Annual Report

2014 LexisNexis® True Cost of Fraud℠ Study

Post-Recession Revenue Growth Hampered by Fraud As All Merchants Face Higher Costs

August 2014

LexisNexis®

Risk Solutions
Retail

Table of contents

Table of figures

Introduction

This annual LexisNexis study establishes the actual cost of fraud borne by U.S. merchants, along with key findings and specific guidance for the industry. Recommendations for mitigating these costs are presented based on an analysis of the underlying drivers of fraud, how different merchant segments are responding to these challenges, and through insight from financial industry leaders.

The key question that this report addresses for merchants is, "How do I grow my business, managing the true cost of fraud, while strengthening customer trust and loyalty?

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.
- International-selling merchants are those operating from the U.S. and doing business globally, including those that accept international orders or ship merchandise outside the U.S.
- Domestic-only merchants do not sell merchandise outside the U.S.
- 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.

Executive summary

Overview

For merchants, the past year was one of the most difficult on record, as a number of factors conspired to challenge their fraud prevention efforts. A combination of several massive data breaches flooding the black market with stolen card numbers, expansion into unknown territory in terms of mobile and alternative payments and virtual currency, and fraudsters' last-ditch effort to make use of counterfeit cards before the implementation of EMV left merchants the worse for wear. Merchants lost, on average, 0.68% of revenue—a 33% greater proportion than the previous year. Merchants also incurred more costs in addition to their fraud losses, with each dollar of fraud costing them $3.08, compared to $2.79 last year.

Though online merchants prospered from a rebounding economy to the tune of a nearly $30 billion increase in online spending this year, large eCommerce and mCommerce merchants are still among the hardest-hit by rising fraud losses and associated costs. International merchants escaped some of the worst of this trend as fraud costs remained mostly stable this year. Unfortunately, fraud loss as a percent of revenue nearly doubled for this segment since last year.

Key takeaways

- **Merchants are paying more per dollar of fraud in 2014 ($2.79 in 2013 to $3.08 in 2014), driven by an increase in costs associated with mobile-channel fraud as more physical-goods retailers begin to accept mobile payments.** Mobile-channel frauds cost merchants $3.34 per dollar of fraud losses, while "other" channels (including mail and telephone) experienced similar fraud costs at $3.29 per dollar of fraud. This is dramatically higher than the online channel at only $2.69 in fees per dollar of fraud.
- **Merchants are also losing a significantly higher percentage of revenue to fraud this year, at 0.68%, compared to 0.51% in 2013.** This increase in fraud losses is the result of a higher volume of fraudulent transactions completed against merchants this year. The average merchant suffered 133 successful fraudulent transactions per month this year, up 46% from last year.
- **Fraudsters keep up the pressure online in the burgeoning online channel.** Consumer spend is on the rise while criminals continue to steal customer PII and payment information for fraudulent misuse. Forty-two percent of merchants who support online channels are reporting an increase in fraud, matching that of 2013.
- **Controlling card fraud may not be easy even with EMV implementation.** EMV protects users at the POS with highly secure "chip-and-PIN" authentication, but the physical card must be present for this technology to be utilized. Although skimming and in-store card fraud may see a further decline in card fraud with EMV implementation, CNP fraud will continue, giving merchants a run for their money.
- **The year of data breaches has taken a toll on the integrity of consumer identities.** Using sophisticated programs to hack into merchants' databases, criminals are becoming very successful in their data breach attempts, leaving consumers and merchants on the hook for fraud committed with the stolen credentials. As breaches increase, so does the relationship between breaches and ID fraud victimization, with 1 in 3 data breach victims suffering identity fraud in 2013. Further, incidents of existing card fraud (ECF) rose to 4.6% in 2014 from 3.14% in 2013.
- **Large eCommerce merchants and International merchants are hard-hit by fraud.** Large eCommerce merchants not only pay more per dollar of fraud, up to $2.33 in 2014 from $2.23 in 2013, but they also saw an increase in the amount of fraud loss to revenue, from 0.53% in 2013 to 0.85% in 2014. For international merchants, the fraud multiplier is only marginally down, by 2 cents, from $2.32 in 2013 to $2.30 in 2014, but fraud losses grew significantly as a percent of revenue, from 0.69% in 2013 to 1.21% in 2014.
- **International merchants are first-movers toward accepting virtual currency, with ambiguous implications for fraud.** Eleven percent of international-selling merchants currently accept virtual currency (11 times the rate of their domestic-only counterparts). International merchants accepting virtual currency were also twice as likely as all virtual currency-accepting merchants to have experienced an increase in fraud through this payment method in the past 12 months. Certain types of virtual currencies cannot be charged back, however. While this fact is to the detriment of consumers, it reduces the cost to merchants of accepting this risky payment type.

Recommendations

- **Track fraud and its related costs by channel and payment method.** Every payment method and channel entails a unique risk-profile and requires different steps for mitigation. Only by tracking can merchants assess the need for investment in fraud prevention solutions; certain solutions may be more tailored to the areas where fraud costs are highest. Communicating with payment providers and FIs about the distribution of fraud across payment types and channels can help the industries present a united front against fraud.

- **eCommerce merchants should utilize a layered approach to fraud prevention.** Merchants accepting online transactions are experiencing a greater proportion of fraud through this channel in 2014 (51%, compared to 42% in 2013). This could be a result of fraud beginning to shift to the online channel in anticipation of EMV. Large eCommerce merchants tend to over-rely on CVV in online card transactions, and this segment uses fewer fraud-prevention solutions in 2014 compared to 2013. No one solution is perfectly effective against online fraud, so eCommerce merchants should take advantage of compensating controls to verify the customer identity, device, and payment method being used to make remote purchases.

- **mCommerce merchants, and those considering accepting the channel, should implement fraud prevention solutions that specifically address threats to this channel.** Mobile is a growing fraud channel that carries the same fraud liabilities as other CNP transactions, except in the case of contactless NFC payments. As mCommerce expands beyond the digital-goods realm, the costs associated with this fraud type increase. Solutions such as device fingerprinting and geolocation are among the options best-suited for mobile transactions.

- **Stay ahead of data security requirements. Becoming complacent in an age of massive data breaches is both a financial and reputational hazard.** Customer attrition, falling stock prices and the cost of remediation all threaten businesses whose customer PII caches are compromised. Furthermore, data breaches make all merchants more vulnerable to fraud because they increase the stolen PII in circulation.

- **Raise thresholds for card fraud detection at the POS, at least temporarily.** The vast majority of card numbers compromised in breaches in 2013 included the CVC1 data required for POS purchases, but not the CVC2 data which allow customers to use for CNP transactions. Until EMV is widely implemented or criminals' caches of stolen card numbers are exhausted, counterfeit cards will proliferate in fraudsters' last-ditch effort to use them at the POS. Extra caution is advised in light of this trend.

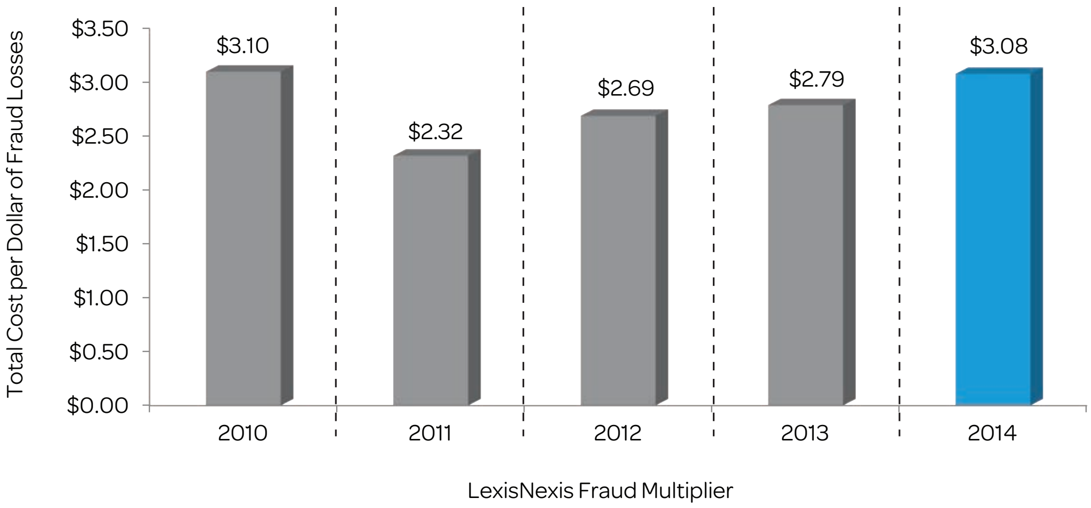
- **Do not rely on EMV to eliminate fraud—tokenization must be used in conjunction with 3-D Secure because multi-channel merchants are attractive data-breach and fraud targets.** While EMV is highly effective at preventing POS fraud, when used for eCommerce purchases card data is still vulnerable to compromise and subsequent misuse – including static CVC2 data. 3-D Secure provides for improved authentication of the cardholder during eCommerce and mCommerce transactions, reducing the efficacy of fraudsters' attempts to misuse card data compromised from a breach. And merchants can safely store and transmit tokens as proxies for primary account numbers (PANs) during authorization without the fear of compromise, because they are often more limited in their use than true card data and are also more easily replaced.

2014 fraud at a glance

General findings for all merchants

The LexisNexis Fraud Multiplier™ has risen for the third consecutive year, with merchants reporting that they are paying from $3.08 for each dollar of fraud losses in 2014, up from $2.79 in 2013 (See Figure 1). As merchants adopt new payment technologies, they are also faced with increased costs resulting from fraud through these channels. The primary driver for the rise in fees is mCommerce, where merchants who accept mobile payments are paying $3.34 for each dollar of fraud losses, compared to online channel or other channels, where merchants providing those payment channels are only paying $2.62 and $3.29 for each dollar of fraud losses (See Figure 2).

Figure 1.LexisNexis® Fraud Multiplier™, 2010 to 2014

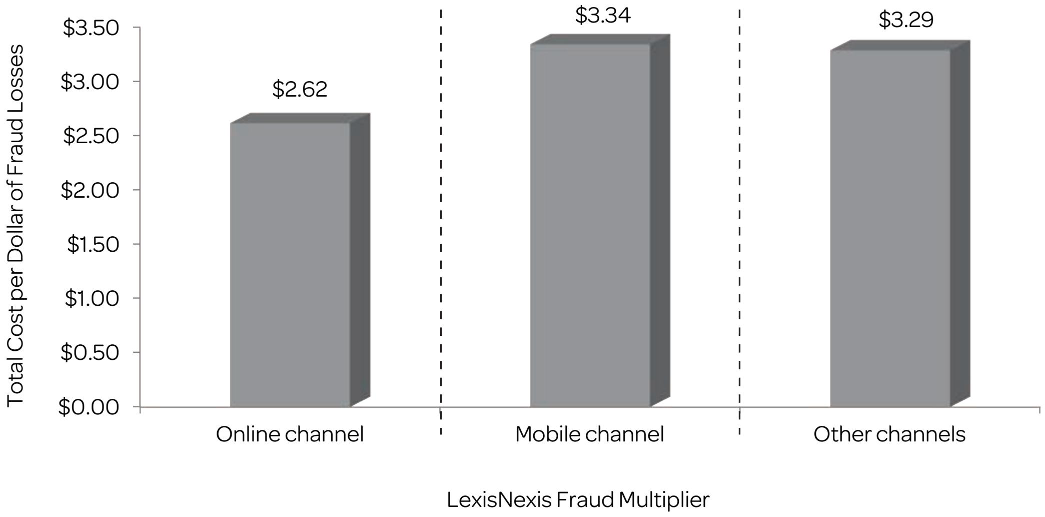


*Weighted merchant data

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.

July 2011 – March 2014, n varies 145 to 712
Base= Merchants experiencing fraud in the past 12 months

Figure 2.LexisNexis® Fraud Multiplier, by Channel



*Weighted merchant data

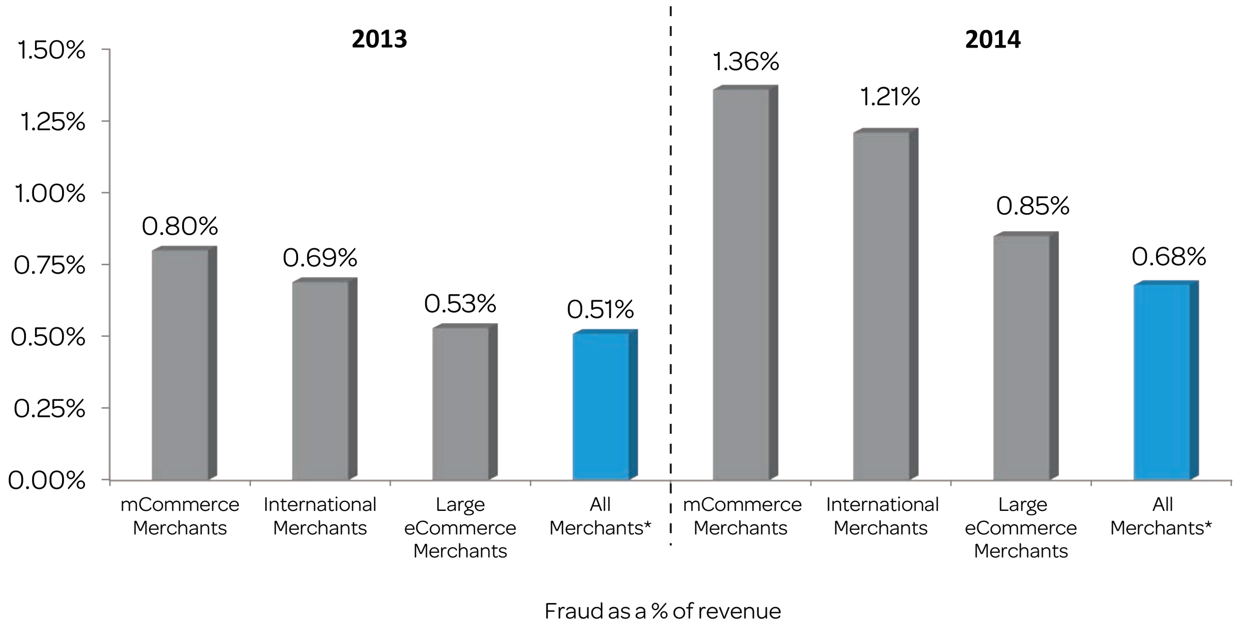
Q: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud costs over the past 12 months.

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

The percent of revenue lost to fraud is up in 2014

Along with the increase in the LexisNexis Fraud Multiplier costs, fraud losses have also increased as a percentage of revenue in 2014, reversing the drop from the previous year. Overall, merchants are reporting fraud loss as a percent of revenue at 0.68% this year compared to 0.51% in 2013 (See Figure 3).

Figure 3.Fraud As A Percent Of Revenue By Merchant Segment, 2013-2014



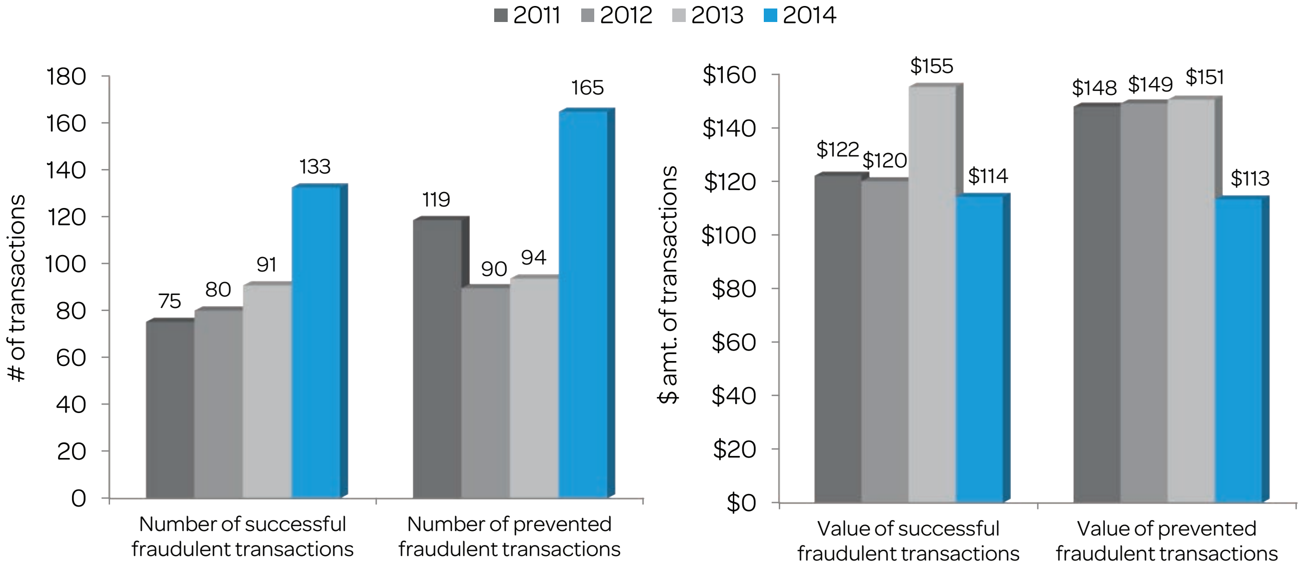
*Weighted merchant data

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.

May 2013 – March 2014, n = varies 118 - 1,142
Base: All merchants, Large eCommerceMerchants, International Merchants, mCommerce Merchants

The primary driver of this increase is the sheer number of successful fraudulent transactions reported by merchants this year. Although the average value of a successful fraudulent transaction fell this year ($155 in 2013 vs. $114 in 2014), fraudsters are bombarding merchants with 61% more attempts at fraudulent transactions—only 55% of which are prevented (See Figure 4). The number of successful fraudulent transactions has shown an upward trajectory since 2011, but has never exceeded a 15% increase in number of transactions in a single year. That rate tripled in the past 12 months, however, as the number of successful fraudulent transactions skyrocketed from 91 to 133.

Figure 4.Number of Fraudulent Transactions Prevented and Completed for All Merchants, 2011-2014

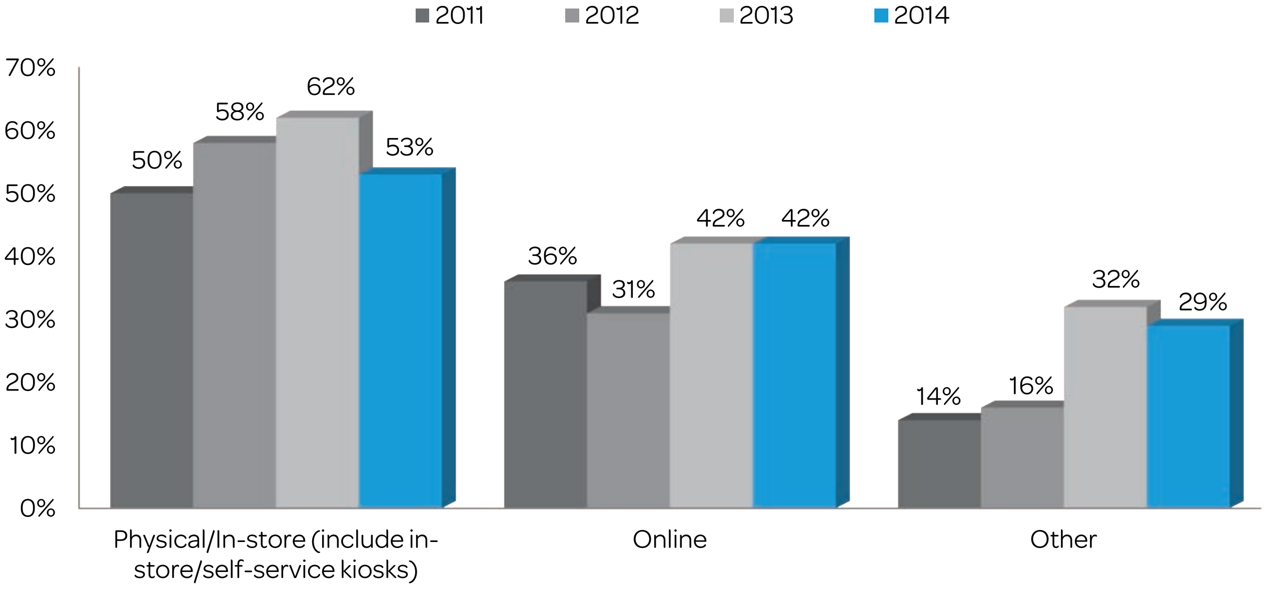


Q. In a typical month, approximately how many fraudulent transactions are prevented by your company? Q. Thinking of the fraudulent transactions that are prevented, what is the average value of such a transaction? Q. In a typical month, approximately how many fraudulent transactions are successfully completed at your company? Q. Thinking of the fraudulent transactions that are successfully completed, what is the average value of such a transaction?

March 2014, n = 100, 581
Base: All merchants, large eCommerce merchants experiencing specific fraud types

On one hand, merchants should be rejoicing at the increase in consumer spending, which is emblematic of a rising economy. Javelin's annual consumer payments survey estimates that the total volume of online payments will increase from $351.9 billion in 2013 to $378.6 billion in 2014.[1] On the other hand, this continues to make the online channel attractive to criminals even while their focus on other channels is on the decline. Merchants accepting payments through the online channel attributed over two-fifths (42%) of the fraud they faced to the online channel, equal to 2013. Merchants accepting physical, in-store payments, however, attributed the lowest proportion of the frauds against them to this channel since 2011. (See Figure 5).

Figure 5.Percent Of Fraudulent Transactions Attributable To Channels Among Merchants Accepting Specific Channels



*Weighted merchant data

Q: Thinking about the total fraud losses suffered by your company in the past 12 months, to the best of your knowledge, what is the percentage distribution of fraud over the following sales channels.

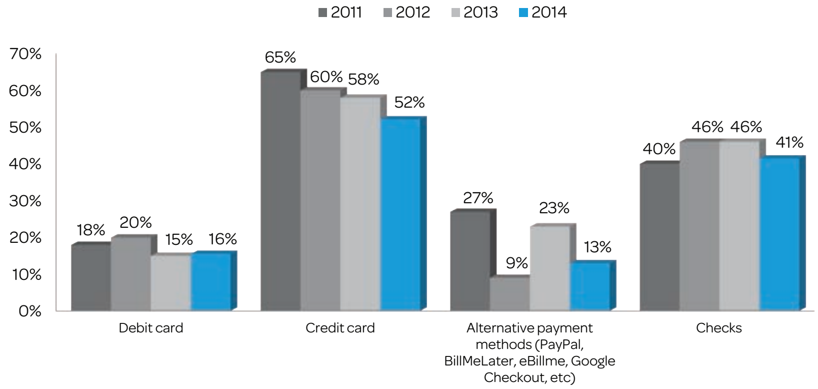
July 2011 – March 2014, n varies 58 to 176
*Base= Merchants experiencing fraud amount greater than $0 in the past year and accept payments through particular channels

Card fraud “declines” yet again in 2014

Data breaches have ensured the accessibility of cheap stolen card numbers and personal information obtained by criminals by hacking merchant databases. Yet despite the flood of such stolen card numbers in the market, credit card-accepting merchants continue to attribute a declining proportion of the frauds against them to this payment method. The primary contributor to this trend is not a real decline in credit card fraud, but rather an increase in the number of payment methods accepted by merchants who also accept credit cards (4.8, up from 3.3 in 2013). This has caused the volume of credit card transactions to fall as a proportion of all transactions for the average credit card-accepting merchant (from 43% in 2013 to 39% in 2014), even as credit cards make up a greater proportion of the total volume of retail payments in the U.S., and likely has the same effect on fraud.[2,3]

EMV technology is expected to have a real downward effect on credit card fraud at the POS. Although CNP fraud may still be lurking around even after EMV technology is implemented, it is expected to control ongoing card skimming and in-store card fraud. Trends with alternative payment fraud, on the other hand, have fluctuated for the past few years. After merchants accepting alternative payments attributed 23% of fraud to this payment method in 2013, this proportion has dropped to 13% in the past year, much closer to the 2012 level of 9% (See Figure 6). This volatility may mirror trends in breaches of user login credentials for alternative payments, and malware targeting the same. Fraudsters are using an array of payment methods to defraud merchants, as no single payment method comes out as the main target of fraud, keeping merchants guessing as to how they will be hit.

Figure 6.Percent Of Fraudulent Transactions Attributable To Payments Methods Among Merchants Accepting Specific Payment Methods



*Weighted merchant data

Q: In thinking about which payment methods are most commonly linked to fraudulent transactions, please indicate the percentage distribution, to the best of your knowledge, of the payment methods used to commit fraud against your company.
Means.

July 2011 – March 2014, n varies 58 to 246
Base= Merchants experiencing fraud amount greater than $0 in the past year and accept particular payments methods

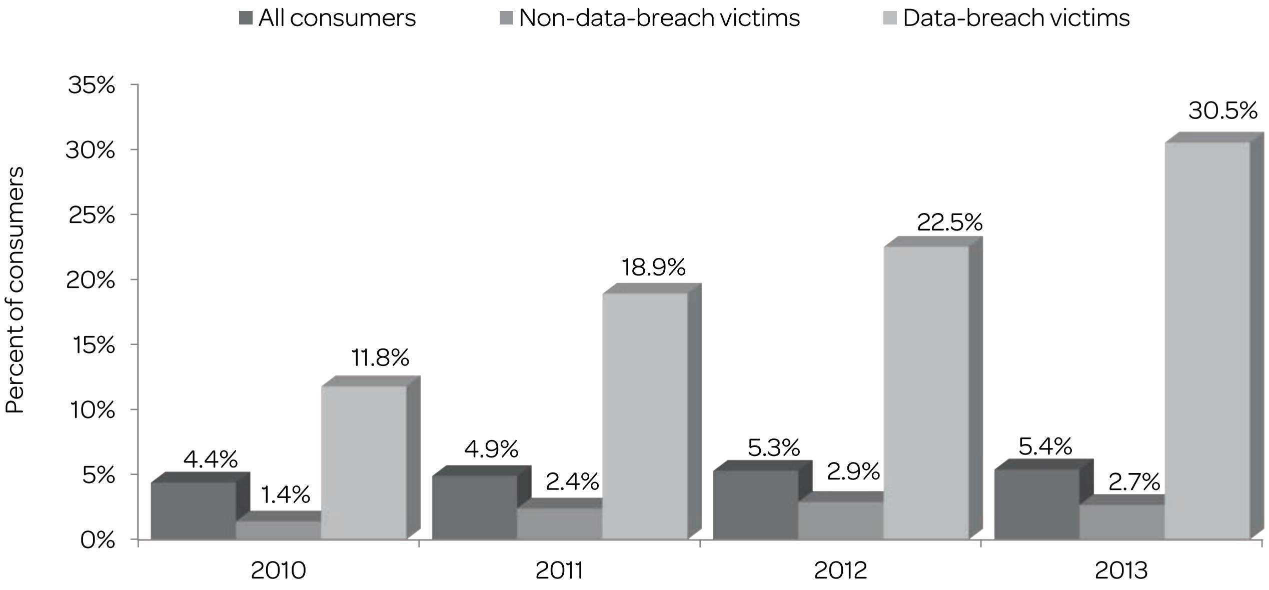
> “Everyone looks at Europe and says look, they implemented EMV and card present fraud went away, and when the US implements EMV card-present fraud will be gone. Fraudsters have to eat just like you and me, so the fraud is going to go somewhere and it will be interesting to see where it goes.”
>
> Executive, Mid-Sized Card-Issuing Institution

Identity fraud 360°: Consumers, financial institutions and merchants

Spotlight: Consumers

Data breaches are a constant threat to businesses and consumers, with nearly 1,500 confirmed breaches in 2013.[4] Not only has the frequency of breaches escalated, but so has the number of records compromised. Over the years, the relationship between data breach and fraud victimization has done nothing but grown, increasing from nearly 1 in 9 consumers in 2010 to nearly 1 in 3 in 2013 (See Figure 7).

Figure 7. Rate of Identity Fraud for All Consumers, Data Breach Victims and Non-Victims (2010-2013)

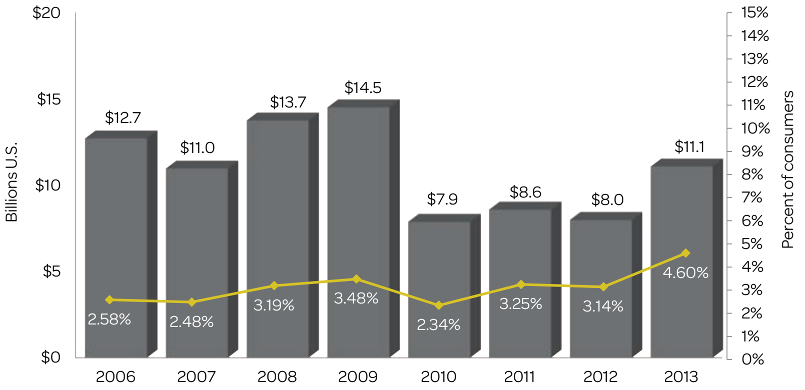


Q2: In the last 12 months, have you been notified by a business or other institution that your personal or financial information has been lost, stolen, or compromised in a data breach?

October 2010 - 2013, n = varies 337 - 5,634
Base: All consumers, data breach victims, non data breach victims

Given the preponderance of card numbers among the tens of millions of records compromised in 2013, it is not surprising that existing card fraud (ECF) skyrocketed in the same year, (to 4.6% incidence, up from 3.14% in 2012)[5] and the total fraud loss due to ECF at a whopping $11 billion, up from $8 billion in 2012.[6] (See Figure 8).

Figure 8.Total Existing Card Fraud Losses and Incidence Rate by Year

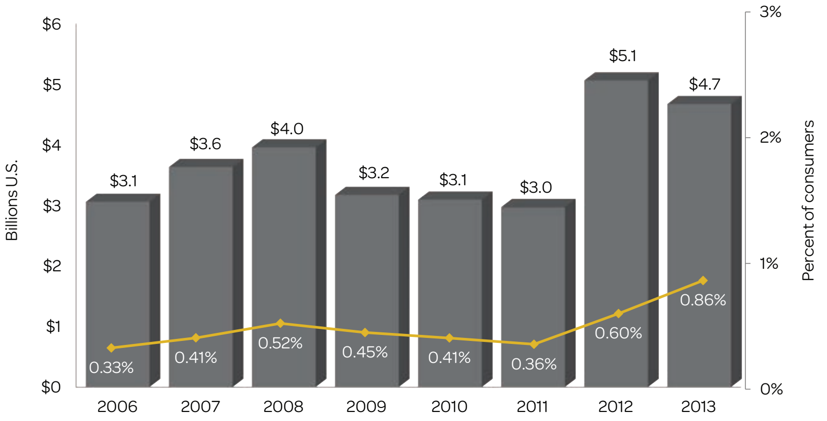


October 2006 - 2013, n varies 5,006 -5,634
Base: All consumers

> "The volume of cards exposed is up a bit, even normalized for recent breaches, but the sense of urgency among criminals is to do more [card fraud]. There is an elevated incident rate, but the methodologies have all remained the same."
>
> Executive, Large Card-Issuing Financial Institution

Account takeover (ATO) fraud has also steadily risen, with incidence of 0.86% in 2013, up from 0.60% in 2012, and is holding its ground in terms of fraud losses at $5 billion for the second year in a row (See Figure 9).Credit card accounts surpassed DDA accounts to become the most commonly taken-over account type in 2013 (36% of account takeovers affected a credit card account, compared to 28%, which involved a DDA account). While previously composing a negligible proportion of cases, internet account takeovers and email payment accounts surged this year to 8% and 15% respectively. All of these types of account takeovers may negatively impact merchants, because credit cards may be merchant-issued, or other credit cards or email payment accounts may be used to make fraudulent purchases with a merchant. When online merchant accounts are compromised, criminals may use customers' saved payment information in authenticated merchant portals to make fraudulent purchases.

Figure 9.Total Account Takeover Fraud Losses and Incidence Rate by Year



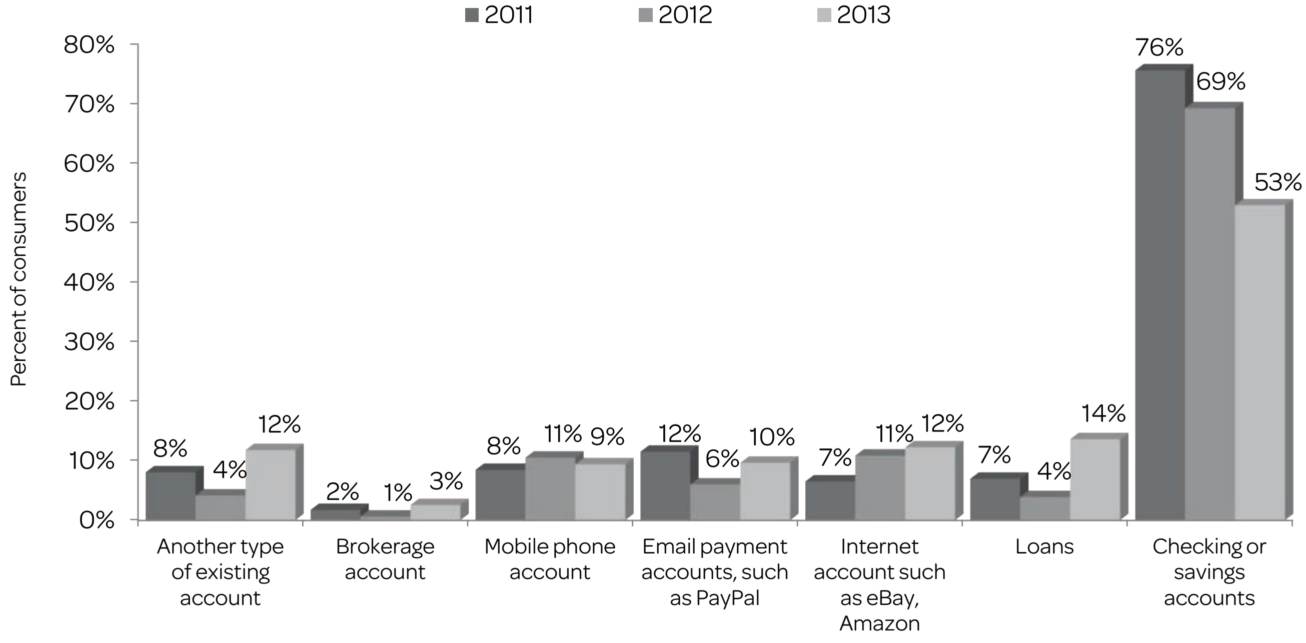
October 2013, n= varies: 5,006 -5,634
Base: All consumers

> "Fraudsters are now taking the next step as opposed to just getting the card data, going out and trying to use it. They are doing their due diligence based on card holder name or whatever data that they're getting, and are able to [use these] personal identifiers to call into the call center, to make transfers into the DDA's, to check credit lines, to place travel notifications. Anything they can do to make it appear that they are the legitimate customers to increase the take they get on their "cash out" if you will."
>
> Executive, Mid-Sized Card-Issuing Financial Institution

Merchants are a ready source of new and existing payment card information and consumer PII for criminals to harvest. A data breach has a ripple effect that reaches far beyond the breached merchant. As seen in recent high-profile breaches, a breached merchant may lose business, consumer trust and stock value. Additionally, even merchants who were not breached may be targeted by fraud using stolen consumer credentials, and incur fraud losses.[7]

While payment card data remains the top breach target (41% of breach victims in the past year had a credit card number compromised, and 21% had a debit card number compromised), fraudsters also relentlessly pursue non-card accounts using credentials compromised in data breaches, or using malware and phishing attacks. Fifty-three percent of existing non-card fraud (ENCF) victims claim their demand deposit account were misused, which puts DDA and savings accounts as the top ENCF targets again in 2013. Internet accounts, including Amazon and eBay, were compromised in 12% of ENCF cases and payment account compromise, such as PayPal, grew from 6% in 2012 to 10% of ENCF victims in 2013 (See Figure 10).

Figure 10.ENCF Targets - Loan, Email, and Internet Accounts



Q9: Did the perpetrator misuse any of the following existing accounts?
Select top responses shown

October 2011 - 2013, n varies 138 to 284
Base: Existing non-card fraud victims

Merchants are aware that minimizing the misuse of consumer PII reaps rewards for merchants beyond containing fraud losses. Forty-four percent of merchants believe that lower fraud rates increase customer loyalty. Thus it is crucial not only to protect customer data once it is in the custody of the merchant, but also to be aware that data breached elsewhere is being used in a variety of ways to defraud consumers.

Spotlight: Financial institutions

General financial institution findings

Financial industry executives agree that the types of fraud they are experiencing in 2014 match those of the previous year, but the rate at which they are occurring is on the rise. The usual suspects (credit and debit) remain the dominant payment types used in fraudulent transactions, and banks have seen an uptick in card fraud in particular. As far as the channels where fraud is occurring, executives suspect that patterns may be changing, but they are unable to measure this because systems are not in place for issuers to track this type of transactional information. Executives also remain skeptical that recent and upcoming changes in regulation and the payment environment (namely, EMV) will have the predicted effects on fraud mitigation, and warn against complacency as a result.

Card fraud

Industry leaders say they haven't seen much change in the payment types used to commit fraud, mainly because there has been no reason for fraudsters to make a change. Last year (2013) saw some of the largest retailer breaches in history. The POS is the predominant point of compromise, with one executive of a large regional issuer attributing 75% of card fraud to skimming and POS malware (compared to only 15% that involved online points of compromise).

The data stolen at the POS typically do not include CVC2 data, which is necessary for making CNP transactions, and, as such, are best suited for reprinting onto counterfeit cards to use at the POS. With EMV implementation on the horizon and a short half-life for caches of compromised card numbers, FI executives assert that fraudsters are in a rush to liquidate their assets and will exhaust their current resources or the timeframe to use them before exploring new avenues .

Chargebacks and fees

Chargebacks are issuers' primary means of recuperating fraud losses for consumers. However, card networks set rules that limit FIs' incentive to issue chargebacks in some cases, and encourage merchants to dispute them. Most notably, transactions under $25 (or under $15 for Visa) are treated as signature transactions regardless of whether a signature was provided,[8] and as of a 2013 update, Visa no longer requires merchants to provide a receipt for a transaction in order to dispute a chargeback.[9]

This limits the benefit to FIs of issuing chargebacks on small transactions, since the likelihood of disputes means that issuers can expect to lose more than they gain from pursuing small amounts. At least one large regional FI has set a minimum transaction value of $25 for issuing chargebacks. An executive at a large national issuer and acquirer says that only 50% of transactions disputed are actually recovered. As the costs accrue in protracted disputes, it is often against banks' interest to vigorously pursue chargebacks.

> "Card is top of mind, that is still just from a pure volume, from a pure dollar point of view, every way you want to slice it. ACH and wire we're less worried about, though that still remains the nuclear risk, one large wire and it's a bad year, whereas credit cards it tends to be death by a thousand cuts."
>
> Executive, Mid-Sized Card-Issuing Financial Institution

Several FI executives agree that the dispute process pits issuers against merchants and networks when they should be collaborating against a common enemy. These executives believe that increasing communication over threats can build back some of the trust that has been eroded by conflicts over fraud liability.

The trouble with tracking fraud types and channels

As new fraud risks are presented by an increasing variety of payment methods and channels, FI executives lament several challenges to tracking new types of payments fraud that may even confound their existing fraud-detection mechanisms. While merchants may choose to track their transactional data by channel or not, FIs have little ability to determine which channel was used to make a fraudulent CNP purchase. Currently, there is no accepted way of encoding transaction data with a "tag" to identify the channel used, which could provide valuable information on CNP fraud channels to issuers and networks.

Furthermore, the proliferation of alternative payments linked to card and DDA accounts means issuers are losing access to some of the information that forms the basis of their fraud detection models. Many FIs use transactional data as inputs into advanced rules-based or machine-learning models which leverage consumers' spending patterns to identify suspicious activity. As more consumers load their card information to be used through alternative payments providers, banks no longer receive the same granularity of information on transactions. Where an issuer might have previously seen the product and location of the purchase, now they might only see "PayPal," or "Apple" along with the amount. This creates an imperative for communication between issuers and alternative payments providers to collaborate on fraud prevention.

EMV and Tokenization

All FI executives interviewed expressed conviction that EMV would not significantly reduce the total amount of payments fraud in the U.S. but rather would shift it to new channels. One executive at a large regional issuer noted that, while the chip aspect is truly more secure against skimming, the primary account number (PAN) can be recovered for use in fraudulent CNP transactions. An executive at another large regional issuer anticipated the greatest post-EMV data security risks in two areas: small, mom-and-pop merchants who are only beginning to come online with their data storage, and alternative payments providers.

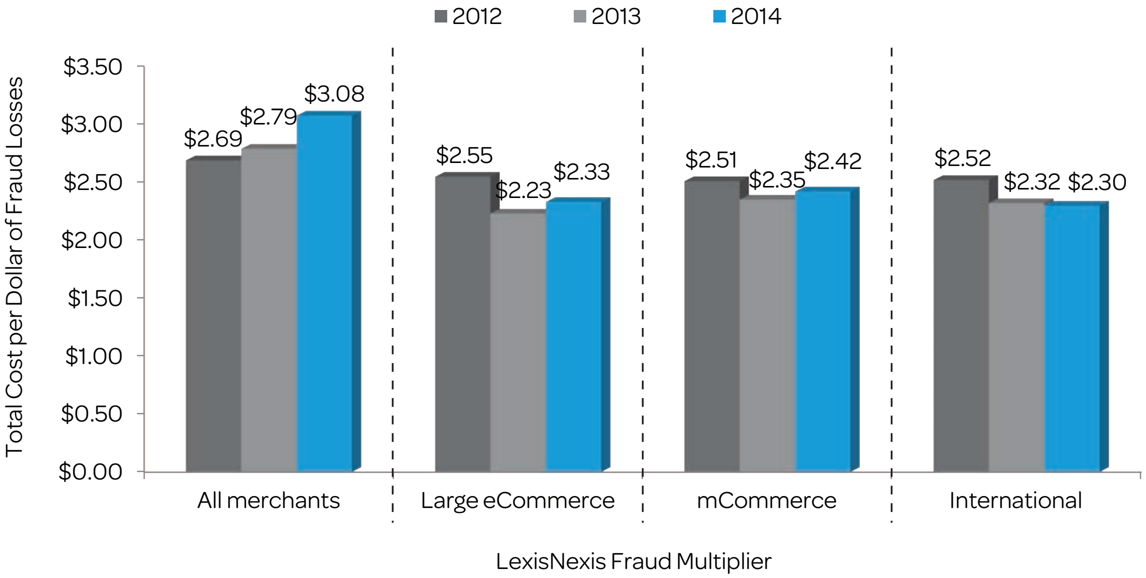
Several FI executives expected to see fraud shifting to CNP channels, and urged all merchants of all sizes to leverage tokenization to prevent criminals from using PAN data compromised in breaches. Tokenization helps to seal the holes in card security by exchanging primary account numbers with non-mathematically derived substitutes, or tokens. Executives also expected to see increases in ATO and new account fraud (NAF), which could include compromised and fraudulent online accounts with merchants.

> "I think more broadly when you start thinking about cards, our concern right now is the security of the merchants. It's obviously very easy to point at a huge one last year, but we're starting to see a lot more up in micro breaches, local mom and pops, this type of store, that type of store. We only anticipate that increasing as more of these mom and pop shops put their point of sales systems on some sort of computer."
>
> Executive, Mid-Sized Card-Issuing Financial Institution

Spotlight: Large eCommerce merchants

Large eCommerce merchants recognize that fraud is a cost of doing business; 50% of this segment believes that fraud is inevitable. After a brief respite in 2013, large eCommerce merchants are experiencing increased fraud-related costs again this year. The LexisNexis Fraud Multiplier rose from $2.23 in 2013 to $2.33 per dollar of fraud losses in the past year (See Figure 11). In addition, fraud loss as a percent of total revenue showed a dramatic increase this year to 0.85% from 0.53% in 2013, mainly attributable to friendly fraud and identity theft (See Figure 5).

Figure 11.LexisNexis® Fraud Multiplier by Merchant Segment, 2012-2014

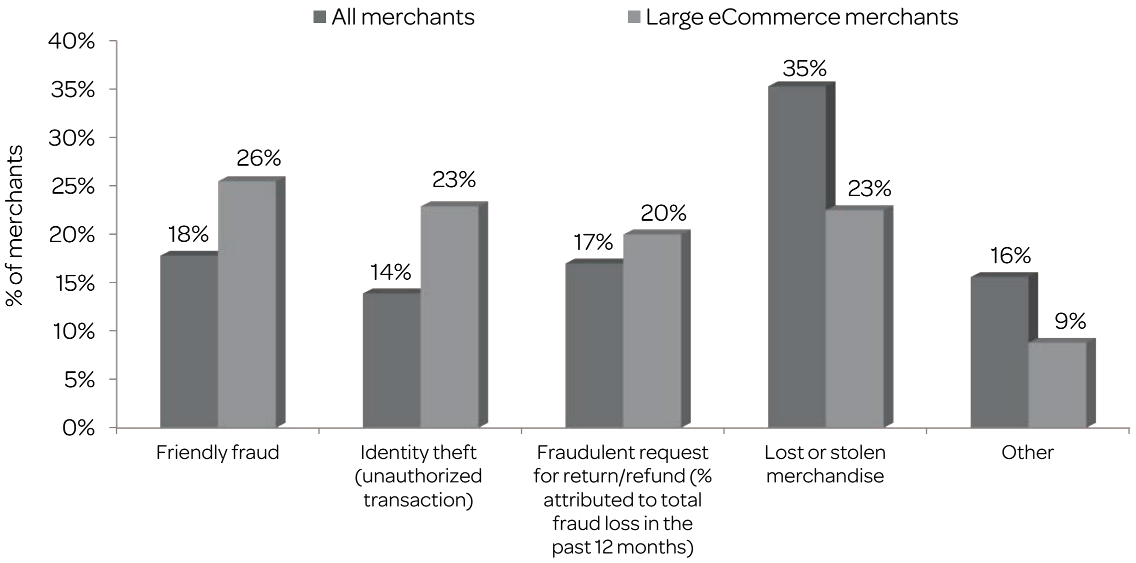


*Weighted merchant data

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.

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

Figure 12.Proportion of Fraud Attributed to Fraud Methods among All Merchants and Large eCommerce Merchants

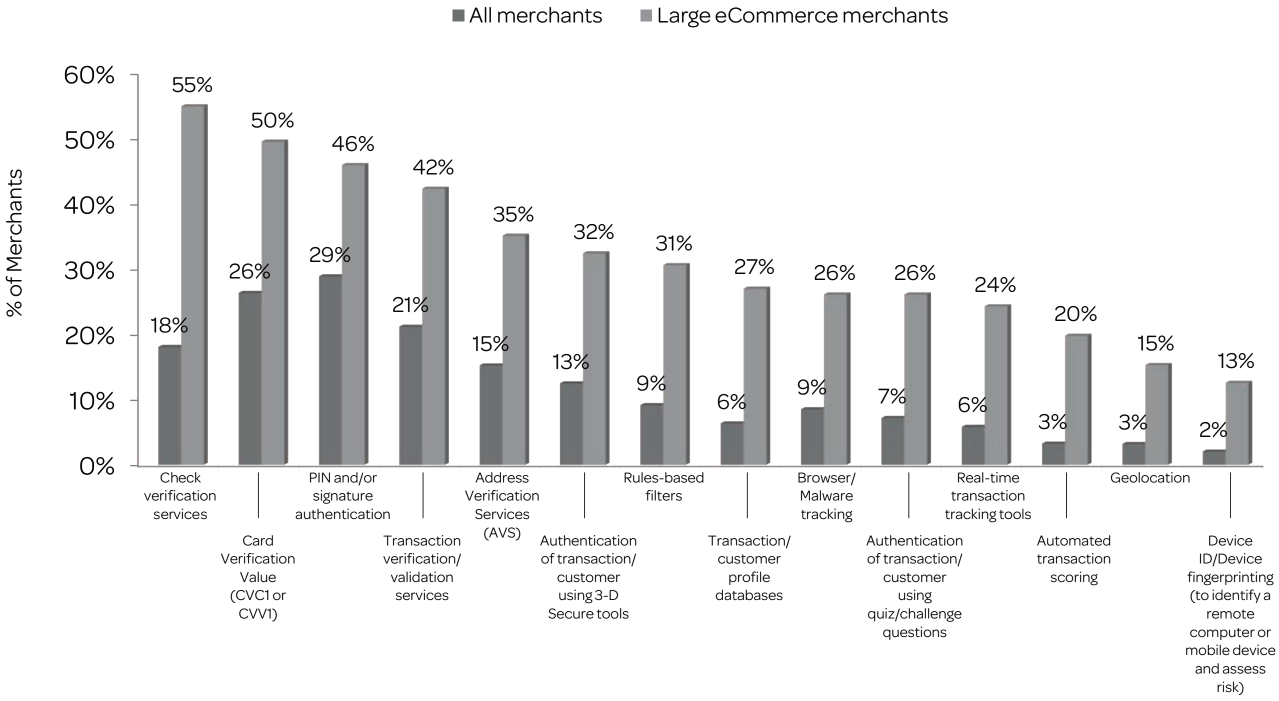


Q10. Please indicate, to the best of your knowledge, the percentage distribution of the following fraud methods below, as they are attributed to your total annual fraud loss over the past 12 months.

March 2014, n = 100, 581
Base: All merchants, large eCommerce
merchants experiencing specific fraud types

Large eCommerce merchants that do not participate in a “3-D Secure” program are liable for all risks associated with CNP transactions. These large eCommerce merchants primarily leverage CVV to prevent card fraud, but this solution is of little value when the information can be easily lost to data breaches, leaving these merchants exposed to CNP fraud risk. Back-end prevention tools such as rules-based filters and transaction-scoring tools, as well as other authentication technologies such as geolocation and device identification can be layered together to create a more secure environment for CNP transactions. Although general awareness and use of existing fraud solutions is high among large eCommerce merchants compared to all merchants, large eCommerce merchants are using fewer fraud solutions this year compared to 2013 (4 vs. 5). This is a disturbing trend considering the use of complementary solutions concurrently could provide more security. (See Figure 13).

Figure 13.Awareness of Established Fraud Solutions is High Among Large eCommerce Merchants

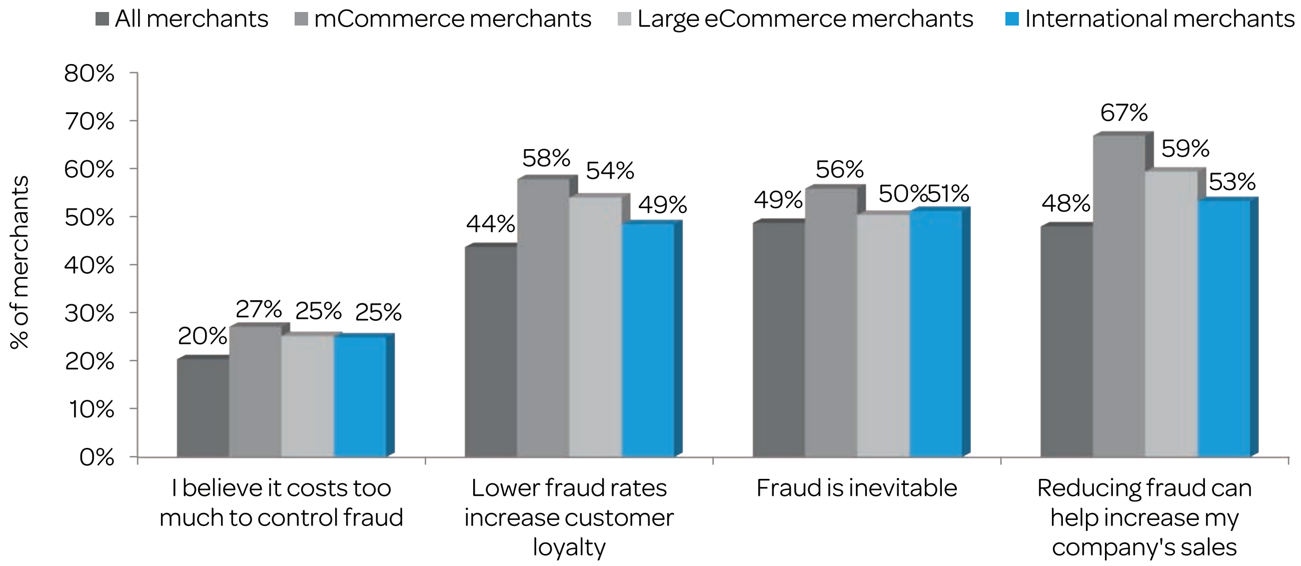


Q: Which of the following best describes your awareness and use of the fraud solutions listed below: Current users

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

In the wake of recent breaches, it is interesting to note that large eCommerce merchants seem to have mixed opinions about combating fraud. While three in five large eCommerce merchants correlate increased sales with reduced fraud, and more than half believe that lowering fraud rates increases customer loyalty (54%), one in four merchants in this segment also believe that controlling fraud costs too much. (See Figure 14).

Figure 14.Attitudes Toward Fraud by Large eCommerce Merchants, International Merchants, mCommerce Merchants and All Merchants



Q: On a scale of 1-5 please indicate the extent to which you agree or disagree with each statement listed below where 1= 'Do not agree at all' and 5= 'Agree completely'

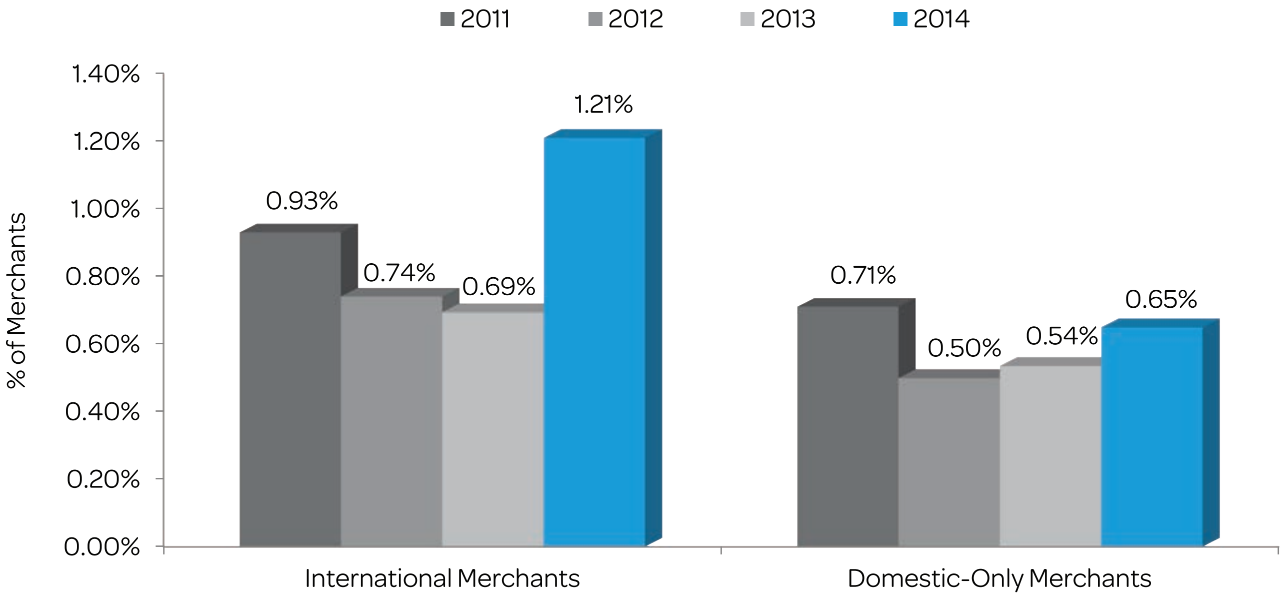
March 2014, n varies 111 - 1,141
*Base: Merchants experiencing fraud amount greater than $0 in the past year

As incidence of CNP fraud for online channel continues to rise this year (2% in 2011 vs. 2.3% in 2012 vs. 2.5% in 2013)[10], large eCommerce merchants need to up their ante in terms of combating fraud through this channel. Fraud is a moving target, and no single fraud prevention solution is 100% effective. Maintaining variability in tools, layering, and regular review and adoption of more effective fraud solutions are a must for large eCommerce merchants to maintain customer loyalty and trust.

Spotlight: International merchants

After experiencing a decline in both the percent of revenue lost to fraud and the LexisNexis Fraud Multiplier from 2012 to 2013, only the fraud multiplier has continued the trend – marginally down, by 2 cents, from $2.32 in 2013 to $2.30 in 2014 (See Figure 11). Unfortunately for international merchants, fraud loss as a percent of revenue grew significantly from 0.69% in 2013 to 1.21% in 2014 – which is nearly twice that of domestic-only merchants (0.65%) (See Figure 15).

Figure 15.Fraud Loss as a Percent of Total Revenue by International Merchants and Domestic Only Merchants, 2012-2014



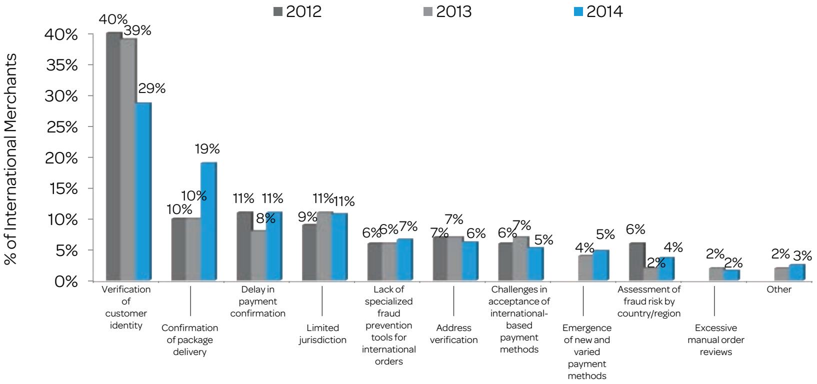
Q: What is the approximate dollar value of your company's total fraud losses over the past 12 months? Fraud losses as a percent of total annual revenue.

March 2014, n = 473, 685
*Base: Domestic-only merchants, international merchants

International merchants do believe that reducing fraud will increase sales (53%), though slightly less so than large eCommerce merchants (59%). However, given the high average number of attempted fraudulent transactions (1,288 attempted and 635 completed), it is no surprise that more than half of these merchants feel that fraud is inevitable (See Figure 14).

International merchants face a plethora of challenges compared to domestic-only merchants. One challenge consistently reported by international merchants is customer identity verification. While it has significantly dropped this year (29% of international merchants consider it to be the top challenge in preventing fraud when selling internationally, compared to 39% last year; see Figure 16), it remains among the top challenges for international merchants.

Figure 16.Key Challenges Faced by International Merchants, 2012-2014



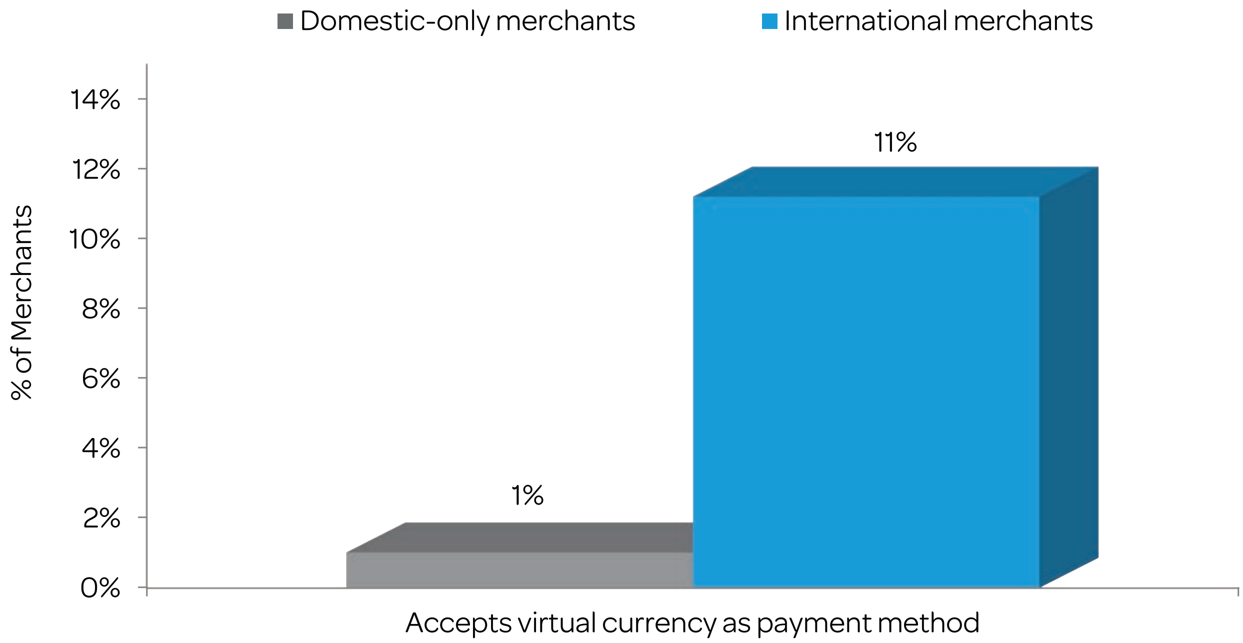
Q: Please rank the top 3 challenges related to fraud faced by your company when selling merchandise to customers outside the US. Top challenge shown.

March 2012 - 2013, n = 473, 666
*Base: International merchants

> "I find a lot of merchants that we speak with are looking more at the dollar [amount], thinking they just made a big sale and not thinking about the risk. It doesn't make sense – why is someone from the Dominican Republic calling this small merchant to make this huge order? Take additional steps to verify the transaction, use the tools that are out there to help mitigate it. But even merchants that we call to try and stop these orders continue to send them out. They are just going to get a chargeback and lose the money."
>
> Executive, Mid-Sized Card-Issuing Financial Institution

Virtual currency acceptance is growing quickly among international merchants; 11% accept this emerging payment method, compared to only 1% of domestic-only merchants (See Figure 17). This type of payment promises to play a nuanced role in fraud prevention. On the one hand, 27% of international merchants accepting virtual currency report that fraud using this payment method has increased over the past 12 months (only 12% have seen a decrease), (See Figure 18). On the other hand, fraud using certain types of virtual currency may be less damaging to merchants. As certain virtual currencies, such as Bitcoin, present a reduced incentive for merchants to verify customer identity – transactions using Bitcoin cannot be reversed, so the merchant is not liable for chargebacks in these fraud cases.

Figure 17.Proportion of Virtual Currency Payment Method Acceptance by Domestic-only and International Merchants

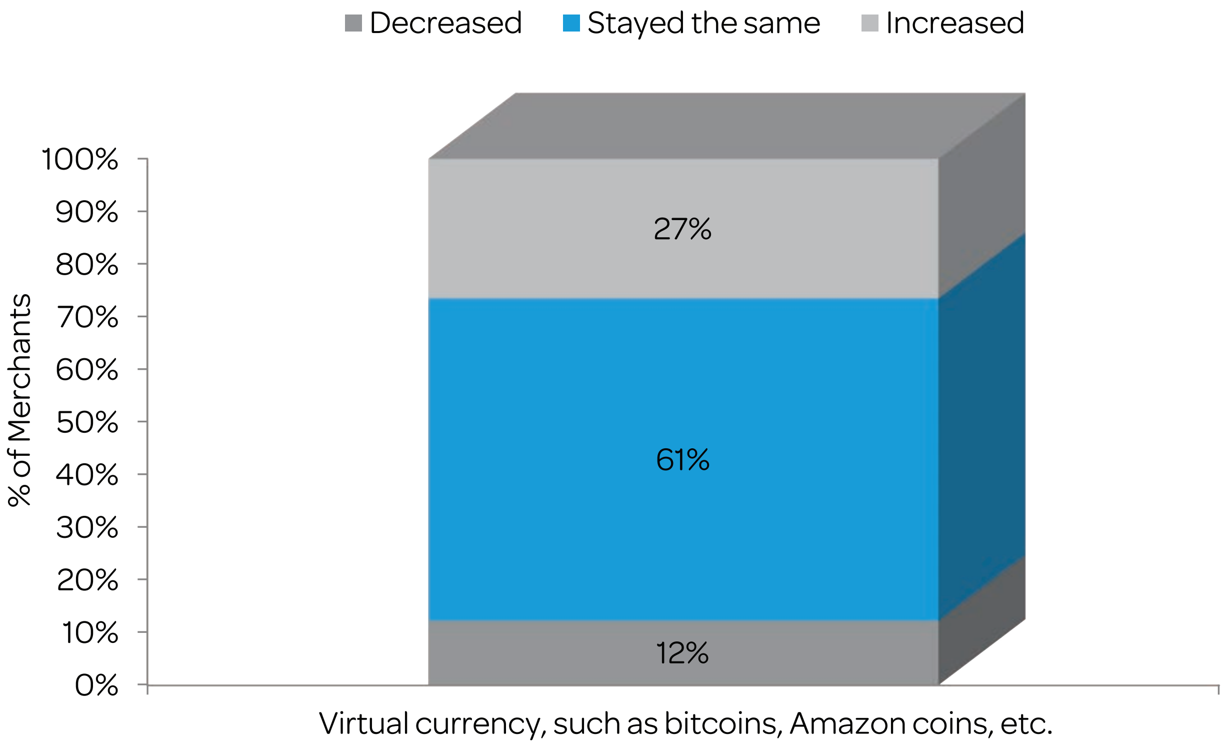


Q. Which of the following payment methods can your customers currently use? Virtual currency, such as Bitcoin, Amazon Coins, etc.

March 2014, n =437, 684
Base: International-selling merchants, domestic only merchants

A lawsuit in early 2012 by Tradehill against Dwolla with regards to chargebacks shows that trust among Bitcoin dealers and processors is low.[11] Virtual currencies are still at a rudimentary stage as a payment method and require a lot of standardization and regulations for consumers to use them as a default payment method and for merchants to accept them without any unforeseen repercussions. Among all merchants accepting virtual currencies, this payment method still constitutes an average of only 6% of the total volume of transactions. Thus it will be a long time before trends in virtual currency fraud become major drivers of overall fraud metrics.

Figure18.Fraud Level Using Virtual Currencies As A Payment Method



Q: To the best of your knowledge, over the past 12 months, has the fraudulent use of each of the following payment methods increased, decreased, or stayed the same, for your company?

March 2014, n = 49
Base: International-selling merchants supporting virtual currency payments

Methodology

In March 2014, LexisNexis® Risk Solutions retained Javelin Strategy & Research to conduct the sixth annual comprehensive research study on U.S. retail merchant fraud. LexisNexis conducted an online survey using a merchant panel comprising 1,142 risk and fraud decision-makers and influencers. The merchant panel includes representatives of all company sizes, industry segments, channels, and payment methods. The overall margin of sampling error is +/-2.90 percentage points at the 95% confidence interval; the margin of error is larger for subsets of respondents.

Executive qualitative interviews were also conducted with financial institutions to obtain their perspective on fraud losses. A total of five interviews were completed with risk and fraud executives. Identity fraud victim data from a survey of more than 5,500 U.S. adults representative of age, gender, income, and ethnicity was also utilized to ascertain the consumer cost resulting from fraudulent transactions. In 2014, 2013, 2012, 2011 and 2010, merchant data was weighted according to the U.S. Census by both employee size and industry distribution.

Industry was weighted by the following classifications: automotive, housewares, computers, hardware, restaurants, drug/health, gasoline stations, textiles, sporting goods, general merchandise stores, non-store retailers, and miscellaneous. In 2011, weights were also updated to match the most recent distributions available. The data set was weighted to match the 2007 and 2008 U.S. Economic Census to better reflect the actual distribution by industry and employee size of the U.S. retail merchant population. 2010 data was adjusted and reweighted to match the latest figures as well and allow longitudinal comparisons. Thus 2010 data is restated.

The 2013 TCOF study also introduced trending of fraud losses as a percent of annual revenue. In adherence to best practices, fraud loss values were imputed for all merchants to account for missing responses. Fraud loss percentages were then recalculated for 2010, 2011 and 2012 to yield more reliable fraud loss trends. The revised fraud loss figures cited for 2012 and 2011 may vary from figures originally cited in past years' studies.

2013 Javelin identity fraud survey

The 2014 Identity Fraud Report based on a survey conducted in October 2013 provides consumers and businesses an in-depth and comprehensive examination of identity fraud in the United States based on primary consumer data.

Survey data collection

The 2013 ID Fraud survey was conducted among 5,634 U.S. adults over age 18 on KnowledgePanel®; this sample is representative of the U.S. Census demographics distribution, recruited from the Knowledge Networks panel. Data collection began October 9th, 2013, and ended Oct. 30th, 2013. Final data was weighted by Knowledge Networks, while Javelin was responsible for data cleaning, processing and reporting. Data is weighted using 18+ U.S. Population Benchmarks on age, gender, race/ ethnicity, education, census region and metropolitan status from the most current U.S. Census demographic data

Margin of error

The ID fraud report estimates key fraud metrics for the current year using data reported by consumers experiencing identity fraud in the past 12 months. Other behaviors are reported based on data from all identity fraud victims in the survey (i.e. based on fraud victims experiencing fraud up to six years ago) as well as total respondents, where applicable. For questions answered by all 5,634 respondents, the maximum margin of sampling error is +/-1.31% at the 95% confidence level. For questions answered by all 936 identity fraud victims, the maximum margin of sampling error is +/-3.20% at the 95% confidence level.

Sources

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

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

[3] 2014 Retail Point of Sale Payment Forecast: The Mobile Payment Square-Effect And Prepaid Card Popularity Drive Cash Down by 10%, Javelin Strategy & Research, May 2014.

[4] http://datalossdb.org/statistics, accessed July 16th, 2014.

[5] 2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends, Javelin Strategy & Research, February 2014.

[6] Ibid.

[7] Ibid.

[8] https://www08.wellsfargomedia.com/downloads/pdf/biz/merchant/intelligencefall2010.pdf, accessed August 11th, 2014.

[9] https://usa.visa.com/download/merchants/chargeback-management-guidelines-for-visa-merchants.pdf, accessed August 11th, 2014.

[10] 2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends, Javelin Strategy & Research, February 2014.

[11] http://arstechnica.com/tech-policy/2012/03/lawsuit-illustrates-bitcoins-chargeback-problem/, accessed July 16th, 2014.

For more information:

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

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.

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.

LexisNexis®