Annual Report

2013 LexisNexis® True Cost of Fraud℠ Study

Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud

September 2013

LexisNexis®

Risk Solutions
Retail

Table of contents

Table of figures

Introduction

The annual LexisNexis® True Cost of Fraud℠ study establishes the actual cost of fraud as borne by U.S. merchants, along with key findings and specific guidance for the industry. Recommendations for successfully 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 costs associated with 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.
- Mobile merchants accept payments through various mobile devices.
- 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

While the rebounding economy is softening the blow of merchant fraud losses, merchants are still paying $2.79 in costs for each dollar of fraud losses they incur, up $0.10 on the dollar from 2012 (see figure 1). A spike in online fraud is responsible for these higher costs, as fraud through the online channel burdens merchants with higher fees and replacement costs than fraud through in-person or other channels. The surge in online fraud is driven by the proliferation of malware and data breaches, which facilitate the theft and misuse of consumers' payment card, merchant account, and alternative payments account information. Merchants would be wise to focus on customer identity and transaction verification, particularly for online transactions, as online fraud and identity fraud take a greater percent of fraud losses in 2013.

Large e-commerce merchants demonstrate exemplary fraud attitudes and behaviors which mitigate the effect of fraud losses on their bottom line. These merchants believe that fraud is inevitable, but understand that their prevention efforts will result in more positive customer relationships (see figure 5). They use a greater number of fraud technology solutions than all merchants (5 solutions vs. 2, on average), and lose a relatively low (and declining) percent of revenue to fraud each year (from .60% in 2012 to .53% in 2013) (see figure 3).

International merchants adhere to the same beliefs and behaviors to a lesser degree, though still more than all merchants (see figures 5 and 13). Although they lose more revenue to fraud each year, they reduced this percent even as their domestic-only counterparts saw an increase this year (see figure 17).

Mobile merchants saw an increase in fraud as a percent of revenue this year (from .64% in 2012 to .75% in 2013) (see figure 3). While displaying similar attitudes to large e-commerce merchants as to the positive effects of reducing fraud, they are most likely among all segments to view fraud mitigation costs as burdensome (see figure 4).

Key takeaways in 2013

- **Merchants are paying more per dollar of fraud in 2013 (2.69 in 2012 to 2.79 in 2013) as a result of an increased proportion of fraud through the online channel.** Online-channel frauds cost merchants $3.10 for each dollar of fraud losses, and the 36% increase in fraud through this channel among merchants accepting online payments is the main contributor to this increase.
- **Merchants are losing a lower percent of revenue to fraud this year, at 0.51%, compared to 0.54% in 2012.** Merchants report stable or decreasing volume of fraudulent transactions across most fraud types, channels, and payment methods. The growing economy is likely bolstering this trend, as rising merchant revenue may exaggerate a stable or downward trend in fraud as a percent of revenue.
- **The distribution of fraud types is shifting towards those associated with the greatest costs.** Lost and stolen merchandise declined from 45% to 36% over the past year. This type of fraud may be factored into shrink, and does not typically burden merchants with additional costs beyond replacing and redistributing merchandise. ID fraud, which can result in greater liability for merchants, rose from 12% of fraud in 2012 to 17% in 2013.
- **Data breaches represent a multifaceted threat to retailers.** Criminals are successfully targeting organizations that store or transmit consumers' personally identifying information (PII) and payment data, including retailers, with 1 in 4 data breach victims suffering identity fraud in 2012.
- **The Durbin Amendment has resulted in substantially reduced processing revenues for the financial industry.** Unexpected fraud losses now have a more devastating impact than ever on FIs. As a result, the industry faces the formidable challenge of placing greater emphasis on preventing fraud while maintaining positive customer experiences.
- **Visa's™ recent change in chargeback liability assignment has negatively impacted the success rate of some issuers.** Issuers report losing chargebacks that would have been successful prior to the recent rule change, though they are still experiencing recovery rates between 70% and 85% on card transactions.
- **EMV may prove to be a double edged sword for preventing retail fraud.** EMV protects users at the POS with highly secure "chip-and-PIN" authentication, but the physical card must be present in order for this technology to be utilized. Based on the experiences of merchants and issuers in the U.K. and Canada, POS fraud is likely to decrease while CNP fraud skyrockets after EMV is widely adopted in the U.S.
- **Large E-Commerce merchants who perceive value in fraud prevention are swayed by their return on investment.** Those who do not believe that fraud prevention is too expensive experience significantly lower fraud as a percent of revenue than those merchants that do (0.39% compared to 0.74%, respectively). Perceptions of value

"The fraudsters are getting better at knowing where the data has been compromised and staying within that particular footprint of that customer, making the detection that much more difficult... As an example, they compromise a restaurant in Houston, they stay in and around Houston to transact the fraud."

Executive, Mid-Sized Card-Issuing Financial Institution

"It cost our revenue, for one, I mean I believe we are down 53% when we looked at our 2012 revenue compared to 2011. Obviously, Durbin was last quarter 2011, and it just put that much more focus on fraud detection."

Executive, Mid-Sized Card-Issuing Financial Institution

"We'll basically lose a potential technicality chargeback that we did have and with that from our analytics that's part of $250,000 per year hit to recoveries on technicality chargebacks we previously got that we won't have now."

Executive, Mid-Sized Card-Issuing Financial Institution

are being driven by the effectiveness of the solutions these merchants deploy to prevent fraud.

- **The LexisNexis® Fraud Multiplier℠ cost shows that international merchants have seen a decline in both the multiplier costs (from 2.52 to 2.32) and the percent of revenue lost to fraud (from 0.74% to 0.69%) in 2013.** The distribution of international and domestic fraudulent transactions is stable from 2012, indicating that international merchants are having success at preventing both domestic and international fraud.
- **Identity fraud remained stable at 21% for international merchants, even as it increased from 12% to 17% for all merchants.** International merchants use a significantly higher number of fraud mitigation solutions compared to all merchants (3 vs. 2 solutions), and their investment is helping them to stave off an onslaught of identity fraud proportionate to what all merchants are seeing.
- **Mobile merchants are incurring the greatest fraud losses as a percent of revenue among all merchant segments (.75% in 2013).** This is the only segment to have not benefitted from a decrease in fraud as a percent of revenue from 2012 to 2013, yet mobile merchants are seeing an increase in revenue through this channel (from 14% in 2012 to 19% in 2013).

Recommendations

- **Focus on preventing fraud through the online channel, as liabilities for fraudulent card transactions are greater through this channel.** Charge-backs, fees and interest to financial institutions, and costs of replacing and redistributing lost and stolen merchandise may all be incurred when fraud occurs through the online channel. Additionally, the advent of EMV in years to come is predicted to push fraudsters to shift to the online channel. Thus, preventing online-channel fraud is a worthy investment.
- **Employ fraud solutions geared toward authenticating customers and transactions across all accepted sales channels and payment methods.** Adequate in-person authentication on card transactions alleviates merchants' liability in the case of fraud, and authentication is the primary means of prevention against ID fraud, which is a growing threat to merchants in 2013.
- **Upgrade data security as breaches become major sources of consumer information used to commit identity fraud.** Securing data against breaches is a worthwhile investment as it limits legal and reputational risk, along with preventing that same data from being later misused in the commission of fraud.
- **Improve consumer perceptions of e-commerce security to maintain a competitive advantage in the age of rising identity fraud.** Nearly one in three identity fraud victims choose to avoid certain merchants after victimization. As anywhere between eight and twelve million U.S.

"Watch your data. Protect your data. Protect your data. I mean that's the hardest thing for them to wrap their heads around, right? It's the what if scenario."

Executive, Large Card-Issuing Financial Institution

"There have been many times that we've contacted a card not present type merchant, because we caught it (fraud) pretty quick, and I would much rather have the merchant not process the transaction and issue me credit and have them even stake the money, then me going through the cost of the chargeback and have something go wrong... There have been times that we called merchants and they don't care."

Executive, Mid-Sized Card-Issuing Financial Institution

consumers suffer identity fraud every year, presenting an image of strong security is necessary to reassure these potential customers that their transaction is safe.

- **Plan to take advantage of EMV's effect on POS card fraud rates to strengthen CNP anti-fraud measures.** E-commerce merchants with a strong brick-and-mortar presence who plan to deploy EMV capable terminals may potentially offset the cost of upgrading their online fraud mitigation solutions by reinvesting anticipated savings from the expected EMV related reduction in POS card fraud.
- **Develop stronger working relationships with financial institutions .** Despite the potential for conflicting interests, merchants and FIs can mutually benefit from greater information sharing. Regardless of where final chargeback liability is assigned, managing the costs of chargeback operations can represent a financial pain-point for both industries. Cooperation in positively identifying potential fraud attempts before they are completed, and in prosecuting those responsible, can result in reduced fraud losses and chargeback costs for all.
- **International merchants should thoroughly investigate the fraud technology solutions they employ, as they show a tendency toward overconfidence in solutions they happen to be using.** Thirty-five percent of international merchants ranked card verification values (CVV) as the most effective solution at preventing international fraud. 3D Secure, a superior means of card payment authentication, was ranked as most effective by only 26%. This can be explained by the fact that a far greater proportion of international merchants currently use CVV, at 44%, compared to only 26% who use 3D Secure.
- **Place mobile transactions under greater scrutiny as fraudsters are attracted to the maturing channel.** Mobile transactions represented a greater proportion of revenue for mobile merchants in 2013. This same segment also experienced an increase in fraud as a percent of revenue, as compared to last year. As overall mobile volume grows, this channel will undoubtedly draw greater interest from fraudsters.

2013 fraud overview: Merchants, financial institutions and consumers

General findings for merchants

The cost of fraud is on the rise as fraud through high-cost channels increases

The LexisNexis® Fraud Multiplier℠ costs showed a moderate increase in 2013, with merchants reporting they are paying $2.79 for each dollar of fraud losses, compared to $2.69 in 2012 (see figure 1). The fraud costs beyond initial fraud losses (including charge-backs) are on the rise. Specifically, fees and interest to financial institutions have risen significantly since 2011, from 11% to 16%. The cost of replacing and redistributing lost and stolen merchandise has remained stable since 2011, comprising the largest portion of fraud costs at 48% (see appendix, figure 21).

The main driver of this increase is a spike in fraud through the online channel, the channel for which merchant liabilities are the greatest (see figure 8). Merchants paid a whopping $3.10 for each dollar of fraud losses incurred through the online channel (see appendix, figure 22).

As the ease of obtaining stolen card numbers and other credentials online—and the added benefit of anonymity—push fraudsters to commit CNP fraud through the online channel, merchants are being hit harder where damage control is most expensive. Merchants, accepting online payments attributed 42% of fraudulent transactions to the online channel this year, compared to 31% in 2012 (see figure 8). The increasing LexisNexis Fraud Multiplier cost is evidence that merchants are already feeling impact of the increasing proportion of fraudulent online payments on overall fraud costs.

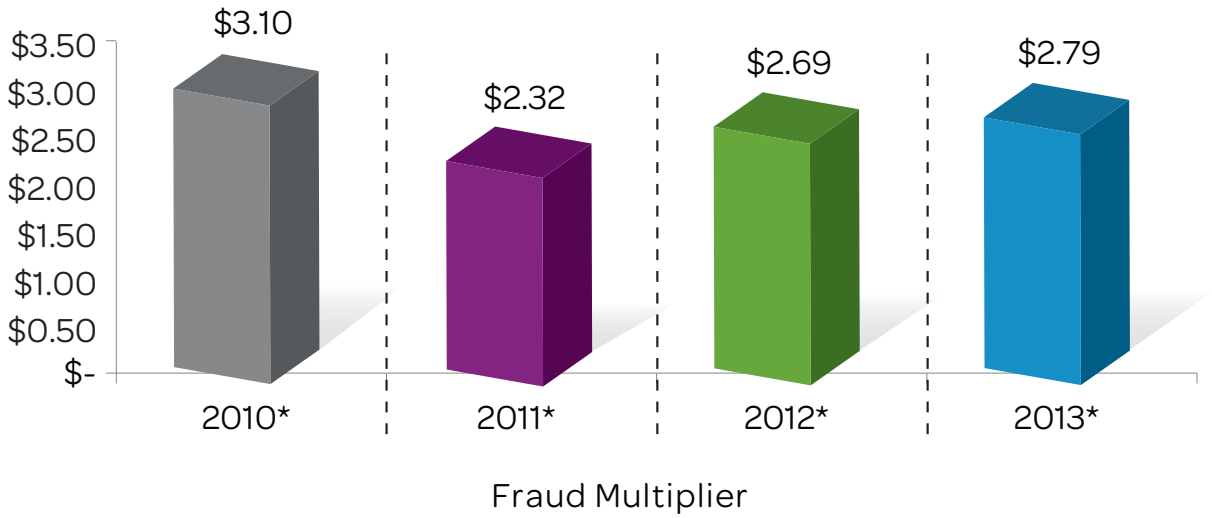
Merchants also reported an increase in the in-person fraud types which contribute to the greatest component of fraud losses. Overall in-person fraud grew as a percent of total fraud for merchants with a physical presence this year, from 58% in 2012 to 62% in 2013 (see figure 8). However, a concurrent decline in the percent of fraud attributable to lost and stolen merchandise (from 45% to 36%) (see figure 6) signifies that fraudulent transactions at the POS are driving the growth in in-person fraud. This increase is not attributable to a particular payment method, as merchants do not report an increase in fraud through any in-person payment method as a percent of all fraud (see figure 7). Thus this increase is likely split over a variety of payment methods which fraudsters are using to commit their crimes.

The costs to merchants beyond initial fraud losses may be greater for fraudulent POS purchases than for lost and stolen merchandise. In both cases, merchants will have to replace or redistribute merchandise. The cost of replacing and redistributing lost and stolen merchandise

The LexisNexis Fraud Multiplier cost calculates the total cost of fraud shouldered by merchants. Merchants not only incur as a loss the amount of chargebacks for which their company is held liable, but they also may pay fees and interest to financial institutions and pay to replace and redistribute lost or stolen merchandise. The Fraud Multiplier cost calculates the ratio of these additional fees to the amount of chargebacks and is expressed as the number of dollars spent per $1.00 of chargebacks.

consistently constitutes the greatest share of total fraud costs (see appendix figure 21). However, fees and interest to FIs constitute a growing minority of fraud costs (from 11% in 2011 to 16% of fraud costs in 2013). For credit card purchases, merchants must prove that authentication measures (such as PIN or signature collection) were executed, or else they may be liable for and fees or interest to FIs in addition to chargebacks and replacement costs. Thus, even where no additional penalties apply to merchants through FIs, fraud is never free for merchants.

Figure 1. LexisNexis Fraud Multiplier Costs, 2010 to 2013



*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 2010 – May 2013, n varies 145 to 712
*Base= Merchants experiencing fraud amount greater than $0 in the past year

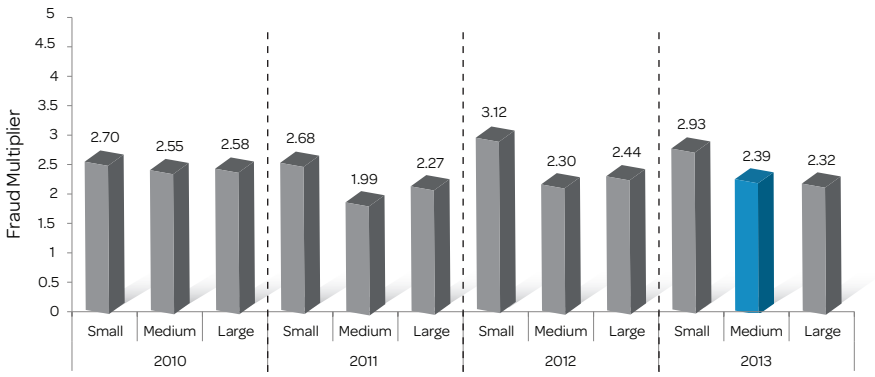
Medium-sized and large merchants are hard-hit by costly online fraud
Medium-sized merchants drove the increase in the LexisNexis Fraud Multiplier cost this year, spending $0.09 more per dollar of fraud losses compared to 2012. All merchants experienced an increase in online-channel fraud this year, but medium-sized merchants have been hit hardest, resulting in an increase in their overall LexisNexis Fraud Multiplier cost. Medium-sized merchants are not accepting payments through the online channel at a higher rate than previously, but those who do are experiencing a much greater percent of fraud through this channel (51%, vs. 30% in 2012). Large merchants, who are much more likely than other merchants to accept online payments (74%, vs. 39% of all merchants) have also seen a significant increase in the percent of fraudulent transactions through the online channel, (45%, vs. 32% in 2012). Small merchants, half of whom accept online payments , saw a smaller increase in online channel fraud (from 45% to 52%) over the past year.

The general trend of increasing online fraud may be the result of resurgent alternative payments fraud in 2013. Fraud using these payment methods fell dramatically from 27% of fraud among accepting merchants in 2011 to 9% in 2012, but has rebounded to 23% in 2013 (see Distribution of Fraud Types section, pg. 11). Online fraud also dipped (though not so dramatically) from 36% in 2011 to 31% in 2012, before spiking in 2013, signaling a connection between these trends. The fact that medium-sized merchants saw a much greater increase in the same time period may be because they are less equipped than their larger counterparts to authenticate online payments, as is indicated by significantly lower rates of use of fraud technology solutions compared to large online merchants (medium-sized merchants use 3 solutions, on average compared to large merchants who use 4).

"We have not seen a huge [upward] trend in micro merchant fraud yet, but that does keep us up at night."

Executive, Mid-Sized Card-Issuing Financial Institution

Figure 2. LexisNexis Fraud Multiplier Costs By Merchant Revenue Size, 2010 To 2013



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 2010 – May 2013, n varies 66 to 458
*Base= Merchants experiencing fraud amount greater than $0 in the past year by total annual revenue

The percent of revenue lost to fraud shrinks in 2013

Despite the rising LexisNexis Fraud Multiplier costs, fraud losses continued to decline as a percent of revenue in 2013, landing at 0.51% from a high of 0.64% of total annual revenue in 2011. It should be noted that this is not a contradiction, as the LexisNexis Fraud Multiplier cost measures the amount of additional fraud costs per dollar of fraud losses, whereas the percent of revenue lost to fraud is a relative measure of the volume of fraud losses.

It may be too optimistic to give sole credit to merchants' anti-fraud practices here without giving mention to an instrumental externality; the climbing economy may be bolstering this downward trend. The 4.7% increase in the value of the private goods-producing sector which drove GDP growth in 2012 indicates a boon to merchant revenues.[1] Higher average revenues would diminish the share of revenue lost to fraud, even if fraud amounts remain constant. However, even amid a rising economic tide which might obscure an upward trend in fraud losses, merchants indicate that absolute amount of fraud is stable or decreasing. Indeed, the majority of merchants reported no change in the incidence of major fraud types (see figure 6).

Figure 3. Fraud As A Percent Of Revenue, 2010-2013

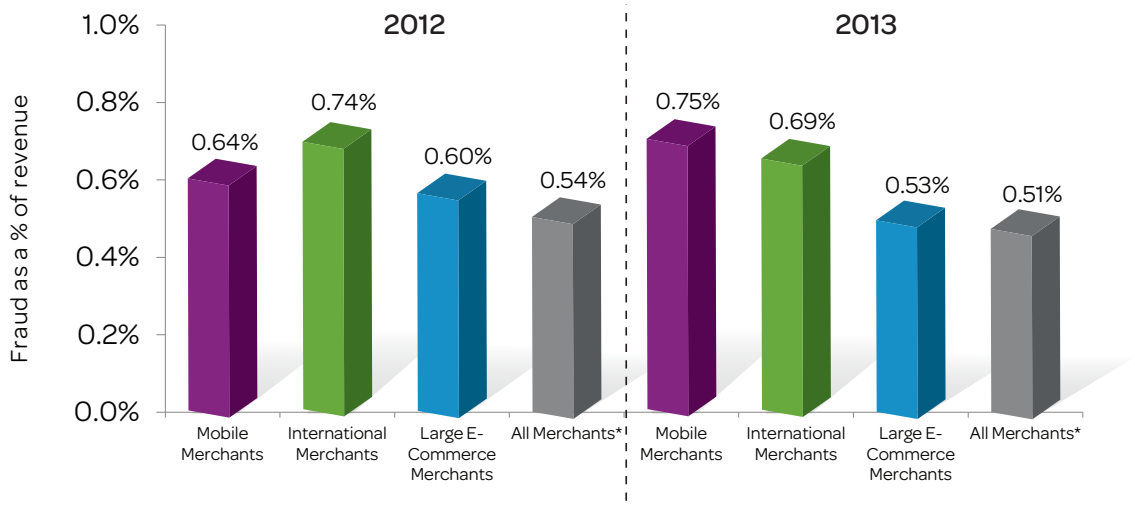
*Weighted merchant data

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 2010 – May 2013, n varies 1,005 to 1,139
*Base= All merchants

While large e-commerce merchants still lose a greater percent of revenue to fraud compared to all merchants, they have seen the most marked decrease since 2012 of any merchant type. A likely factor in their improvement is a healthy approach to fraud, supported by the attitude that successful fraud mitigation will improve sales and customer retention. Large e-commerce merchants understand that while not all fraud is preventable, wise investments in fraud mitigation can be beneficial to the bottom line.

Figure 4. Fraud As A Percent Of Revenue By Merchant Type



*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.

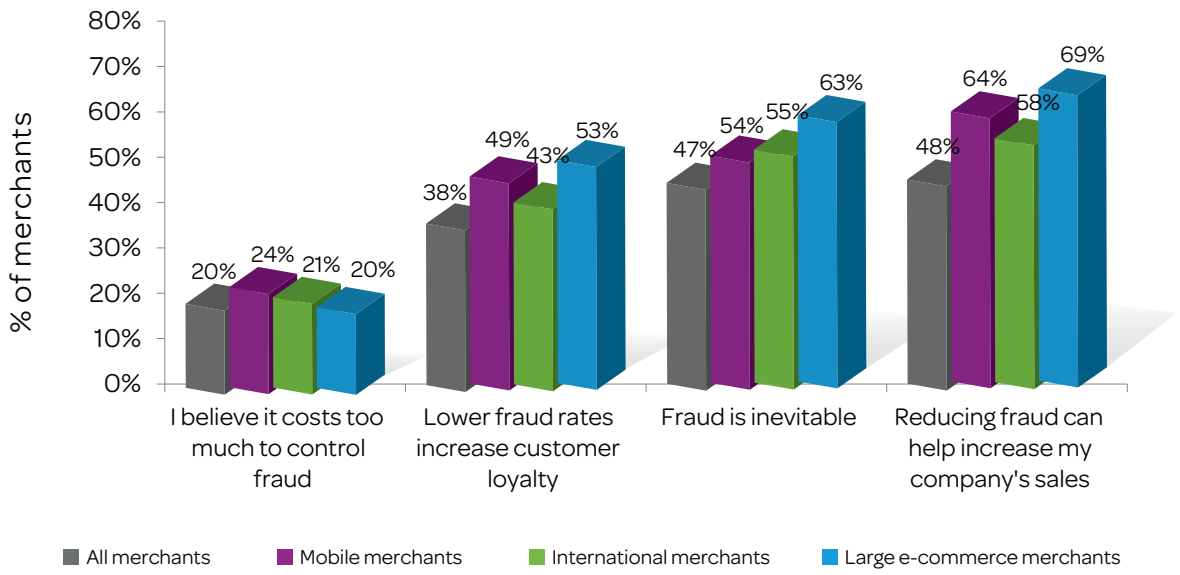
July 2012, July 2013, n = varies 118 - 1,139
Base = All merchants, Large eCommerce Merchants, International Merchants, Mobile Merchants

Large e-commerce merchants are more likely to believe that fraud is inevitable (63% vs. 47% of all merchants), but that reducing fraud can help sales (69% vs. 48%), and improve customer loyalty (53% vs. 38%) (see figure 5). In keeping with these attitudes, large e-commerce merchants also employ more fraud technology solutions than all merchants (5 vs. 2 solutions) (see figure 13), and prevent nearly ten times as many fraudulent transactions as are successfully completed in a given month (see figure 14) (see Spotlight: Large E-Commerce Merchant section).

Similar to large e-commerce merchants, International merchants also experienced a dip in fraud as a percent of revenue, though not quite as pronounced, having decreased from .74% in 2012 to .69% in 2013. International merchants are also more likely than all merchants to hold constructive attitudes toward fraud (see figure 5), and to invest in a variety of technology solutions, though not to the same extent as e-commerce merchants in either case. While international merchants employ a significantly higher number of fraud technology solutions than all merchants (3 vs. 2), they still fail to prevent 18% of attempted fraudulent transactions (see figure 15). (For more detail on international merchants please see the Spotlight: International Merchants section, page 27).

Unlike large e-commerce and international merchants, mobile merchants have experienced an increase in fraud as a percent of revenue over the previous year (from .64% in 2012 to .75% in 2013) (see figure 4). These same merchants deploy twice as many fraud mitigation solutions as all merchants (4 vs. 2, respectively) (see figure 13). Losing the greatest proportion of revenue to fraud, while investing in a relatively large number of defenses, mobile merchants believe more than any other segment that fraud costs too much to control (24%) (see figure 5).

Figure 5. Attitudes Toward Fraud By Large E-Commerce, International Merchants And All Merchants



cq35: 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'

July 2013, n = 1,030, 1,139
*Base= Merchants experiencing fraud amount greater than $0 in the past year

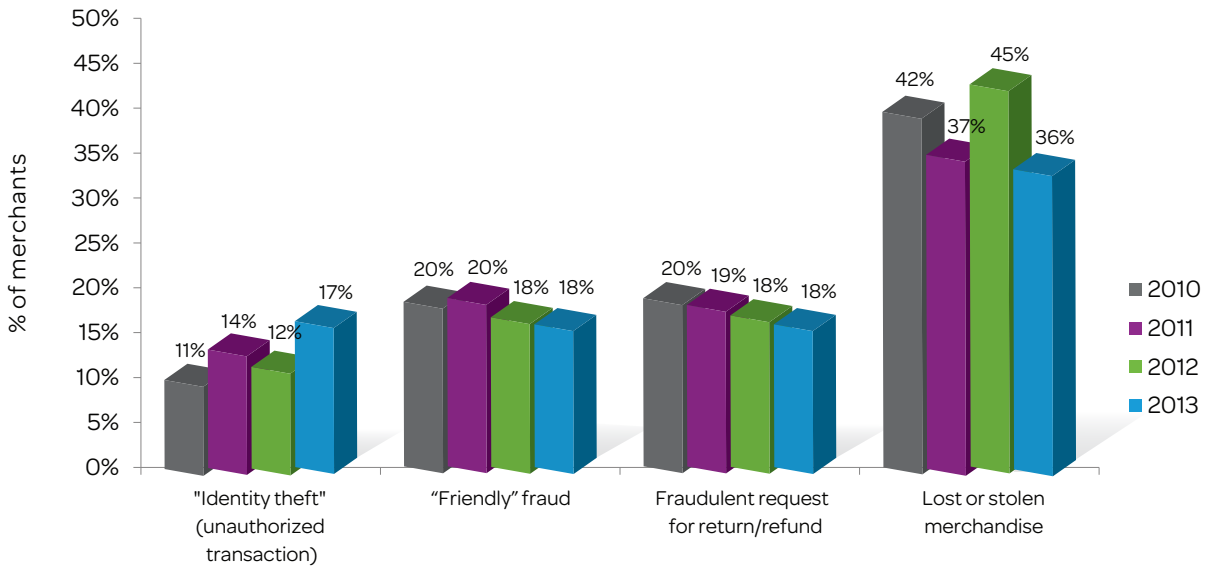
Distribution of fraud types

Merchants report less lost and stolen merchandise, but ID fraud takes a greater share of fraud losses

Lost and stolen merchandise has declined as a percent of fraud losses since 2012, but remains the largest constituent. Fraudulent requests for return and refund and friendly fraud have remained relatively stable since 2010, but still compose a considerable minority of fraud losses. When merchandise is lost or stolen, merchants face replacement and redistribution costs, and these costs constitute the largest share of fraud costs (see appendix, figure 21). However, friendly fraud results in both replacement costs and charge-backs (and in some cases fees and interest to FIs).

Merchants report in 2013 that identity theft is on the rise, accounting for 17% of fraud this year, compared to 12% in 2012. This finding is supported by Javelin consumer data, which shows that over 1 million more U.S. consumers were victims of identity fraud last year than the year before, and merchants are feeling the impact (see figure 9). Fraud via identity theft often results in a lengthy resolution process which may involve charge-backs to the merchant. Smaller online merchants are particularly hard-hit by this fraud type—even when they were not responsible for the compromise of consumer data. 15% of fraud victims, regardless of where their information was stolen, report avoiding smaller online merchants as a result of fraud (see figure 10 in the present state of identity fraud section).

Figure 6. Percent Of Fraudulent Transactions Attributable To Fraud Types



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: Mean.

July 2010 – May 2013, n varies 442 to 712
Base = Merchants experiencing fraud amount greater than $0 in the past year

Card fraud declines in 2013, but alternative payment fraud resurges from a dip in 2012

Card fraud (both credit and debit) declined in their proportion of fraudulent transactions among merchants accepting these payments methods. Indeed, Javelin finds that card fraud is declining in absolute terms as well, as 11% fewer consumers were defrauded via existing card accounts in 2012 compared to 2011. Fraudsters are opting instead to open new fraudulent accounts, or to take over users' accounts in order to make fraudulent purchases.

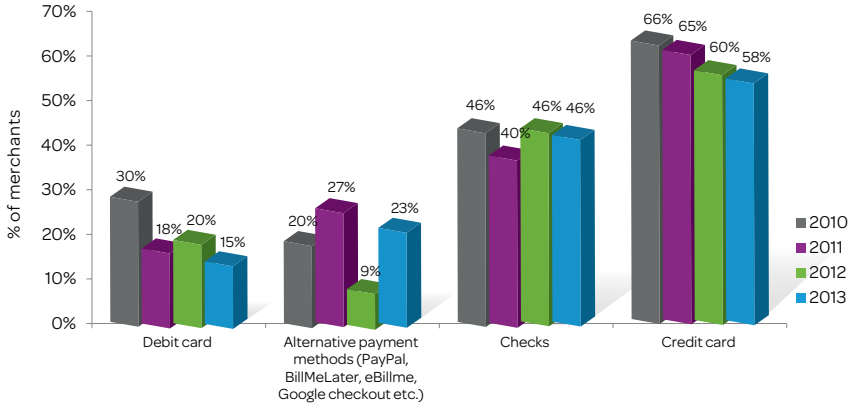
Malware designed to glean login credentials or launch Man-in-the-Browser (MitB) attacks is on the rise, and allows fraudsters to access and transact through merchant accounts where any type of payment data is saved. Usernames and passwords to merchant accounts and alternative payment accounts may also be gleaned through data breach. Even if the database compromised does not belong to the merchant, consumers' frequent re-use of login credentials across accounts leave merchant accounts vulnerable when data breaches occur elsewhere.

Companies accepting alternative payment methods reported that the share of fraudulent transactions involving this payment method rebounded to nearly their 2010 levels (see figure 7). The dramatic drop in 2012 is anomalous, however a major contributor may have been heightened vigilance on the part of PayPal™ and its users as appropriate steps were taken to prevent fraud in the wake of a data breach in 2011.[2] Since PayPal™ is the most prevalent alternative payment method (accepted by 60% of merchants, compared to only 8% for Google™ Checkout, and 9% for all other alternative payments methods), it is not implausible that security precautions taken by the company and its users would affect trends in the entire alternative payments market. While

"I think, you know, we haven't really seen any large consolidated schemes, like this is the best way to say. We have our PayPal™ fraud here and there, but nothing that I will consider a coordinated scheme to exploit a weakness in the PayPal™ ecosystem if you will."

Executive, Mid-Sized Card-Issuing Financial Institution

Figure 7. 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.

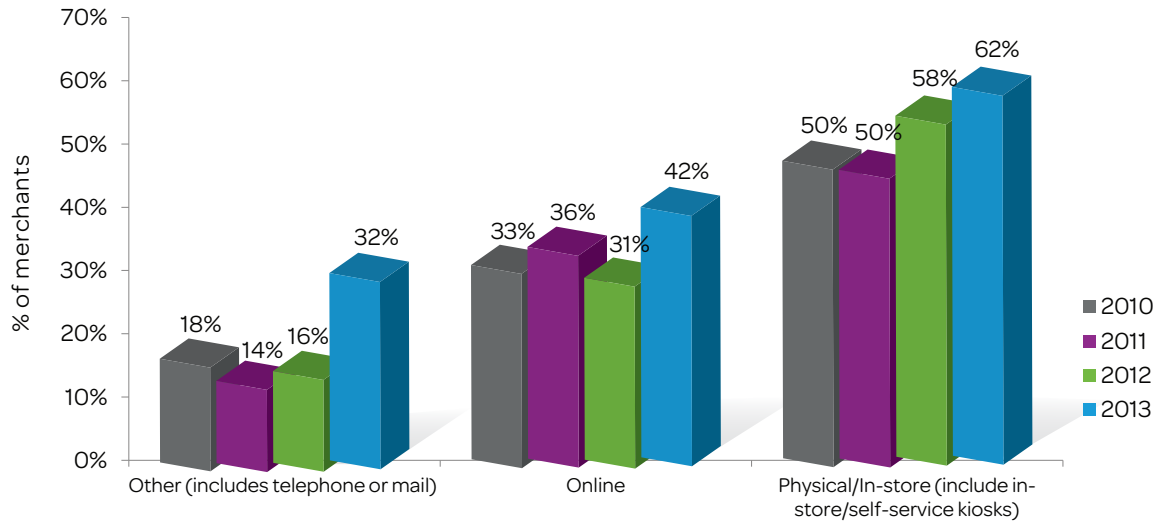
July 2010 – May 2013, n varies 58 to 246
Base= Merchants experiencing fraud amount greater than $0 in the past year and accept particular payments methods

friendly fraud may also involve purchases made using alternative methods, it is possible that the large-scale changing of usernames and passwords, and the employment of secondary authentication by temporarily-more-cautious PayPal™ users helped to reduce identity fraud during this period.

CNP and other remote payment fraud is on the rise in 2013, with the proportion of fraudulent transactions initiated online increasing by 36%, and those initiated by mail or telephone doubling in the same time period. As discussed above (see general findings section), opportunity and anonymity make CNP and other types of remote payment fraud appealing to fraudsters. Varied means exist to glean and misuse user payment information and account credentials. However, the fact that fraudsters are exploiting the online channel does not mean that they are abandoning the physical channel just yet. Merchants with a physical presence saw an increase in the proportion of fraud through the physical channel as well.

Lost and stolen merchandise is declining as a percent of fraud losses (see figure 5). Therefore, identity theft (involving fraudulent card, check, or mobile payments), and, to a lesser extent, fraudulent requests for return and refund, are likely driving the increase in the proportion of physical channel fraudulent transactions in all fraud. Proper authentication at the POS will help merchants avoid the charge-backs and fees to financial institutions which may result from identity fraud. Improving company policies designed to limit fraudulent returns and refunds may be a difficult balancing act for customer-service focused merchants, but may help to curtail the not-inconsequential 18% of fraud losses resulting from this fraud type.

Figure 8. 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 2010 – May 2013, n varies 58 to 176
*Base= Merchants experiencing fraud amount greater than $0 in the past year and accept payments through particular channels.

The present state of identity fraud

Spotlight: Consumers

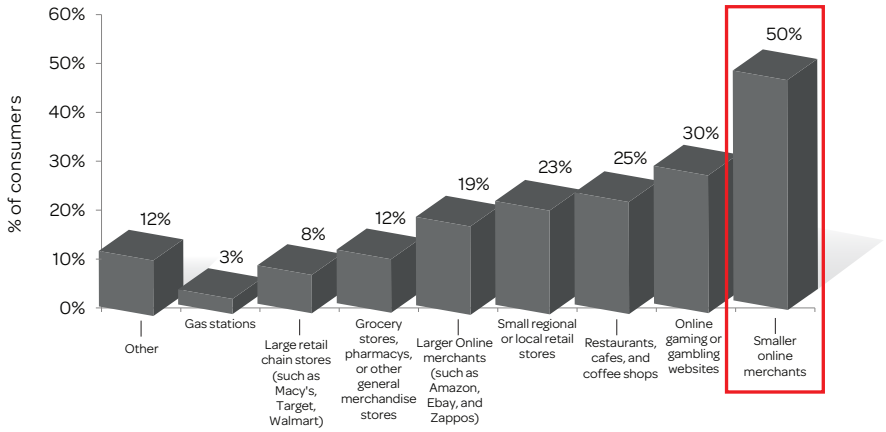
After witnessing a significant decline in both incidence rate and total fraud amount between 2009 and 2010, identity fraud has been trending upward with 12.6 million victims, and $21 billion in total fraud having occurred, in 2012.[3] Merchants were undoubtedly affected by the increase in consumer identity fraud as they are prime targets for criminals looking to monetize stolen payment data or accounts fraudulently opened with compromised PII. A byproduct of identity fraud, victim perceptions of merchants also suffer, resulting in reduced future business with potential customers.

Figure 9. Overall Measures of the Impact of Identity Fraud, 2005-2012

Survey Report									
	Trend	2012	2011	2010	2009	2008	2007	2006	2005
U.S. adult victims of identity fraud (in millions)	↑	12.6	11.6	10.2	13.9	12.5	10.2	10.6	11.2
Fraud victims as % of U.S. population	↑	5.26%	4.90%	4.35%	6.00%	5.44%	4.51%	4.71%	5.04%
Total one-year fraud amount (in billions)	↑	$21	$18	$20	$31	$29	$25	$29	$32
Mean fraud amount per fraud victim	↑	$1,653	$1,543	$1,948	$2,262	$2,313	$2,415	$2,713	$2,861
Median fraud amount per fraud victim	↓	$350	$472	$637	$727	$711	$801	$846	$908
Mean consumer cost	=	$365	$354	$352	$384	$437	$524	$539	$614
Median consumer cost	=	$0	$0	$0	$0	$0	$0	$0	$0
Mean resolution time (hours)	=	12	12	13	14	15	16	17	17
Median resolution time (hours)	=	3	2	3	4	4	4	4	5

Among fraud victims, 29% avoid certain merchants as a result of their victimization. Reinforcing the perception of a secure transacting environment is critical to maintaining the patronage of these consumers. This is especially true for smaller online merchants, as 50% of fraud victims that avoid certain merchants as a result of being defrauded will specifically avoid patronizing these businesses in the future (see figure 10).[4]

Figure 10. Merchant Types Avoided Among Fraud Victims That Avoid Certain Merchants Post-Fraud



Q: Which of the following merchant types do you avoid?

October 2012, n=244
Base: Consumers who avoid certain merchants

Minimizing the misuse of consumer identity and payment information to commit fraud protects retailer profits in two ways. Criminals rely on consumer data to defraud merchants, while victimized consumers subsequently change their shopping behavior to the detriment of merchants. Deploying effective transaction security is necessary to not just prevent malicious activity, but to also preserve legitimate volume.

"I think that the merchants should really invest in their security infrastructure and then the training of their employees in order to have a culture of fighting fraud. That would be a great thing."

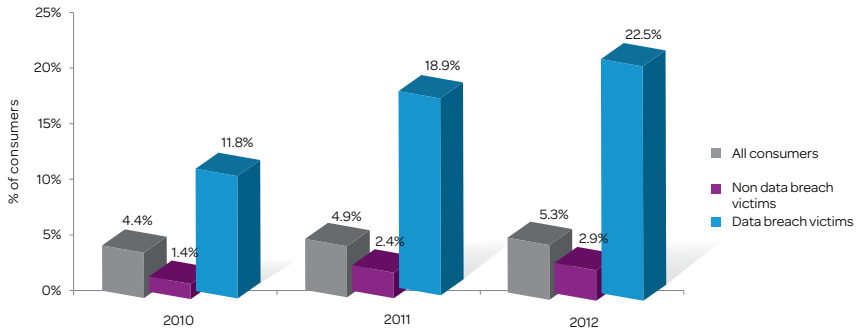
Executive, Mid-Sized Card-Issuing Financial Institution

Data breaches beget identity fraud

In order to successfully defraud merchants, criminals need a ready source of sensitive consumer PII or payment data. New identity theft methods can now facilitate both anonymity and the ability to obtain PII and payment data en masse. In 2012, a record number of data breaches were reported with 75% having been motivated by financial gain.[5,6] Data breaches have come to replace mail theft and dumpster diving as the methods of choice for criminals seeking fuel for their fraud schemes. Worse yet, merchants themselves are high-profile breach targets as they are known to transmit the very data that is of interest to criminals.[7]

The incidence of fraud victimization among data breach notification recipients has been outpacing that of all consumers since 2010 (see figure 10). This trend indicates that criminals are increasingly relying on information compromised during data breaches to facilitate fraud. Compromised payment card data is especially dangerous for online merchants, as criminals can use this information to commit fraud almost immediately after the breach has occurred. Depending on the number of compromised cards, millions of dollars in fraud can be committed with the information from a single breach.[8]

Figure 11. Fraud Incidence Rate Among All Consumers, Data Breach Victims, And Non Data Breach Victims (2010 -2012)



Q: 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 - 2012, n = varies 337 - 5,249
Base: All consumers, data breach victims, non data breach victims.

Effective transaction security is only part of the puzzle for merchants seeking to reduce their exposure to the risks posed by data breaches. Improving data security is an important second step, as merchants that suffer data breaches may face civil lawsuits, while also placing other retailers at risk of being defrauded by criminals using the very data exfiltrated from their systems.[9]

"[Merchants] need to look at their point of sale environments and treat it like an ATM environment. It needs to be on a segregate network, it can't be a multipurpose Wintel machine ... they need to treat it as a hardened environment because it is truly where all of the exploits that have been going on."

Executive, Large Card-Issuing Financial Institution

Spotlight: Financial institutions

Executives express concern about a variety of fraud mitigation challenges, ranging from newly emerging threats to those just over the horizon. A major concern: card fraud represents a substantial portion of many FIs' total fraud losses, with executives acutely aware of the impact of malicious Point-of-sale (POS) and Card-Not-Present (CNP) activity, along with the disruptive potential of EMV. Continually changing regulation presents a formidable challenge for institutions still reeling from the Durbin Amendment of the Dodd-Frank Act in 2011, as a 2013 industry change in how chargeback liability is assigned is squeezing already razor-thin profit margins.

Nearly all of the FI executives interviewed report that credit and debit cards continue to represent both the highest volume of fraud among their product lines and their greatest area of exposure. Some attributed 30%-40% of their overall fraud losses to fraud associated with their credit card and debit card products. Among the types of issues that they are experiencing at the POS, skimming and counterfeit cards continue to be a major problem. Card-Not-Present fraud is on the rise, and as consumers continue to use online and mobile retail channels, issuers are faced with potential for growing fraud exposure.

Issuers and merchant acquirers suggest that the deployment of EMV is a way to mitigate card fraud at the POS. However, many of them are quick to point out that EMV will not stem the rising tide of CNP fraud based on past experience, but will rather motivate it further upward. EMV integration in the United Kingdom and Canada introduced upticks in CNP fraud ; as POS fraud became more difficult for fraudsters, they migrated online.

The Durbin Amendment continues to inform issuers' risk threshold as large fraud losses can dramatically impact an institution's bottom line. Issuers report that the amendment continues to affect an overall decrease in operating revenue. Since the amendment was enacted, many have been forced to focus more attention on fraud prevention and detection. As for acquirers, they now place a greater emphasis on supporting and enabling merchant's preferred method of payment whenever possible.

Visa's™ April 19th, 2013 chargeback rule change is negatively impacting the success rates of charges backs among some issuers. By only requiring that merchants provide evidence that the card in question was presented to the cashier, issuers are losing what may have previously been successful chargebacks. They are experiencing a rise in debit card charge backs, particularly through online channels, with charge back recovery rates of about 70% to 85% for most card products. However, many issuers reported lower success rates with debit cards compared to that of credit cards. Enhancements to chargeback management platforms are

"I am sure everybody is pointing to card not present in Europe as a lesson learned for EMV in the US but that really hasn't impacted us, yet."

Executive, Mid-Sized Card-Issuing Financial Institution

"Our particular bank will be underwater for at least three months based on the Bashas' breach. It's much easier to lose money or it's quicker to get underwater based on fraud with the limited revenue that we now have with Durbin."

Executive, Mid-Sized Card-Issuing Financial Institution

being made by some issuing institutions, as they attempt to improve their recovery rate in spite of the recent rule change.

Issuers and acquirers are managing legacy threats while preparing for those yet to be fully realized, while regulatory changes continue to negatively affect FIs' fraud losses. Improved fraud mitigation hinges in part on pending technological advancements that may offer some relief, but the greatest opportunity may lie with improved cooperation between acquirers, issuers, and merchants. Executives expressed a desire for greater information sharing, with the hope that all stakeholders can benefit from reduced fraud and overall lower costs.

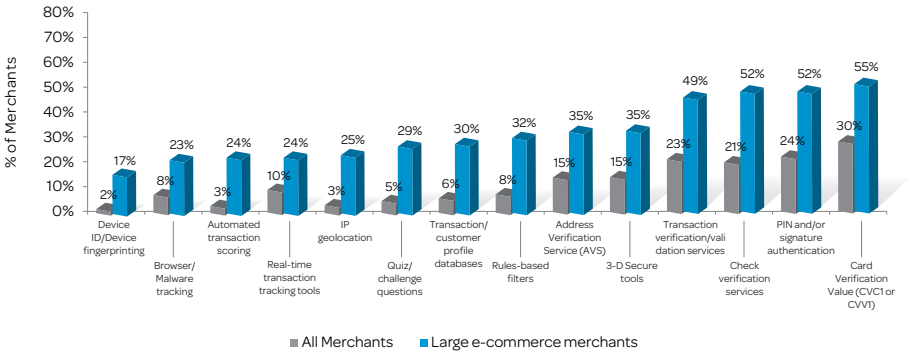
Spotlight: Large e-commerce merchants

Large e-commerce merchants have a strong vested interest in deploying e-commerce fraud mitigation tools, but their use is not uniform. As a whole, this segment has benefitted from the deployment of these solutions, along with a strengthening U.S. economy. But it is the attitudes displayed by merchants in this segment which directly affect which solutions are used, and in turn fraud's impact on their profitability.

"Everybody needs to come to the table and understand that, as businesses, we should work jointly at combating fraud, and that's how we should treat it as an industry... I think fraudsters count on the division."

Executive, Mid-Sized Card-Issuing Financial Institution

Figure 12. Use of Fraud Solutions Among All Merchants and Large E-Commerce Merchants

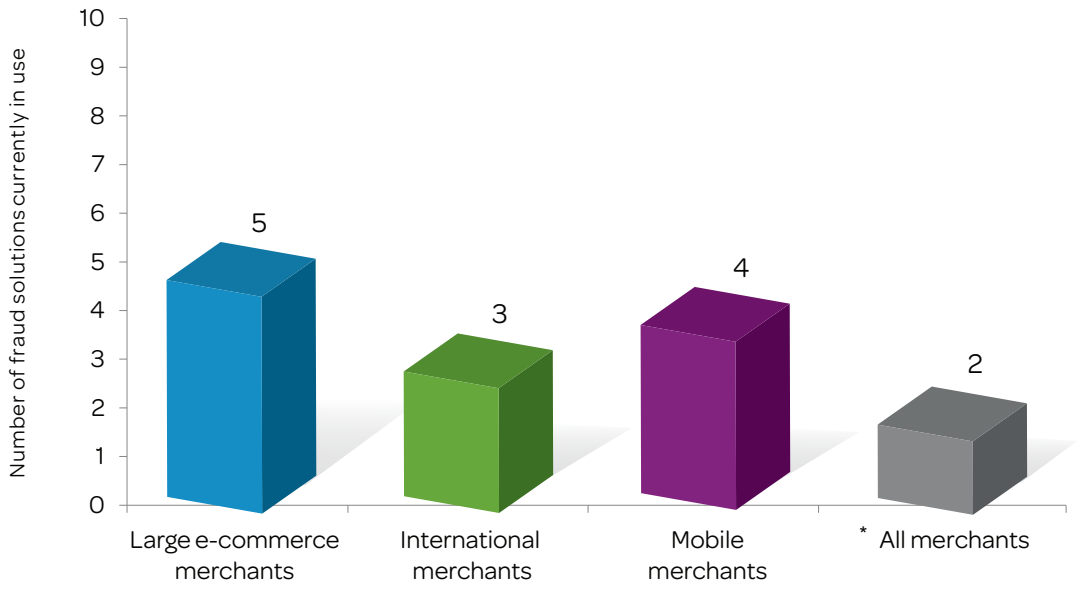


C: Which of the following best describes your awareness and use of the fraud solutions listed below: Current Users

May 2013, n = 196, 1,139
*Base= All merchants, large e-commerce merchants

The validity of a transaction must often be determined by large e-commerce merchants without the physical presence of the consumer or the form of payment. As a result, large e-commerce merchants are significantly more likely to deploy every fraud mitigation solution than merchants as a whole. From commonly deployed solutions such as CVV and PIN/signature authentication, to backend solutions with much lower penetration among all merchants, large e-commerce merchants are roughly 2 to 8 times as likely to employ the solution. Further still, they rely on a greater number of solutions than all merchants or international merchants (5 compared to 2 and 3, respectively).

Figure 13. Number of Fraud Mitigation Solutions Used by All Merchants, International Merchants, and Large E-Commerce Merchants



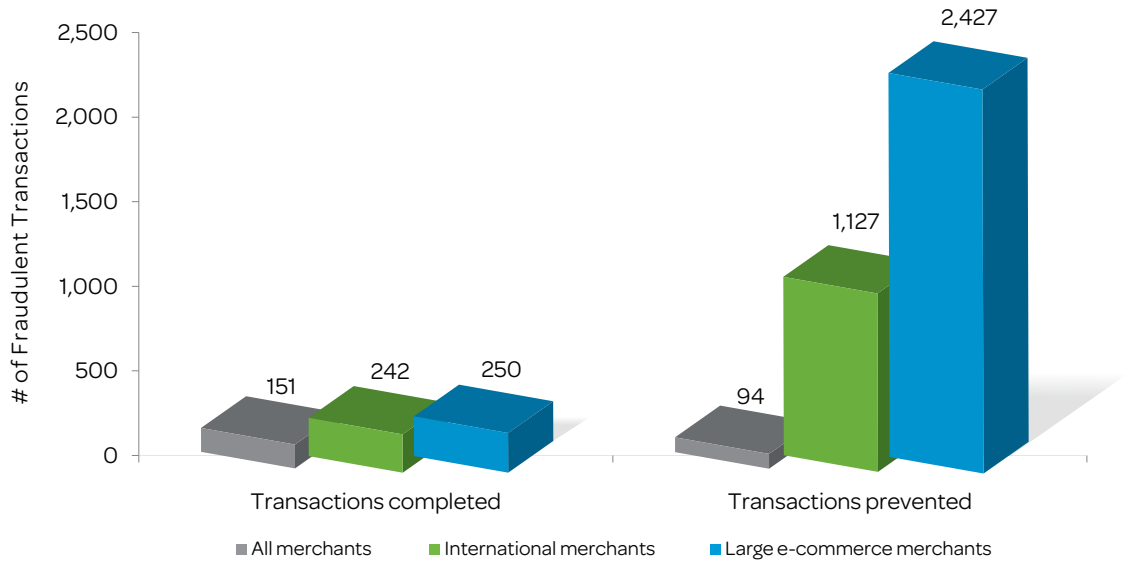
*Weighted merchant data

Q: Which of the following best describes your awareness and use of the fraud solutions listed below? My company currently uses the solution.

May 2013, n varies 196 to 1,139
*Base= All merchants, large e-commerce merchants, international merchants

It is the regular use of these tools which enable large e-commerce merchants to parse substantial transaction volume in their search for fraudulent activity. These merchants prevent nearly ten times as many fraudulent transactions than those which are completed. Maintaining these ratios is a necessity in the fight against relentless fraudsters who attempt copious online transactions with less conspicuity than those would do so at the POS.

Figure 14. Number of Fraudulent Transactions Prevented and Completed for All Merchants, International Merchants, and Large E-Commerce Merchants

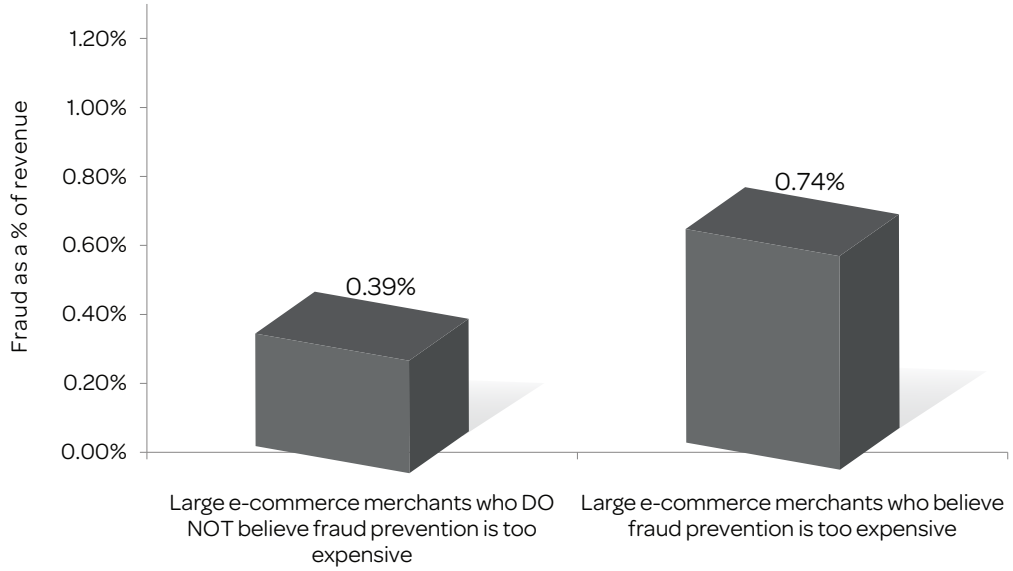


Q: In a typical month, approximately how many fraudulent transactions aresuccessfully completed at your company?

May 2013, n varies 281 to 1,139
Base: All merchants, international merchants, large e-commerce merchants

Fraud among large e-commerce merchants as a percent of revenue declined from .60% in 2012 to .53% in 2013 (see figure 4). This can be attributed to the improving U.S. economy which is resulting in an increase in overall sales (see Fraud Overview section, pg. 12), while the proportion of sales through the online channel remained relatively flat from last year (see Appendix, Figure 26).

Figure 15. Fraud as a Percent of Revenue Among Large E-Commerce Merchants Who Believe/Do Not Believe That Fraud Prevention is Too Expensive

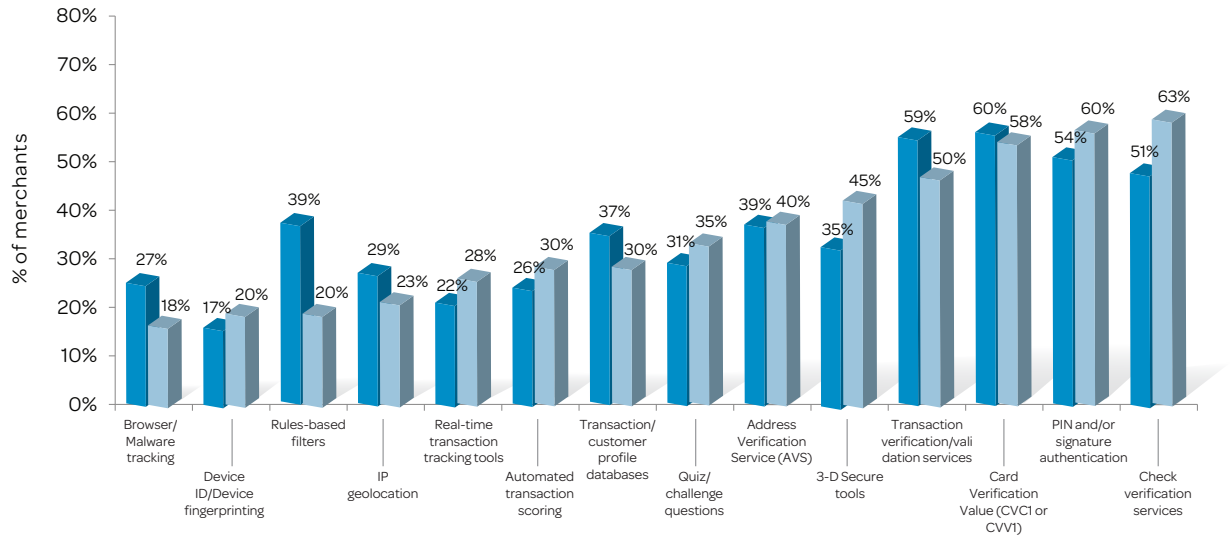


Q: What is the approximate dollar value of your company's total fraud losses over the past 12 months? Fraud losses as a percent of total annual revenue.

May 2013, n = 196, 1,139
*Base= Large e-commerce merchants by beliefs about fraud prevention

Perceptions as to the cost of fraud prevention are directly related to the effect of fraud on a merchant's bottom line. Large e-commerce merchants depend on a variety of solutions to mitigate fraud, expenses which are not typically incurred by merchants in other segments. Regardless, the positive perception of the value of these solutions correlates with experiencing less fraud as a percent of revenue (0.39%, compared to 0.74%). Merchants who do not perceive value in the use of fraud prevention tools are significantly more likely to rely on check verification services (63% compared to 51%) and 3-D Secure (45% compared to 35%) (see figure 15). Conversely, merchants who believe that fraud mitigation solutions are cost-effective are significantly more likely to use transaction verification/validation tools (59% compared to 50%) and rules based filters (39% compared to 20%) (see figure 16).

Figure 16. Use of Fraud Mitigation Solutions Among Large E-Commerce Merchant Who Believe/Do Not Believe That Fraud Prevention is Too Expensive



*Caution: low base
Q30: Which of the following best describes your awareness and use of the fraud solutions listed below?
My company currently uses this technology

July 2013, n = 40, 94
Base= Large e-commerce merchants who believe that fraud is too expensive, large e-commerce merchants who do not believe that fraud is too expensive.

Preventing fraud for large e-commerce merchants necessitates the use of a variety of solutions, but not all provide the same degree of perceived value. Merchants will benefit as long as consumer spending maintains an upward trajectory, but the advent of EMV may have a disproportionate effect on large e-commerce merchants as fraud shifts from the POS to online (see Spotlight: Financial Institutions section, pg. 21). Selecting cost-effective tools must be made with an eye to the future, as fraud is always a moving target.

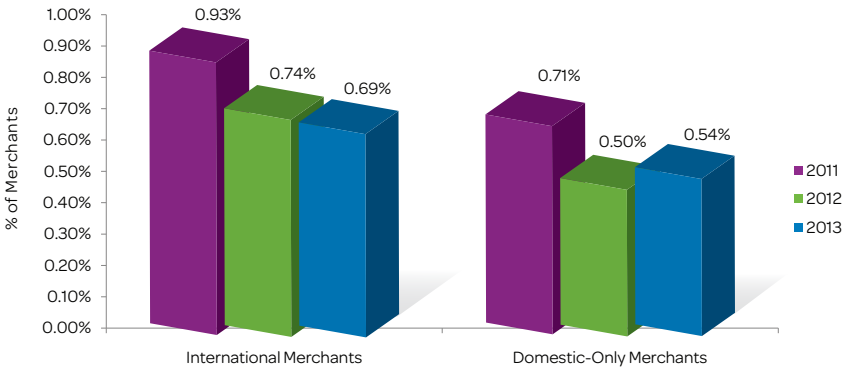
Spotlight: International merchants

International merchants saw a decline in two key fraud metrics this year, the LexisNexis Fraud Multiplier cost, and fraud as a percent of revenue. The LexisNexis Fraud Multiplier cost for international merchants dropped by twenty cents on the dollar this year from $2.52 per dollar of fraud losses in 2012 to $2.32 in 2013 (see appendix, figure 25). International merchants have lost more revenue to fraud than their domestic-only counterparts for each of the past three years. However, both international and domestic-only merchants saw a steep decline in the percent of revenue lost to fraud when compared to 2011, and international merchants continued this trend even as domestic-only merchants saw an uptick in 2013. The fraud losses international merchants incur through domestic and international orders is approximately proportionate to the revenue generated through each type of order (see appendix, figure 23). The distribution of both fraud and revenue between domestic and international orders remains stable from 2012.

"Card not present merchants need to step up... as we move down this path towards EMV and card not present merchants become the path of least resistance, we're going to see a heck of a lot of more fraud than they do now and they need to prepared for it, they need to put systems in place. I mean, there can be some significant financial damage on some of the most unsuspecting merchants if they are not being careful."

Executive, Mid-Sized Card-Issuing Financial Institution

Figure 17. Fraud As A Percent Of Revenue Among International And Domestic-Only Merchants

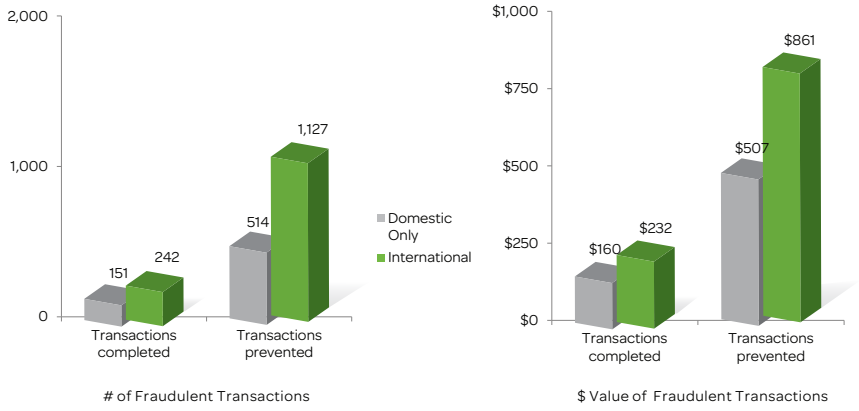


Q: What is the approximate dollar value of your company's total fraud losses over the past 12 months? Fraud losses as a percent of total annual revenue.

May 2013, n = 473, 666
*Base= Domestic-only merchants, international merchants

International merchants lose more revenue to fraud compared to domestic-only merchants as a result of the higher volume of frauds attempted against them, and the higher average ticket value of the transactions. International merchants prevent a greater proportion of attempted fraudulent transactions than do their domestic-only counterparts (82% vs. 77% of attempted fraudulent transactions are prevented), yet international merchants still experience a number (242 vs. 151 fraudulent transactions per month) and ticket value ($232 vs. $160) of fraudulent transactions which are roughly 50% greater than those waged against domestic-only merchants.

Figure 18. Monthly Prevented And Successful Fraudulent Transactions Among International And Domestic-Only Merchants



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

May 2013, n = 473, 666
*Base= Domestic-only merchants, international merchants

International merchants experience several unique challenges to controlling fraud, including issues of jurisdiction (11% rank this as their top challenge), challenges in acceptance of payment in internationally-based payment methods (7% rank this as their top challenge), a lack of specialized tools for controlling international fraud (6% rank this as their top challenge), and assessment of risk by country or region (only 2% rank this as a top challenge) (see appendix, figure 19).

However, the challenge international merchants most commonly cite as their primary obstacle, verifying customer identity, is one they share with domestic-only merchants. Thirty-nine percent of merchants consider verifying customer identity to be the most challenging aspect of selling to consumers abroad. However, while all merchants are struggling against a spike in identity-related crime, international merchants appear to be better fortifying themselves against this trend. The percent of identity theft in all fraud has remained stable for international merchants (at 21% of total fraud losses) even as it increased for all merchants (from 12% of all fraud in 2012 to 17% in 2013.)

"Earlier this year we saw a lot of debit card international [fraud]... We modified the rules and the strategies and tightened down on that. We probably went through a similar period with credit card last year. The rate of fraud on international purchase volume is higher than it is on domestic."

Executive, Large Card-Issuing Financial Institution

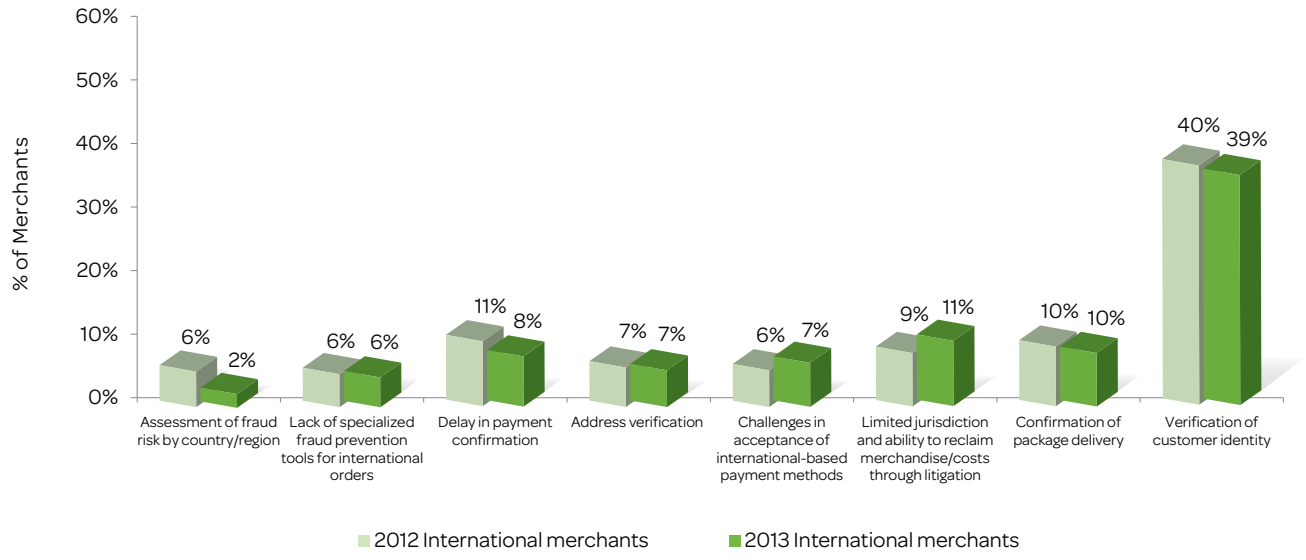
"So, for our US based merchants that are leveraging our solution... when we leverage device ID and device fingerprinting, they'll have a US internet or IP proxy, but then when we pierce the proxy we're able to see that activity coming from Malaysia, Philippines, Vietnam."

Executive, Large Merchant Acquirer

The stable distribution of international and domestic fraud since 2012 (27% of fraudulent orders were generated internationally in both 2012 and 2013) indicates that international merchants are seeing a reduction in revenue lost to both domestic and international fraud. Steps taken to better verify customer identity abroad have also likely had a positive impact on verifying domestic customer identity.

The fact that international merchants do not report diminished concern over customer identity verification since last year indicates that they may still be bombarded by this fraud type, but preventing more of it. Likely, international merchants invest more in preventing this fraud type as a result of the higher level they experience, and this investment paid off in the prevention of a proportionate increase to the one seen by all merchants in 2013. Their success cannot be attributed to any particular fraud technology solution, as they are no more likely than all consumers to use any individual solution. However, International merchants' generally more constructive attitudes toward fraud (see figure 5) and use of a greater number of fraud technology solutions in general (see figure 13) may be responsible for their ability to stave off the onslaught of identity-related crimes.

Figure 19. Top Challenges In Controlling International Fraud In 2012 And 2013



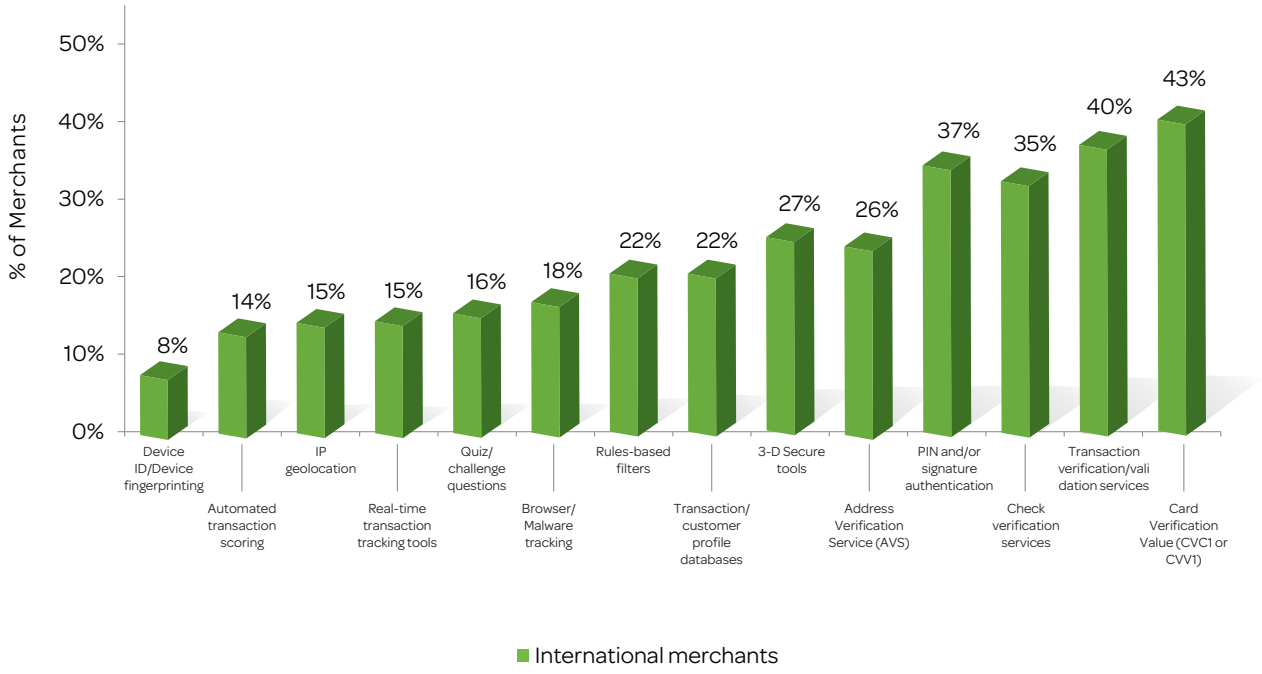
Q: Please rank the top 3 challenges related to fraud faced by your company when selling merchandise to customers outside the US. Items ranked as top challenge.

July 2012 - May 2013, n = 467, 473
*Base= International merchants

The same fraud technology solutions international merchants are currently using are the ones they perceive to be most effective at preventing international fraud (see figure 20 and appendix figure 24). In some cases, however, it seems to be the case that merchants are overconfident in the solutions they currently use, rather than doing enough background research to select what are truly the most effective solutions.

One example of this is evident when comparing card verification values (CVC1 or CVV1) to 3D Secure technology. Card verification values are static and can be stolen along with card numbers by MitB or other malware attacks, or by data breach. 3D Secure often involves backend authentication using customer and transaction profiles and risk-scoring, or secondary authentication on the part of the user. 3D Secure technology is superior to CVV, and yet international merchants perceive CVV to be more effective (35% vs. 26%). This may be a case where familiarity and use of a technology give a false perception of effectiveness, as 43% of international merchants currently use CVV, and only 27% currently use 3D Secure.

Figure 20. Use Of Fraud Technology Solutions By International Merchants



Q: Which of the following best describes your awareness and use of the fraud solutions listed below?
My company currently uses this technology

July 2012 - May 2013, n = 473
*Base= International merchants

Methodology

In May 2013, LexisNexis Risk® Solutions retained Javelin Strategy & Research to conduct the fourth annual comprehensive research study on U.S. retail merchant fraud. LexisNexis conducted an online survey using a merchant panel comprising 1,139 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 in order to obtain financial institutions' perspective on fraud losses. A total of nine interviews were completed with risk and fraud executives. Identity fraud victim data from a survey of more than 5,000 U.S. adults representative of age, gender, income, and ethnicity was also utilized to ascertain the consumer cost resulting from fraudulent transactions. In 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 in order to better reflect the actual distribution by industry and employee size of the U.S. merchant 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 introduces 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 percents were then re-calculated 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 2013 Identity Fraud Report on a survey conducted in 2012 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

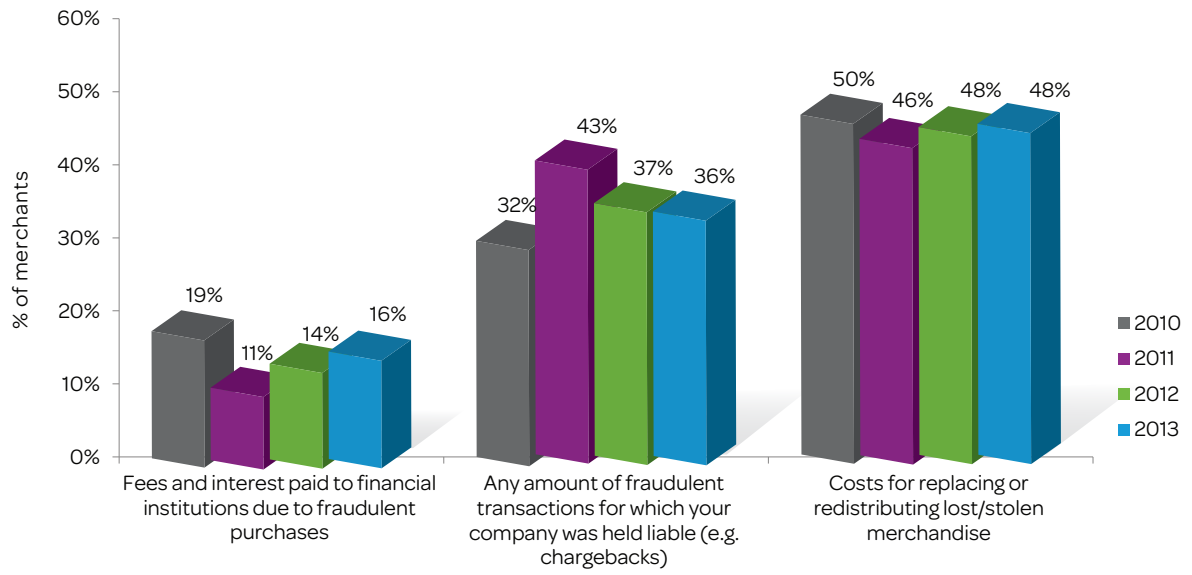
The 2013 Identity Fraud Report was conducted among 5,249 U.S. adults over age 18 on KnowledgePanel®; this sample is representative of the U.S. census demographics distribution, recruited from the Knowledge Networks panel. Data collection began Sept. 29, 2012, and ended Oct. 12, 2012. Final data was weighted by Knowledge Networks, while Javelin was responsible for data cleaning, processing and reporting. Data is weighted using 18+ U.S. Population Benchmarks 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 6 years ago) as well as total respondents, where applicable. For questions answered by all 5,249 respondents, the maximum margin of sampling error is +/1.35% at the 95% confidence level. For questions answered by all 857 identity fraud victims, the maximum margin of sampling error is +/3.35% at the 95% confidence level.

Appendix

Figure 21. Distribution Of Fraud Costs, 2010 To 2013

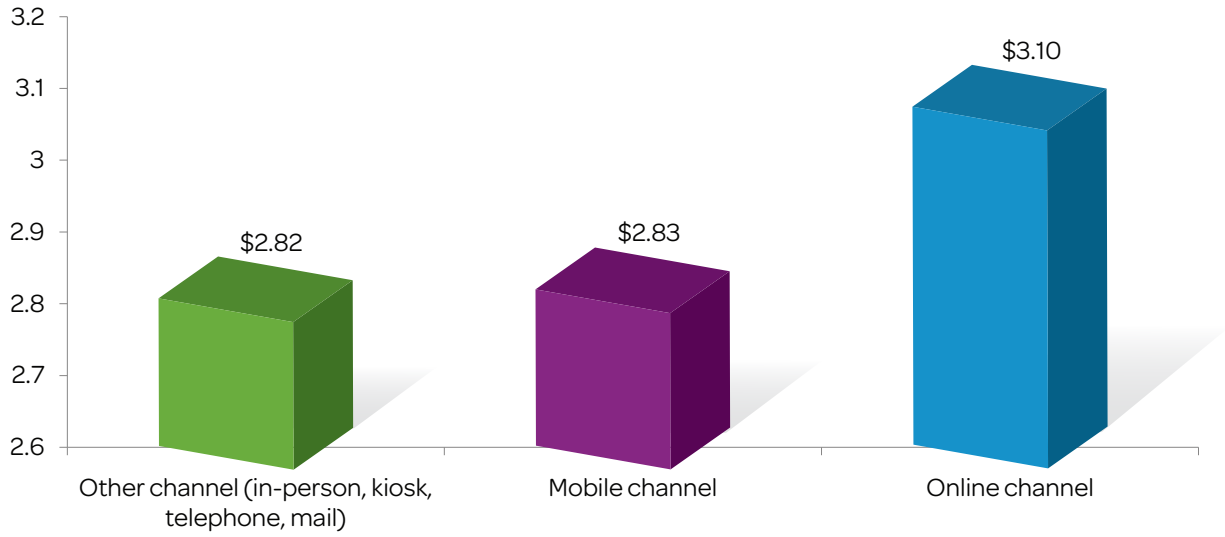


Weighted merchant data

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. Means

July 2010 – May 2013, n varies 145 to 712
Base= Merchants experiencing fraud amount greater than $0 in the past year

Figure 22. LexisNexis Fraud Multiplier Cost By Fraud Channel

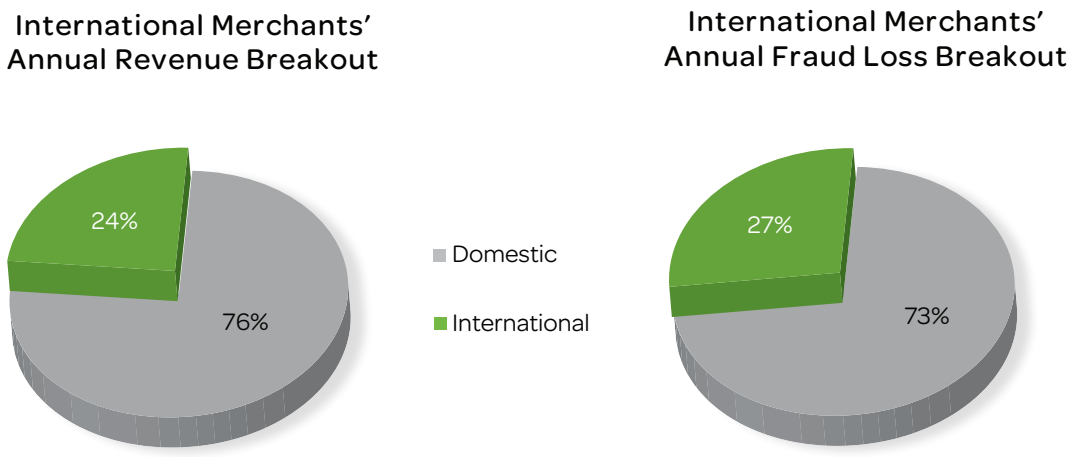


Weighted merchant data

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.

May 2013, n varies 41 to 152
Base= Merchants experiencing greater than $0 fraud through specific payment channels

Figure 23. Distribution Of Revenue And Fraud Losses Generated Through Domestic And International Orders



Q: Please indicate the percent of annual revenue generated through domestic compared to international sales in the last 12 months. International sales are orders that originate from customers outside the U.S. 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.

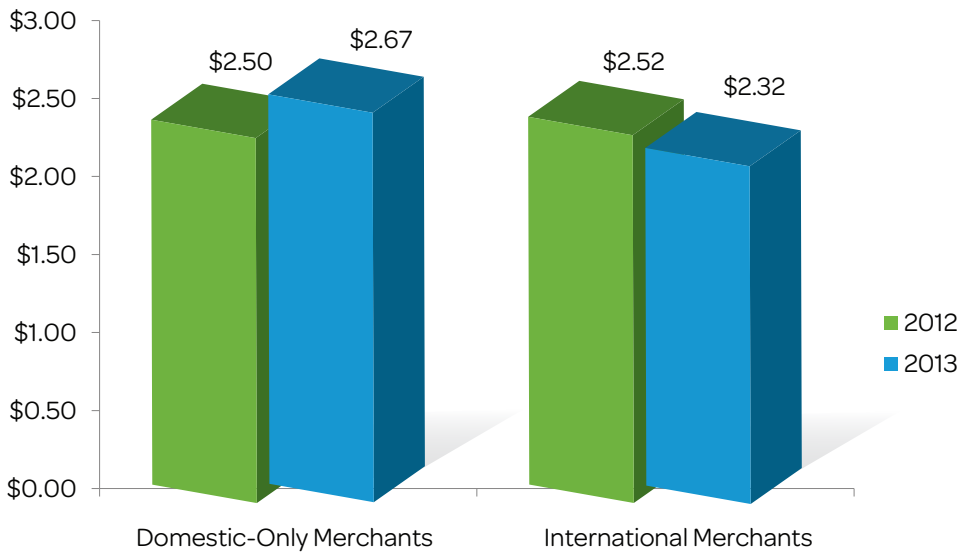
May 2013, n = 473
*Base= International merchants

Figure 24. Fraud Technology Solutions Ranked As Effective For Controlling International Fraud

Q: In your opinion, which of the following solutions is most effective in controlling fraud when you are selling outside of the U.S. (i.e. controlling international fraud)?

May 2013, n = 196, 1,139
*Base= International merchants

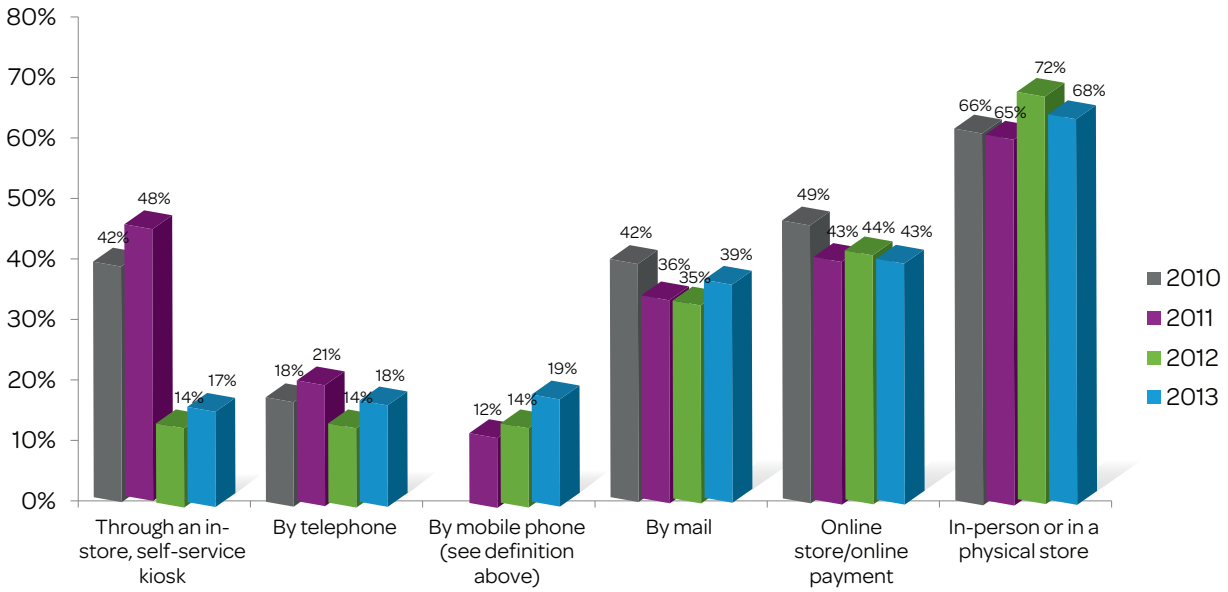
Figure 25. LexisNexis Fraud Multiplier Cost By International Merchants And Domestic-Only Merchants



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, May 2013, n varies 467 to 666
*Base= Domestic-only merchants, international merchants
© 2013 Javelin Strategy & Research

Figure 26. Percent Of Annual Revenue Attributable To Channels Among Merchants Accepting Payments Through Specific Channels By Year

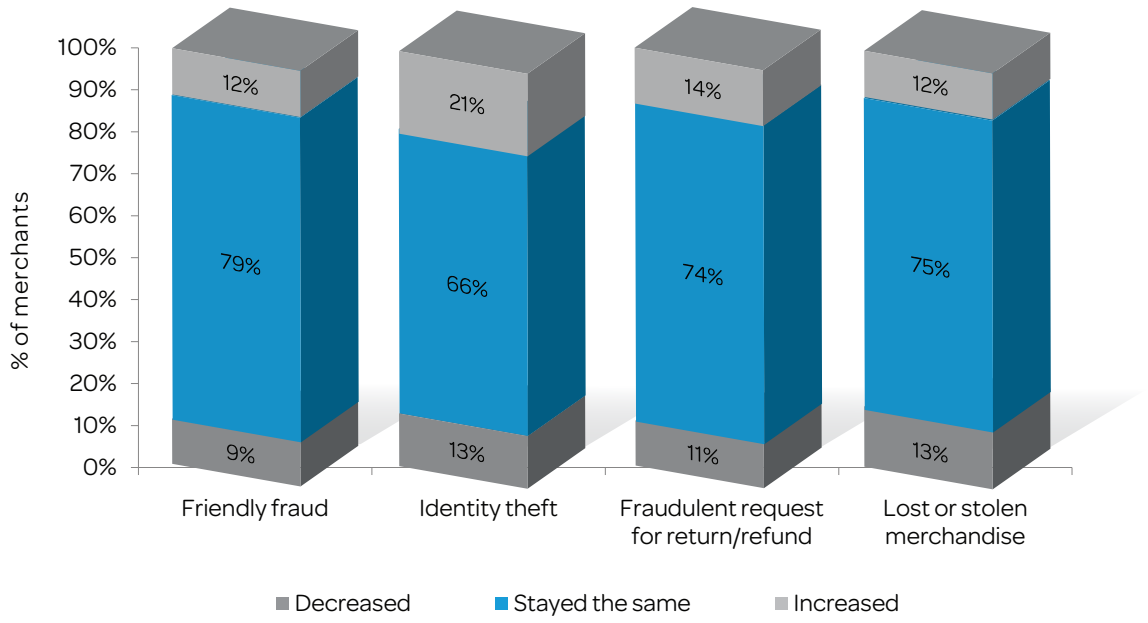


Weighted merchant data

Q: How does your company's total annual revenue over the past 12 months break out by sales channel?

July 2010 – May 2013, n varies 45 to 845
*Base= Merchants accepting payments through specific channels.
© 2013 Javelin Strategy & Research

Figure 27. Change In Incidence Of Fraud Types Over The Past 12 Months



Q: Please indicate whether the incidence of each of the following fraud types has increased, decreased, or stayed the same during the past 12 months.

May 2012, n = varies 577 to 725
Base: Merchants experiencing specific fraud types.

Sources

[1] https://www.bea.gov/newsreleases/industry/gdpindustry/gdpindnewsrelease.htm, accessed July 11th, 2013.

[2] http://blogs.carouselindustries.com/security/it-security-security/march-security-breach-roundup-evernote-paypal-and-making-the-case-for-two-factor-authentication/, accessed July 11, 2013

[3] 2013 Identity Fraud Report: Data Breaches Become a Treasure Trove for Fraudsters, Javelin Strategy & Research, February 2013.

[4] Ibid.

[5] http://datalossdb.org/statistics, accessed July 11, 2013.

[6] 2013 Data Breach Investigations Report, Verizon, April 2013.

[7] http://www.bankinfosecurity.com/network-hack-linked-to-card-fraud-a-5483/op-1, accessed July 10, 2013.

[8] 2013 Data Breach Fraud Impact Report: Mitigating a Rapidly Emerging Driver of Fraud, Javelin Strategy & Research, May 2013.

[9] http://www.computerworld.com/s/article/9239534/Schnucks_wants_federal_court_to_handle_data_breach_lawsuit, accessed July 10, 2013.

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.