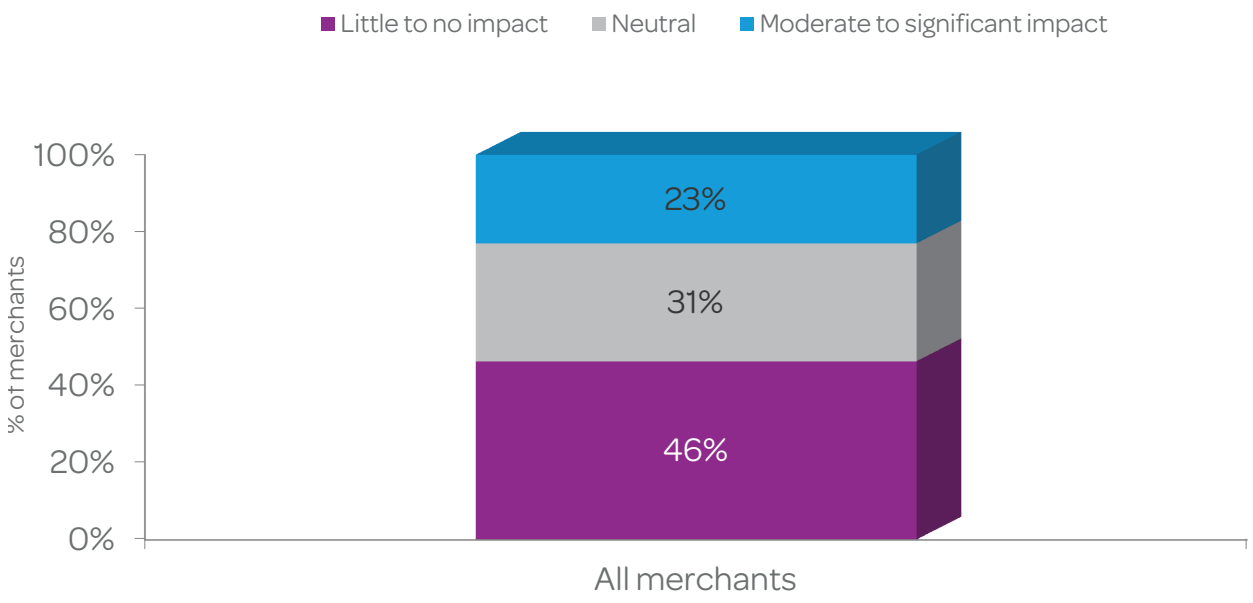


Q. Which of the following fraud solutions do you believe are effective for preventing the following fraud types? International fraud show.

March 2014, n varies 198 to 248
Base: mCommerce merchants who have heard of specific solutions

Nearly a Quarter of All Merchants Believe Mobile Payments Will Affect Business Strategy

Figure 20.Effect of Mobile Payment Acceptance on Overall Business Strategy

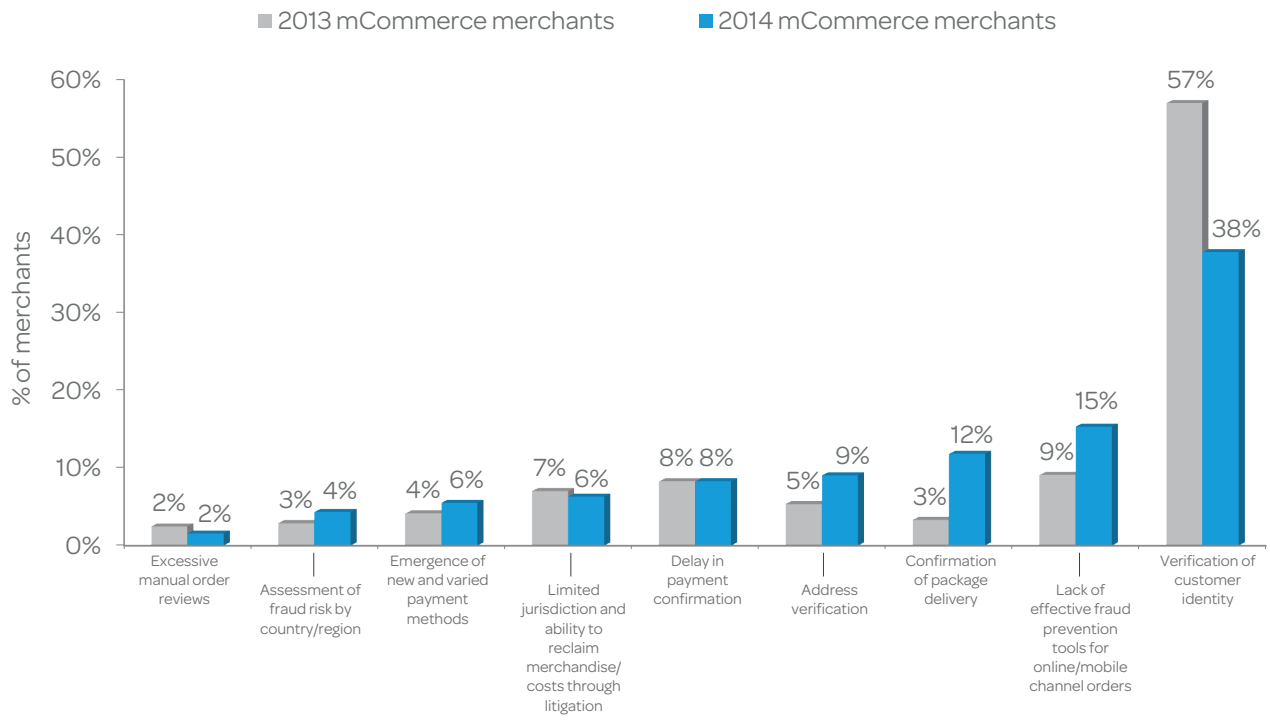


Q. To what extent do you expect the evolution of mobile as a payment device or a payment channel to impact your overall business strategy?

March 2014, n = 1,142
Base: All merchants

Fewer mCommerce Merchants Stress Over Identity Verification, But Lack of Effective Online/Mobile Fraud-Prevention Tools Seen as a Bigger Challenge

Figure 21.mCommerce Merchants' Top-Ranked Challenges for Preventing Mobile Fraud

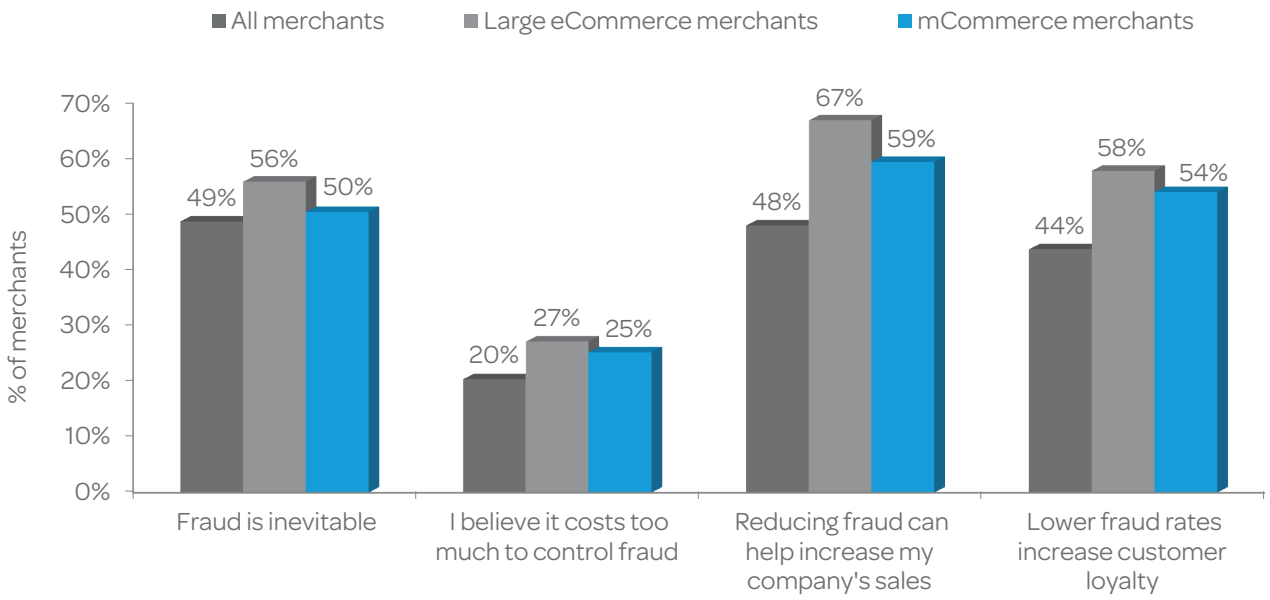


Q. Please rank the top 3 challenges related to fraud faced by your company when selling merchandise to customers using Mobile channel (payments accepted via mobile device). Top-ranked challenges shown.

March 2014, n = 242, 255
Base: mCommerce merchants by year

One in Four mCommerce Merchants Believes it Costs Too Much to Control Fraud

Figure 22.Fraud Attitudes by Merchant Type



Q. On a scale of 1 to 5, please indicate the extent to which you agree or disagree with each statement listed below.

March 2014, n varies 111 to 1,142
Base: All merchants, large eCommerce merchants, mCommerce merchants

Sources

[1] Consumer Survey, Javelin Strategy & Research, November 2014.

[2] 2014 Data Breach Fraud Impact Report: Consumers Shoot the Messenger and Financial Institutions Take the Bullet, Javelin Strategy & Research, June 2014.

[3] http://www.zdnet.com/article/apple-pay-and-security-could-tokenization-be-the-tool-that-curbs-data-breaches/, accessed January 6, 2014.

[4] http://digitaltransactions.net/news/story/Tokenization-Plays-the-Central-Role-in-Visa_s-New-Cloud-Payment-Suite, accessed January 6, 2014.

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

[6] http://btctheory.com/2013/10/30/fraud-chargebacks-and-bitcoin/

For more information:

Call: 866.818.0265
Visit: lexisnexis.com/retail-ecommerce
Or email retailsolutions@lexisnexis.com

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, we provide 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 Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

All information provided in this document is general in nature, is provided for educational purposes only, and may contain errors. It should not be construed as legal advice. For legal advice applicable to the facts of your particular situation, you should obtain the services of a qualified attorney licensed to practice in your state.

About Javelin Strategy & Research
Javelin Strategy & Research, a division of Greenwich Associates, provides strategic insights into customer transactions, increasing sustainable profits for financial institutions, government, payments companies, merchants and other technology providers.

The views expressed by Javelin Strategy & Research are not necessarily those of LexisNexis.

The opinions and quotes expressed in this paper are those of the interviewees and do not necessarily reflect the positions of LexisNexis.