Annual Report

LexisNexis® 2012 True Cost of Fraud

Merchants are facing an emerging frontier of fraud in global and mobile markets

September 2012

LexisNexis®

Retail

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions (www.LexisNexis®.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, 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.

Our eCommerce & retail solutions for automated scoring, identity management, workflow management and manual review assist organizations with protecting revenue, maximizing operational efficiencies and predicting and preventing eCommerce & retail fraud.

About Javelin Strategy & Research

Javelin Strategy & Research provides strategic insights into customer transactions, increasing sustainable profits for financial institutions, government, payments companies, merchants and other technology providers. Javelin's independent insights result from a uniquely rigorous three-dimensional research process that assesses customers, providers and the transactions ecosystem.

Introduction

The LexisNexis® True Cost of Fraud study, now in its fourth year, provides a look at the ways fraud affects U.S. merchants, consumers and financial institutions. This study identifies and quantifies the losses realized by these primary stakeholders when they become involved in a fraudulent retail transaction. It also explores emerging channels for retailers and the impact fraud may have on the effectiveness of these channels. Because retail merchants today are paying exorbitant amounts to combat and recover from fraud while trying to expand sales into new areas that increase exposure to fraud, this study meets a primary need often cited by merchants: guidelines and best practices, in the form of research-based benchmarks and recommendations, to help reduce fraud and confidently enter new markets.

The key question the 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

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

Quick Links

- Link to Merchants
- Link to Financial institutions
- Link to Consumers
- Link to Mobile-accepting merchants
- Link to Large ecommerce merchants
- Link to International merchants

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-accepting 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.

Key takeaways in 2012

- The LexisNexis® Fraud Multiplier, which calculates the "true cost" of fraud shouldered by merchants, has increased this year: Merchants now incur $2.7 in costs for each $1.00 of fraud compared with $2.3 in 2011. The increase is due to factors such as the impact of lost and stolen merchandise on the bottom line.
- Merchants are incurring additional post-fraud costs from customer attrition, yet most retailers are unaware of this finding. Although merchants believe that fraud does not impact loyalty or acquisition, one out of every three consumer fraud victims will change where they shop based on victimization.
- Acceptance of mobile payment is showing significant early growth, increasing by half over that in last year's study. Indeed, merchants have high expectations for the emerging mobile payments channel as a way to increase revenue and acquire customers. Says one merchant, "We think mobile wallets will be huge!"
- The Fraud Multiplier is now dramatically higher for mobile-accepting merchants. In stark contrast, a shockingly low 2% of merchants cite a greater need for security as major area of impact of mobile evolution on their overall business strategy.
- Large eCommerce merchants incur higher losses per fraudulent transaction, averaging a fraud ticket value of $219, than do merchants overall, at $120 per fraudulent transaction. This differential may result from larger merchants often being use to larger ticket amounts (and thus not having alarms raised on analytic systems).
- Large merchants can benefit from increased awareness of specific solutions and best practices. Despite being better educated than all other merchants about fraud-mitigation solutions, large retailers still know relatively little about device recognition and browser protection technologies. They also face challenges in integrating technology security solutions with identity-based data, which could help them to secure and authenticate card-not-present (CNP) transactions.
- Merchants that sell internationally are under siege in two measures of criminal activity: attempted (prevented) fraud as well as successful fraudulent transactions. Merchants in this category report being the target of over five times as many attempted fraudulent transactions as all merchants. Even though these global merchants stop a large number of attempts, fraudsters still succeed at defrauding them over four times as often as all merchants in general.

In preventing payments fraud, mental preparation (as in "preparing for the worst") is correlated with profitability. Surprisingly, merchants that believe fraud is inevitable are more likely to act as though they can change the course of fraud. The "fraud fatalists" uncovered in this study also tend to be the best-educated merchants about a gamut of fraud technology solutions.

Conclusions and recommendations

The dynamic nature of fraud requires that merchants compare themselves closely with their peers on the basis of size, market channel and more. Because the size and pattern of fraud are significantly impacted by economic conditions, this turbulent time requires merchants to be more vigilant than ever. Merchants often have no choice but to seek global or mobile markets for growth, yet this study shows that an "eyes-open" approach to preparing for the worst (as fraud fatalists do) is likely to predict success against persistent and inventive criminals. Even though increased technology solutions are also vital (and this study identifies several key protective methods that are surprisingly low in adoption), merchants must realize that customer relationships are just as important. Consumer research clearly indicates that customers vote with their feet after fraud, but a surprising majority of merchants surveyed in this study are not aware of this costly after-effect of fraud.

This study's recommendations include:

- Make fraud protection a higher priority. As merchants increasingly do business online, over mobile devices and around the world, they must take advantage of the many solutions available to aid in a battle that will become increasingly pitched and complex. Expect the worst to achieve the best, and use this study to benchmark levels of fraud and implementation of solutions.
- Improve overall profits by allocating more resources to retaining or even attracting customers who have been defrauded. Shoppers are often obsessed with their safety (and in particular, when shopping online), and they increasingly even want to play a role in their own self-protection. Productive engagement requires careful implementation of solutions, education and partnerships.
- Fully train and equip all staff members with the strongest possible policies and technologies. Because large merchants are the subject of higher-value fraudulent transactions, they must ensure that they are prepared to fight fraud at every level.

In short, expect the worst while becoming the best, through a multi-pronged strategy that includes the latest protective measures, customer-engaged communication or solutions and increased prioritization of specific solutions as you grow larger, more mobile and more global.

2012 fraud overview: Merchants, financial institutions and consumers

Merchants

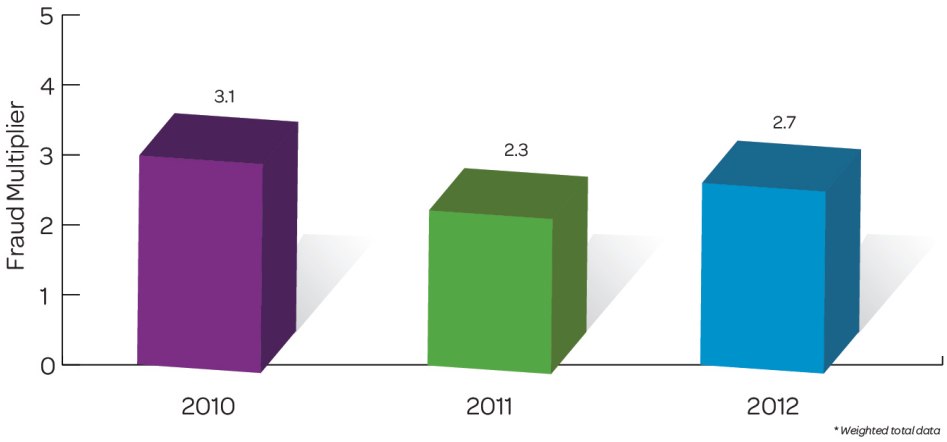
The overall LexisNexis® fraud multiplier has increased after a decline in 2011 from 2010. On average, merchants report they are paying $2.7 per $1.00 in fraud, a dramatic increase of $0.40 from last year. See Figure 1.

In 2011, this study predicted an upswing in CNP fraudulent transactions as a result of the spike in data breaches, which compromised the information of 15% of American consumers. This year, executives agree that an increase in CNP fraud is partially responsible for a rise in chargebacks.

With the limitations of today's mainstream consumer technology, merchants operating in CNP environments may have no way of knowing that counterfeit payment accounts are being used, but this research confirms that many fraudulent transactions are now occurring based on this popular criminal method.

True Cost of Fraud on the Rise in 2012

Figure 1. 2010, 2011 and 2012 Fraud Multiplier- by Total Merchants



Q15: 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, n = 527; July 2011, n=455; July 2010, n=712
*Base= Merchants experiencing fraud amount greater than $0

An executive from one medium-sized card-issuing bank explains the rise in chargebacks: "From a fraud perspective, the chargebacks are going up primarily due to the increase in card-not-present fraud. The chargeback line pretty much follows those cases, and as we see those continue to rise, we will see the chargebacks rise on that."

The LexisNexis® Fraud Multiplier calculates the true 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 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.

Large and medium-sized merchants pay less per dollar of fraud than small merchants do but still pay more than they did last year

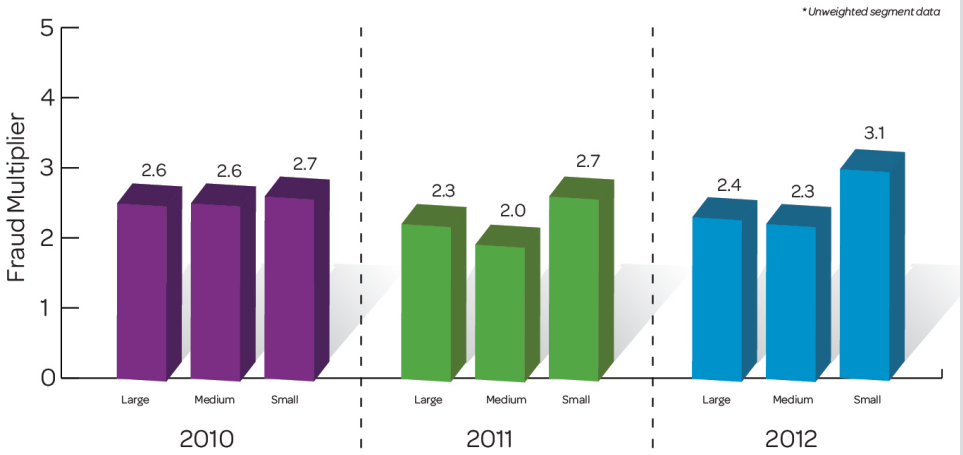
Large merchants are now paying a whopping $2.4 per $1.00 of chargebacks incurred, and over the past two years, small merchants bore the highest Fraud Multiplier (see Figure 2). For 2012, research found that a slight increase in the Fraud Multiplier for both large and medium-sized merchants could be driven by an increase in lost and stolen merchandise as a percentage of overall fraud. Large merchants are significantly more likely than all merchants to report an increase in lost and stolen merchandise (28% vs. 12%). Meanwhile, small merchants report the highest levels of lost and stolen merchandise (37% vs. 33% for medium-sized and large merchants) and attribute the greatest percentage of fraud costs to replacement and redistribution (46% for small merchants vs. 39% for medium-sized merchants and 40% for large merchants). Because they are the biggest targets for criminals, it's not surprising that large merchants were found to be the most likely to have heard of or tried the fraud solutions presented to them by researchers.

"They (merchants) probably don't know that there are counterfeit cards; they just know they get chargebacks, and if it's a face-to-face transaction, they don't really get the chargeback. It's really the card-not-present merchants that take it on the chin. . . You're going to hear [about chargebacks] more from card-not-present merchants, [but] you're going to hear it more from merchants who haven't invested in the detection tools themselves. You're not going to hear it as much from Amazon as you're going to hear from a tier II merchant."

–Executive at a large issuer and acquirer

True Cost of Fraud Still Lower Among Medium-Sized and Large Merchants

Figure 2. 2010, 2011 and 2012 Fraud Multiplier by Merchant Size



Q15: 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, July 2011, July 2012, n = varies 123 to 404
Base =Small Merchants, Medium Merchants, Large Merchants

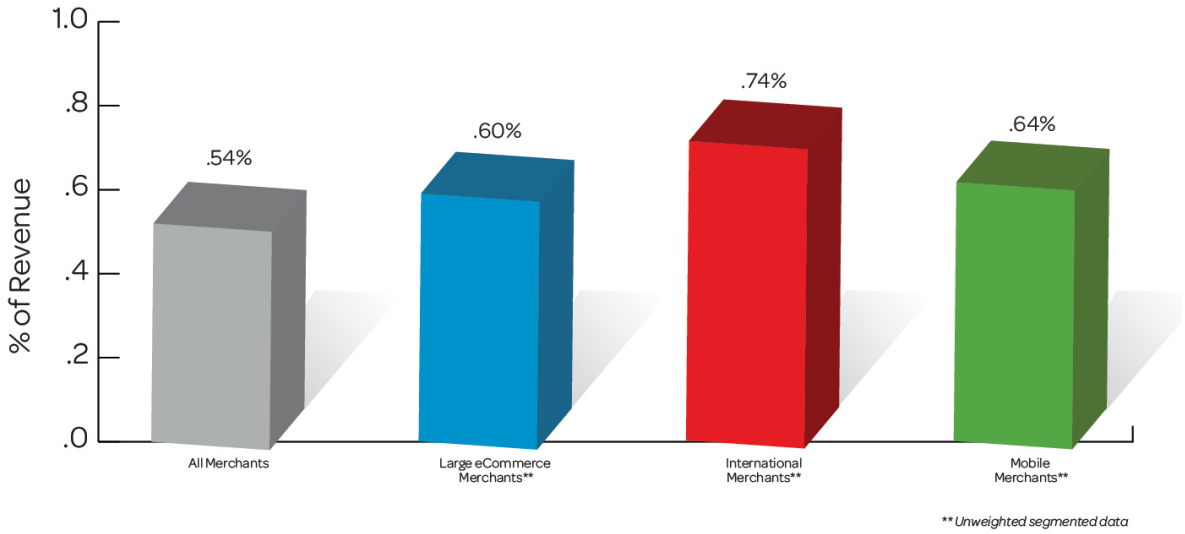
Credit card fraud is down to 60% of total fraudulent transactions in 2012 from 65% in 2011, while debit card fraud is on the rise again—20% this year after falling from 30% in 2010 to 18% in 2011. Check fraud has returned to its 2010 level of 46% after falling to 40% in the previous year's study.

Large eCommerce, mobile and international merchants experience higher rates of fraud

In addition to surveying 1,030 U.S. merchants, this study interviews key risk and fraud executives from FIs. Last year, FI executives anticipated a spike in more sophisticated types of attacks that would misuse false identities in "bust-out schemes" and collect money from credit card issuers' shell businesses as well as more advanced phishing schemes, Card Verification Value (CVV) cracking, ATM skimming and botnet hacking. FIs also predicted an upsurge in CNP fraud, fraud involving goods that are easily bought and sold and fraud among large e-commerce merchants. Consistent with these predictions, the study revealed higher-than-average rates of fraud as a percentage of revenue among large eCommerce merchants. Mobile and international merchants experience even higher rates of fraud losses.

Large eCommerce, International and Mobile Merchants Experience Higher Rates of Fraud

Figure 3. Fraud as a Percent of Revenue by Merchant Segment



Q15: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud costs over the past 12 months:

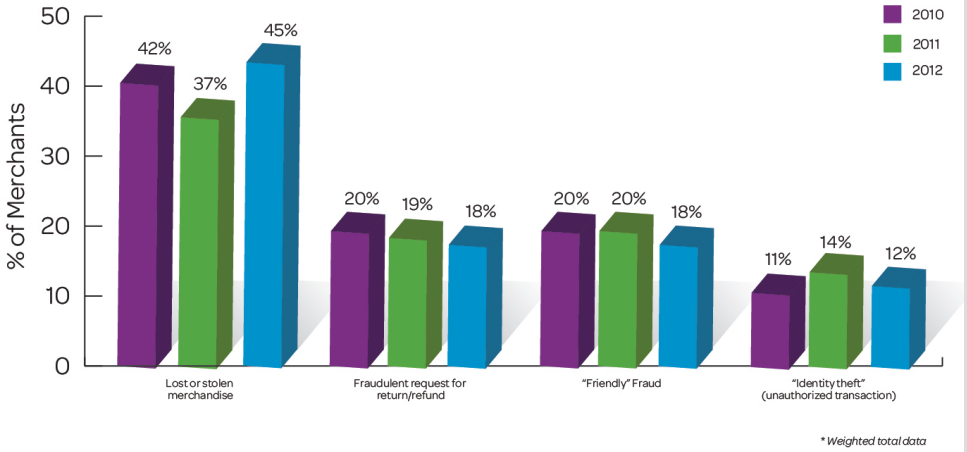
July 2012, n = 118, 183, 467, 1030
Base = All merchants, Large eCommerce Merchants, International Merchants, Mobile Merchants

Overall merchants report an increase in lost and stolen merchandise, quite possibly as a symptom of continuing difficult economic times. Friendly fraud has decreased from 20% in 2010 to 18% of total fraud losses (see Figure 4).

While friendly fraud has decreased as a percentage of fraud overall, mobile merchants and large e-commerce merchants still suffer the highest rates of this fraud type at 26% and 24%, respectively.

Lost and Stolen Merchandise an Increasing Problem for Merchants

Figure 4. 2010, 2011 and 2012 Fraud Loss by Fraud Type



** Weighted total data*

Q16: 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:

July 2010, July 2011, July 2012, n = 1005, 1006, 1030
Base: All merchants

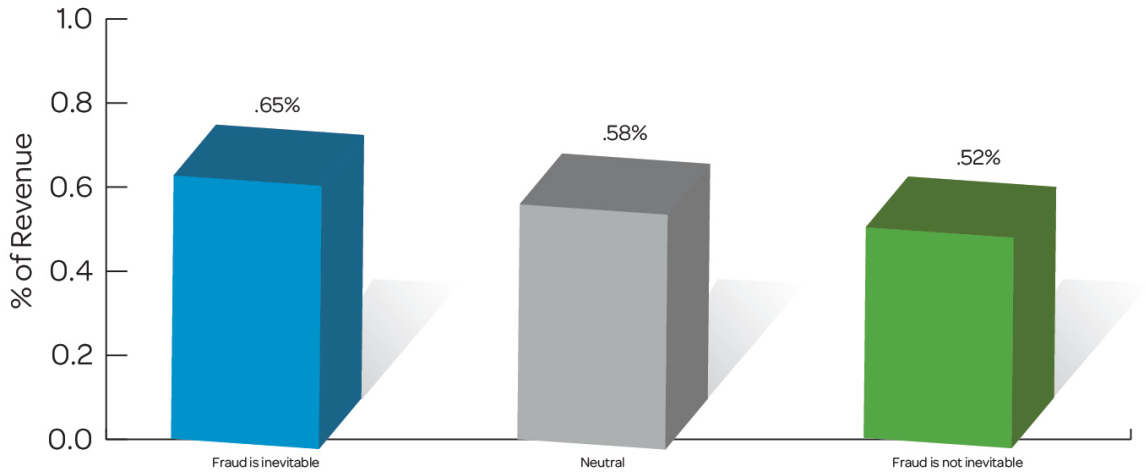
Fraud fatalists show healthy resolve to combat fraud despite incurring higher fraud losses

Merchants should emulate the mindset of fraud-fighting leaders at top merchants, which have prepared themselves for the worst while taking more active steps to accomplish the most profitable outcome. This research revealed that merchants that believe that fraud is inevitable are more likely to act as though they can change the course of fraud. These "fraud fatalists" tend to be the best-educated merchants about the gamut of fraud technology solutions. In fact, those that were aware of all 14 fraud solutions presented overwhelmingly believed that fraud is inevitable (59% compared with 19% that did not believe that fraud was inevitable). When combined with this study's qualitative interviews, this data likely indicates that leaders with the greatest expertise also view fraud as highly evolving and see no singular or combined offering of mitigation efforts as airtight solutions. However, this educated perspective is not correlated with a defeatist attitude among merchants—in fact, the opposite seemed to be the case as fraud fatalists were much more likely to employ at least one fraud solution (76% vs. 61% of those who did not believe fraud was inevitable).

Large merchants are significantly more likely than all merchants to be fraud fatalists (63% vs. 53%), demonstrating that those with responsibility for managing more transactions have armed themselves to manage the increased losses that come with increased sales. Yet, as Figure 5 shows, those that believe fraud is inevitable (among all merchants) lose a higher percentage of revenue to fraud than do merchants overall. In short, merchants do well to expect more encounters with fraudsters, and responding with the best techniques and solutions to protect profits.

Merchants with Fatalistic Fraud Attitudes Experience Higher Rates of Fraud in Total Revenue

Figure 5. Fraud as a Percent of Revenue by Merchants' Attitudes about Fraud



** Unweighted segment data*

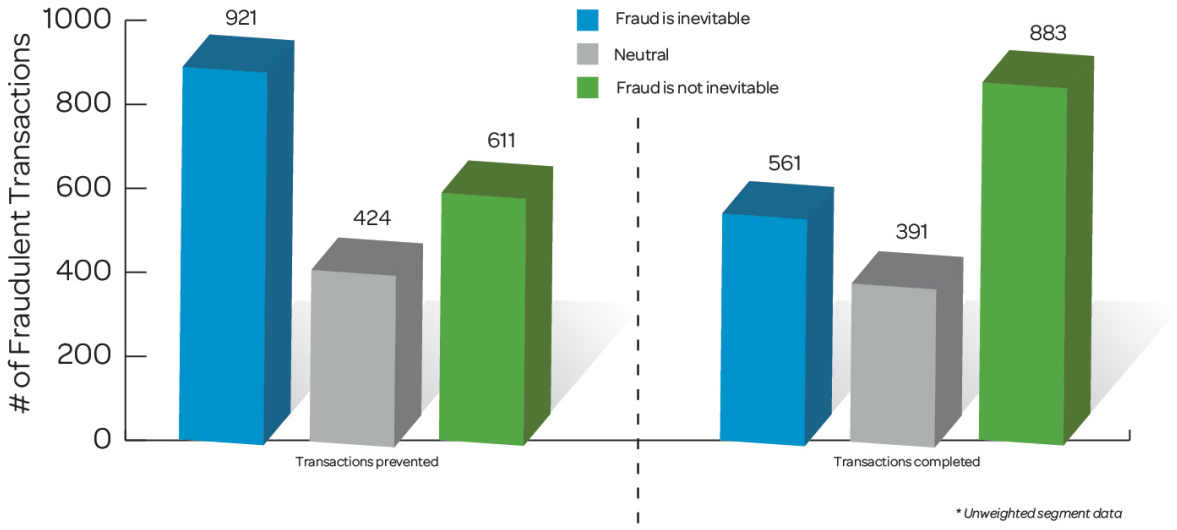
Q14: What is the approximate dollar value of your company's total fraud losses over the past 12 months?

July 2012, n = 215, 235, 580
Base: Merchants agreeing fraud is inevitable, neutral merchants, merchants not agreeing fraud is inevitable

However, this higher percentage of fraud losses in total revenue cannot be attributed to a lack of trying on the part of fraud fatalists. In fact, those that believe that some amount of fraud is inevitable show greater dedication than merchants overall to mitigating fraud as much as possible. Fraud fatalists are more likely to employ all fraud technology solutions than are merchants that believe fraud can be prevented absolutely, and they prevent more fraudulent transactions and experience fewer successful fraudulent transactions than those that do not believe fraud is inevitable. See Figure 6.

Fraud Fatalists Excelling in Fraud Prevention

Figure 6. Prevented and Successful Fraudulent Transactions by Fraud Attitudes



Q21: Thinking of the fraudulent transactions that are prevented, what is the average value of such a transaction?
Q23: Thinking of the fraudulent transactions that are successfully completed, what is the average value of such a transaction?

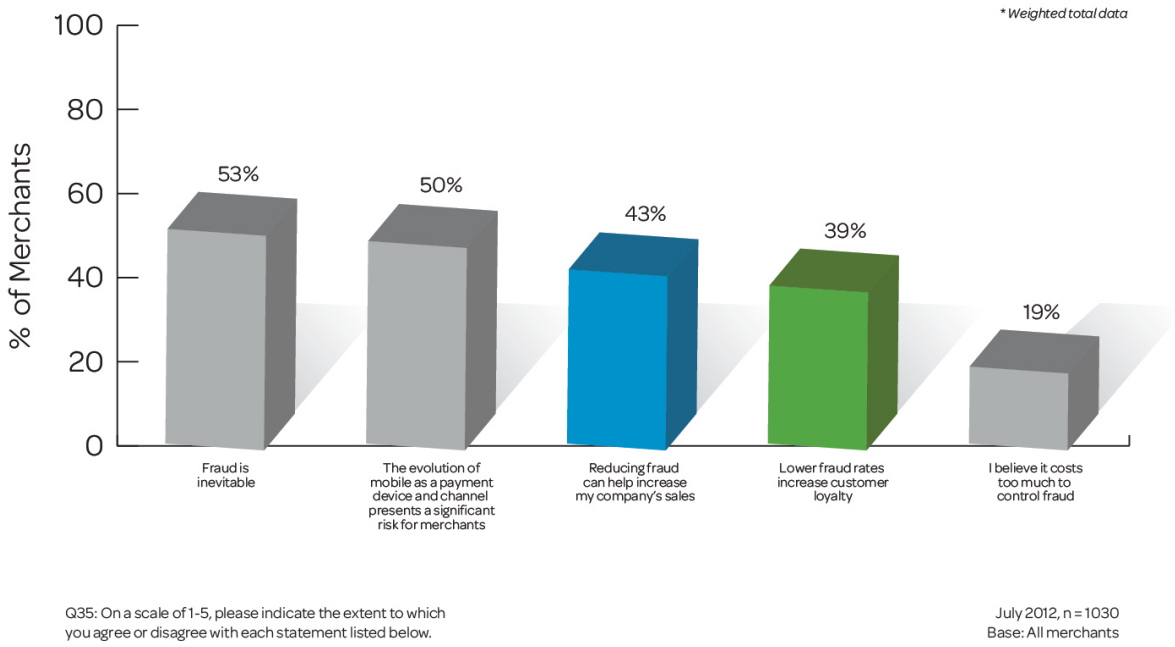
July 2012, n = 215, 235, 580
Base: Merchants agreeing fraud is inevitable, neutral, merchants not agreeing fraud is inevitable

More merchants need to view fraud as a customer loyalty measure

Through a comprehensive fraud-prevention strategy, merchants have the opportunity not only to minimize lost revenue in the immediate term but also to attract and retain customers through a stellar reputation for security. Figure 7 shows the rate at which merchants agree with common beliefs about fraud.

Two Fifths of Merchant Community Agrees Fraud Prevention is Tied to Sales and Customer Retention

Figure 7. Overall attitudes toward fraud: Proportion of Merchants Agreeing (i.e. Top 2 Box)



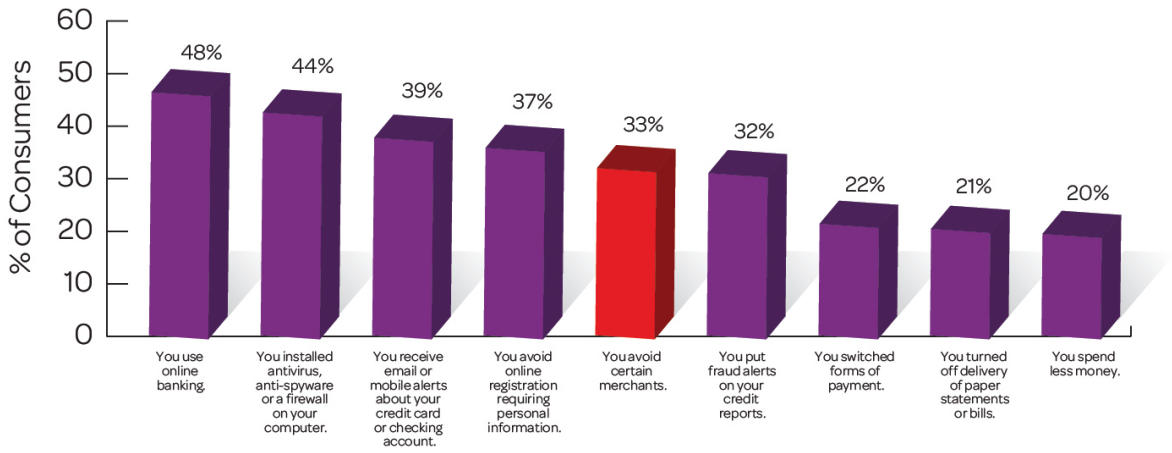
Among all merchants responding, 43% acknowledged that reducing fraud can help increase their company's sales, and slightly fewer (39%) agreed that lower fraud rates can increase customer loyalty. The implication is that roughly 60% don't relate fraud reduction to helping them achieve return on investment (ROI) or think reducing fraud can improve customers' loyalty to their business.

Yet of the 37% that expect some or significant impact from mobile commerce, meeting customers' demands and expectations—a loose proxy for loyalty—scored the highest among reasons for that impact.

Clearly, merchants with good records in preventing fraud and protecting customer information are trusted merchants. Thirty-three percent of Americans who fall victim to fraud avoid certain merchants as a result (see Figure 8). Customer confidence is critical in maintaining and improving reputation, and having the right attitude and actions to ensure strong security, including fraud risk mitigation, translates into returning customers for merchants demonstrating they have earned that trust. Conversely, merchants that have had breaches or publicly disclosed fraud losses are at risk of losing business and increasing their costs related to mitigating vulnerabilities and responding to incidents. Merchants must pay close attention to the often-overlooked impact of fraud on customer loyalty because losses due to customer attrition caused by the perception of poor security create a serious problem.

One Third of Fraud Victims Avoid Certain Merchants as a Result of Being Defrauded

Figure 8. Consumers' Actions as a Result of Being Defrauded



Q38: As a result of being a fraud victim, are any of the following statements true of you? Other response options available.

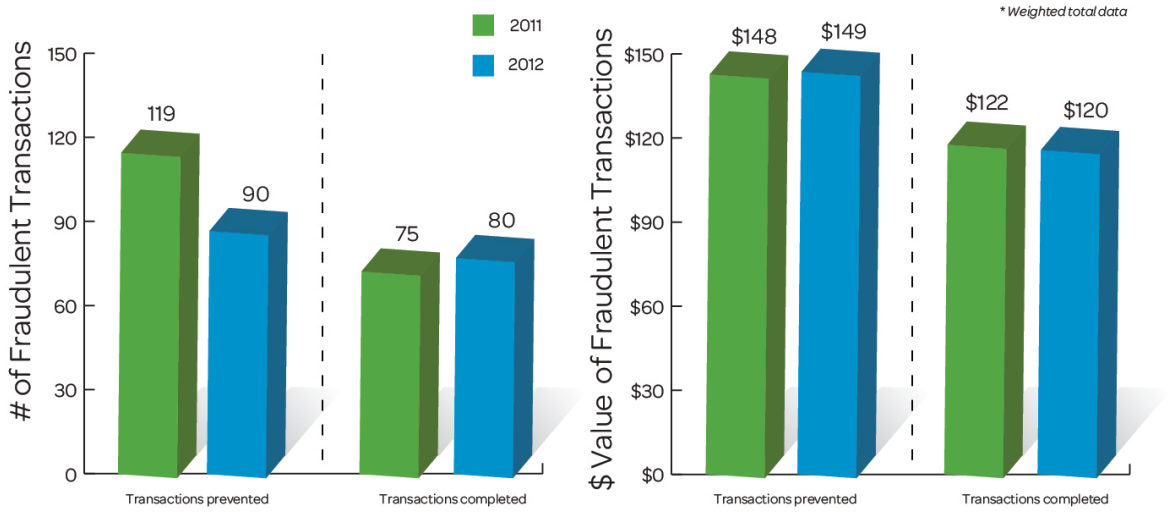
October 2011, n = 818
Base: Fraud victims

Criminals slip more transactions past merchant defenses

Merchants are preventing fewer fraudulent transactions in 2012 than in 2011, both in absolute numbers and relative to the number of successful fraudulent transactions detected (see Figure 9). This trend indicates that criminals outgamed merchants last year. Merchants will have to implement additional fraud strategies to outpace fraudsters and to retain customers through a solid reputation of fraud prevention.

Merchants Prevent Fewer Fraudulent Transactions Per Month in 2012 than in 2011

Figure 9. 2011 and 2012 Prevented and Successful Fraudulent Transactions



Q20: In a typical month, approximately how many fraudulent transactions are successfully completed at your company? Q21: Thinking of the fraudulent transactions that are prevented, what is the average value of such a transaction? Q22: In a typical month, approximately how many fraudulent transactions are successfully completed at your company? Q23: Thinking of the fraudulent transactions that are successfully completed, what is the average value of such a transaction?

July 2012, n = 1030
Base: All merchants

One reason merchants are preventing fewer fraud transactions is that many of them are unaware of the various antifraud and fraud-detection tools and techniques available. Also, a large number that were aware admitted not having used a specific technology or approach called out in this survey. Although the level of unawareness is surprising, the lack of implementation is not: 63% said they leverage services available through their processor or payment solutions providers. Respondents relying on a processor or other third parties tend to be smaller merchants. Larger merchants, including the massive online variety and big box retailers, have invested in antifraud tools.

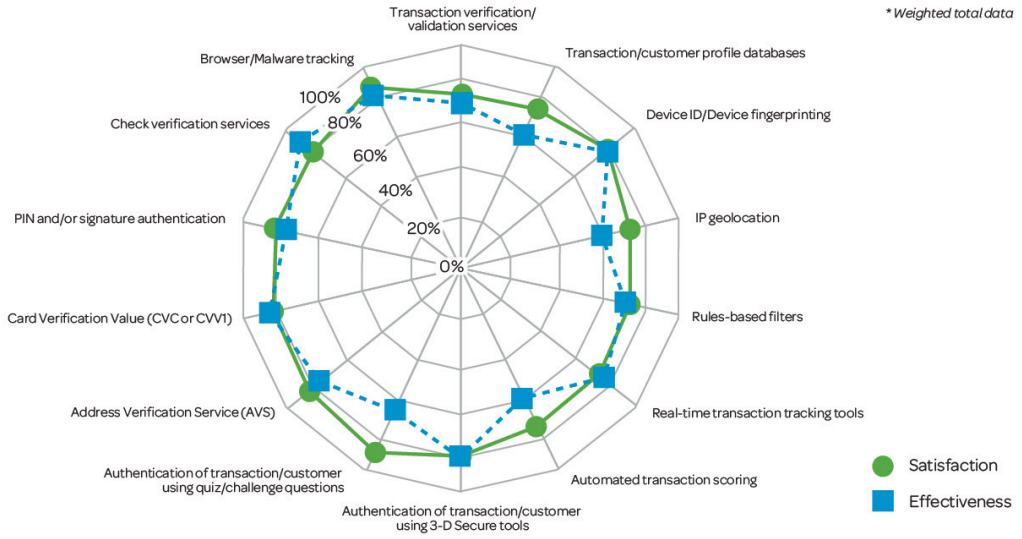
Merchants listed various methods of customer identity verification as top practices for controlling both friendly fraud and international fraud. Unsurprisingly, many of the fraud-prevention methods rated as most effective for preventing fraud (PIN/signature verification, check verification and card verification values) also show the highest rates of current use. Says one merchant, the top factor that could help the company prevent fraud would be to "confirm international identities and addresses."

In contrast, more than half of merchants (55%) had never heard of automated transaction scoring, and just below half had never heard of device fingerprinting, browser/malware tracking, IP geolocation and transaction/customer profile databases (47%, 47%, 47% and 46%, respectively).

Merchants are consistently pleased with the fraud solutions they utilize; between 70% and 90% of merchants indicate that they are satisfied or extremely satisfied with their fraud solution. In most cases, satisfaction maps closely with the perceived effectiveness of the solutions. For several methods, however, satisfaction exceeds perceptions of effectiveness, demonstrating that merchants are finding additional intangible benefits of value in solutions such as IP geolocation, quiz/ challenge questions, transaction/customer profile databases and automated transaction scoring. Such intangible benefits could include ease of implementation or operation or even enhancement of customer relationships (due to bolstering all-important online shopper confidence). See Figure 10.

Largest Gap Between Satisfaction and Perceived Effectiveness for Authentication Using Quiz/Challenge Questions, Automated Transaction Scoring and IP Geolocation

Figure 10. Satisfaction vs. Effectiveness of Fraud Solutions



* *Weighted total data*

Q33: On a scale of one to five, please indicate your satisfaction level with your current fraud detection solution(s). Q34: On a scale of one to five, please indicate how effective you feel your current fraud detection solution is in reducing potential fraud losses.

July 2012, n = varies 33 to 271
Base: Merchants using solution

Financial institutions

FI executives identified a variety of continuing fraud types, including counterfeit cards, card not present, check fraud, fraudulent new accounts, card magnetic stripe skimming and merchant account takeover. They highlighted shifting areas of concern, particularly in merchant account takeover, which can lead to high-value fraud in ACH, wire and other types of money transfer.

Merchant account takeover is an emerging fraud technique used by scammers who gain access surreptitiously to merchant's account and then conduct fraudulent transactions. The results of such crimes are larger rewards for the perpetrators because account takeover opens doors to fraud related to wire, ACH and money transfer transactions. Such financial tools would otherwise be out of reach for fraudsters, who previously focused on attacking individual merchants with a few fraudulent transactions.

The creativity and skills of hackers are apparent in other ways; one FI fraud manager reported finding a class of merchants' point-of-sale software compromised, leading to fraudulent transactions from that type of merchant in a specific geographical region.

The executives further verbalized concerns about growth in mobile fraud as that channel gains acceptance and volumes increase and (most critically) as scammers focus more on mobile commerce and mobile payments as a target of opportunity. One hope cited by executives was EMV (Europay MasterCard Visa, a global standard for payment cards with embedded chips), often referred to as Chip and PIN technology. Executives emphasize the need for merchants to pay increased attention to such card solutions that are ready for online and mobile fraud detection. EMV is exclusively able to directly address in-person fraud (unless consumer purchasing devices are outfitted with card-reading capabilities at some future time).

However even as executives held out hope that EMV would help reduce fraud in North America they also realized that strengthening antifraud controls in existing areas would push scammers to other exploitable areas in what one executive likened to the carnival game of "whack-a-mole." FIs and others told researchers it would be only a matter of time before determined fraudsters both find workarounds in the technology and migrate to the online and mobile channels where there is no method to read the information encoded on the EMV chip.

EMV was the subject of spirited speculation by many research respondents. Optimism over the technology's impact on in-person fraud-mitigation capabilities was widespread, and the common question asked was, "Why is it taking the U.S. so long to catch up with the rest of the world?" Yet leaders are also thinking about where persistent criminals will go next (namely, online and mobile), while worrying over ways criminals could exploit the technology itself.

FI executives report a surprisingly wide range of costs associated with fraud (including fraud losses as well as the costs of addressing incidents), which demonstrates the rapid state of evolution for the field of fraud mitigation. Depending on the size of the institution, fraud losses of as little as $3 million to as much as $45 million for a specific institution were reported. The average fraud amount was $200 on debit cards, over $300 on credit cards used by the consumer and much higher (over $1,000) for commercial accounts, depending on the channel used to commit the crime. In terms of staffing and other expenses of addressing criminal incidents, FIs report having resolution staffing levels as low as four full-time equivalents (FTEs) plus oversight and infrastructure costs, or approximately $200,000 to $300,000 for a bank that sold off most of its credit card portfolio and, at the other end of the scale, up to $13 million and staffing in the low hundreds

CNP and counterfeit cards continue to dominate merchant fraud, followed by merchant account takeover and skimming. Scammers gain access to accounts through e-mail hacking, malware and man in the browser (MitB) attacks. Small merchants are particularly vulnerable to these forms of attack because they lack technology resources (IT, dedicated fraud professionals, security software, firewalls, etc.).

Accompanying this trend of account takeovers is fraud in ACH, wire and money transfers, in which scammers use taken-over merchant accounts to penetrate these payment methods that can, in some cases, be less exposed to outsiders yet have fewer standardized network-based safety controls.

Also, mobile fraud is growing. The number of mobile users only recently reached critical mass, attracting the attention of scammers. Existing tools are helping to prevent losses in mobile transactions but will require bank experts to keep ahead of scammers.

Recommendations to merchants from financial institutions (FIs)
FI executives freely offered advice to merchants to help reduce fraud. In the FI executive interviews this year, two primary themes emerged: The need for more communications and collaboration and the suggestion that the retail and FI sectors move more dynamically toward current technology and process solutions (such as address verification, CVV and even 3-D solutions offered by networks as well as infrastructure changes in North America, specifically related to adoption of EMV cards).

"We need better working relationships between the banks and merchants and the associated fraud teams. Developing and training fraud specialists on the bank side with merchant knowledge and terminology can help bankers understand the concerns and needs of merchants."

–Leading card-issuing banker

.

Recommendations for collaboration and cooperation

Time and again, FI executives called for more communication and collaboration between banks (including issuers or acquirers, depending on the opportunity) and merchants, sometimes with facilitation by payment networks. Although various forums do exist for the exchange of ideas, advice and support, none of the interviewed executives identified such industry groups as the venue for these discussions. One even passed the buck to the card associations:

"There's not a lot of communication between the issuers and the merchants. It's not like if you see fraud coming from a given merchant that you're going to call them and say 'what did you do in this transaction three weeks ago?' and they're going to spend time on it. It seems it should be the card associations [reaching out] since their brand should be facilitating and coordinating the communications on risk controls, emerging trends and so forth to both the issuers and merchants. They generally do that, but at times, this seems to be a bit too political and they are more concerned with CYA with regards to any legal risk, which is understandable. But at times it's also unfortunate because it waters down the communications. "
–Executive at a medium-sized issuer and acquirer

But FI executives are willing to help. For example, one said that banks could provide more fraud intelligence information and could even offer payment card industry (PCI) compliance consulting to allow merchants to test and certify compliance with the PCI's recommendations. But the theme of having better interactions among FIs and merchants was repeatedly aired:

"We need better working relationships between the banks and merchants and the associated fraud teams. Developing and training fraud specialists on the bank side with merchant knowledge and terminology can help bankers understand the concerns and needs of merchants."
—Executive at a medium-sized issuer

The attitude that both groups share the concerns and responsibility came through from the FIs, but with some frustration over the nature of the discussion:

"No one of us holds the magic wand. We all need to be accountable. We're all in this together; we're going after the good transaction and working to stop all the bad transactions. [But] you have to have the stick, the liability to say, 'Hey, you didn't hold up your end of the bargain, you didn't do everything you could, so now you've got to be accountable.' You feel there is so much contention that the notion of liability almost clouds our vision from what we're really trying to solve. It seems every conversation comes back to that, and we don't have the upstream conversation about what we can collectively do to stop every bad (transaction) and approve every good. We get too focused on the tail wagging the dog."
–Executive at a large issuer and acquirer

Recommendations for technology and process

The theme of working together came through in conversations that turned to matters of technology and process. One FI executive discussed sharing information about risk infrastructures:

"Sometimes it's very easy to tell when there's counterfeit activity if you do a little zip code, time and space analysis . . . We're putting in some enhancements in our system to be able to calculate for every card-present transaction what the miles per hour would be required to go between those two zip codes."

–Executive at a medium-sized issuer
"Merchants can learn more about the risk infrastructures that banks use, recognizing that they can be very different from those used by merchants, depending on size, type, risk profile and other factors."
—Executive at a medium-sized issuer and acquirer

Understanding the banking industry's approach from a card-issuing perspective, merchants were urged to increase verification of consumer data while verifying information (such as the shipping address against the billing address). FI executives spent much time stating their belief that merchant verification of consumer data is imperative to prevent fraudulent transactions, yet it is nearly impossible for online merchants to do such verification online (for example, because the card cannot be held and observed by a remote merchant). Other issuers mentioned joint industry solutions around terminals and negative databases, such as terminated merchants and terminated originators, and the importance of openly sharing such information.

"Authentication is the number one tool merchants can use to reduce loss, chargebacks and fees associated with fraud. It's really 'know your customer' on the due diligence side."
—Executive at a medium-sized issuer

The introduction of self-service terminals in retail settings highlighted one executive's concern, a point-of-sale location that becomes a point-of-fraud location because no one is monitoring the situation.

"My pet peeve is self service terminals where people stand there running card after card after card that gets declined before they find one that gets approved. I think it raises all sorts of red flags if someone is pulling card after card to get that $500 to go through."
—Executive at a medium-sized issuer

Some issuers complained of a perceived lack of motivation on the part of merchants, believing that clerks can prevent much more in-person fraud by verifying with a picture ID or comparing signatures. "There's just no incentive, and we all eat the cost," said a pair of debit issuer fraud executives. Biometric solutions could help in such situations, particularly if incorporated within standardized clerk verification procedures.

And finally, there is hope that upgrading the infrastructure for acceptance of EMV-enabled cards would do much to assist in the fight against fraud, but the effort requires (once again) collaboration and cooperation:

"Chip cards, chip cards and chip cards. Certain kinds of fraud are migrating here [to North America] because we don't use chip cards. We're still on old-fashioned magstripe cards. The crime is migrating to the local market."
—Executive at a medium-sized issuer and acquirer

"Upgrading terminals for EMV is a merchant expense for the most part, but I would like to see more effort on both sides for moving to EMV because I think merchants will benefit from EMV. We need to do a much better job working together. I don't see that collaboration currently."
—Executive at a medium-sized issuer

One debit card issuer called for networks to mandate two changes:

- Indicate when a stored-value card was used in a transaction in order to consider the higher risk, just as cash back is sometimes indicated now.
- Transmit Zip codes, indicating the physical merchant (or even ATM) locations. This information can, in turn, be used by analytic systems to calculate the likelihood of fraud based on time and space of adjoining transactions.

Table 1 compares the differing perspectives among FIs who primarily serve merchants (as acquirers) versus those who serve consumers in a card-issuing capacity:

Table 1. Trends and Recommendations of Merchant Acquirers and Issuing Banks, 2012

FI Interview Topic	Merchant-Acquirer Banks	Issuing Banks
Highest-priority fraud trends in the past 12 months	Rise in online cyber crime	Counterfeit cards
	New account fraud	Card-not-present fraud
	Deposit fraud	Merchant account takeover
		Wire transfer fraud
Recommendations cited for merchants	Share information	Learn your bank's fraud infrastructure
	Share customer and fraud databases to help merchants authenticate customers and transactions	Know what authentication, security and verification methods are available
	Take advantage of third-party authentication solutionS	Train employees to recognize the signs of fraud
	Begin the shift to EMV technology	Watch for individuals cycling through multiple cards after being declined
	Reach out to merchant security groupS	Watch for individuals distributing purchases across multiple cardS
	Learn what new threats and security strategies other merchants are facing and employing	Establish clear lines of communication with your FI

Consumers[1]

Fraud incidence rose to 4.9% among the U.S. adult population of consumers over the past year, and the largest quantity of transactions is occurring in CNP payment cards. Because the mean fraud amount has dipped, however, the total fraud amount dropped to a record low of $18 billion in 2011. Mean consumer costs per fraud victim have flatlined rather than decreased in proportion to the mean fraud amount, despite decreasing hours spent in resolving fraud incidents.

The stability in consumer costs of fraud despite decreasing fraud amounts and a decrease in the number of resolution hours is reflective of trends in the types of fraud and the payment channels through which fraud is taking place. Trends in card fraud, mirror the upward trend in total fraud, rising from 2.3% in 2010 to 3.2% in 2011, as Table 2 shows. However, the mean consumer cost for card fraud fell 20% from $298 to $240, perhaps resulting from the reduction in mean detection time. For the first time in history, this study's data shows that electronic detection methods—correlated with lower mean detection times—have surpassed the volume of fraud cases in which consumers detected fraud by reviewing their paper bank statements.

Table 2. Existing Card Fraud (Debit and Credit Combined), 2009–2011

Consumer Fraud Measures	2011	2010	2009
Incidence Rate (past 12 months)	3.2%	2.3%	3.5%
Total Annual Cost	$8	$8	$14
Mean Fraud Amount	$1,324	$1,790	$2,072
Median Fraud Amount	$400	$587	$665
Mean Consumer Cost	$240	$298	$384
Median Consumer Cost	$0	$0	$0
Mean Detection Time (in days)	30	38	52
Mean Misuse Time (in days)	37	54	60
Mean Resolution Time (in hours)	9	11	12
Median Resolution Time (in hours)	2	3	3

Data breaches are becoming increasingly dangerous. This year, both the number of exposed records per data breach and the correlation between having one's records exposed and becoming a fraud victim have increased—pointing to a losing battle for privacy. From 2010 to 2011, the percentage of Americans notified that their information was compromised in a data breach in the past 12 months rose from 9% to 15%. Data breach victims are 9.5 times more likely to have their information misused than those whose information was not compromised in a data breach, which represents a sharply increased correlation between security and fraud incidents over four consecutive years of Javelin's annual Identity Fraud consumer surveys.

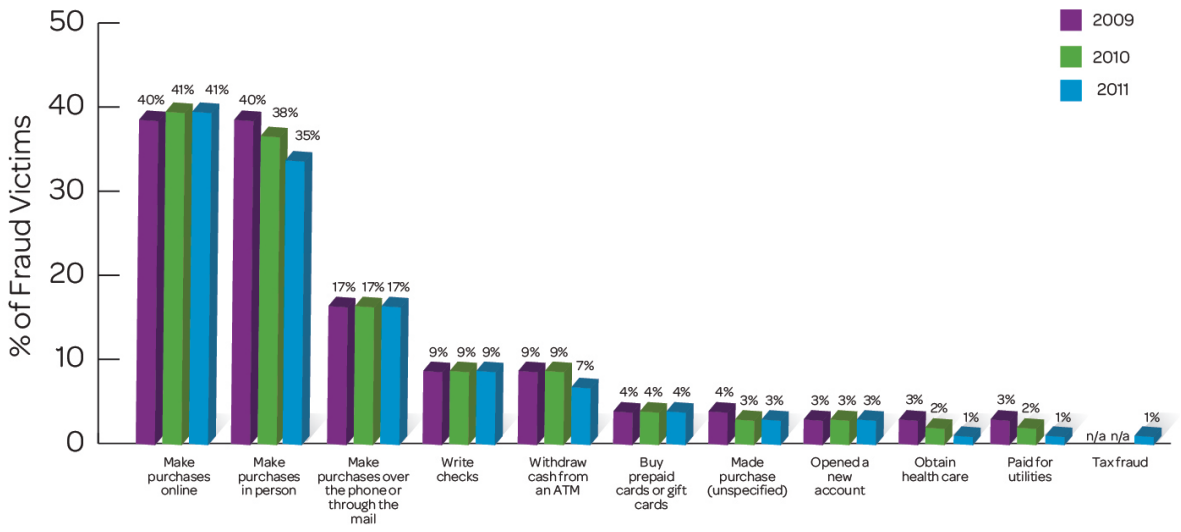
In the case of a data breach, merchants can minimize customer attrition and damage to their reputation by helping consumers prevent misuse of their breached information. Including instructions on where to set fraud alerts or purchase credit or personal data monitoring services along with providing notifications of data breaches can help reduce losses to customers and show that the merchant cares.

Minimizing costly fraud that stems from breached data requires a two-thrust merchant strategy: protect data and stop fraudulent transactions. Breaches and other privacy violations can be damaging to overall reputation while exposing firms to active regulators, attorneys, consumer activists and even self-policing networks. Fraud mitigation requires educating and equipping both clerks and customers, and evidence shows that customers are increasingly motivated to take charge of their own data separately.

Figure 11 shows how fraud victims' information was misused.

Fraudulent Online Purchases Surpass In-Person Purchases as Primary Fraud Channel in 2011

Figure 11. Consumer Information Misuse Trends, 2009–2011



Q12. How was your information misused? Was it used to...?

October 2011, 2010, 2009, n= 799, 423, 649
Base: All fraud victims.

Large merchants that issue store-branded credit cards should note that their customers may incur higher costs when fraud occurs through this channel. Customers whose store-branded card was misused incurred 1.6 times higher fraud losses and almost twice the amount of consumer costs as did credit card fraud victims who were victims of fraud through a major network-branded credit card (see Table 3). A likely reason for the difference is that network credit cards offer a number of consumer-facing security measures—such as customizable alerts and zero-liability policies—that help consumers to detect fraud faster and protect them from out-of-pocket costs.

Table 3. Costs of Fraud Related to Store-Branded and Network-Branded Credit Cards, 2011

Credit Card Type	Mean fraud amount (in dollars)	Mean consumer cost (in dollars)	Mean detection time (in days)	Mean resolution time (in hours)
Store-branded useable only at a specific store	$2,317	$591	64	11
Credit card usable anywhere	$1,406	$299	23	9

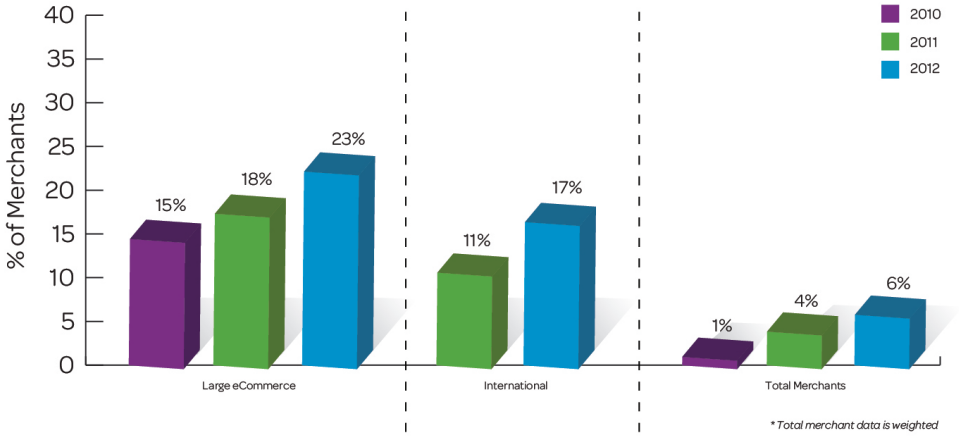
II. Spotlight: Mobile-accepting merchants

Acceptance of mobile as a payment channel has increased by half over the past year to 6% of all merchants, up from 4% in last year's merchant survey. Most merchants that accept mobile payments do so through the mobile browser; the mobile application is a runner-up. Large eCommerce and international merchants are leading in mobile acceptance at 23% and 17%, respectively (see Figure 12).

Of merchants that do not currently accept mobile payments, 17% say that they plan to expand into this channel within the next 12 months.

Large eCommerce Merchants Drive Mobile Payments Acceptance

Figure 12. Mobile Payments Acceptance Rates by Merchant Segment



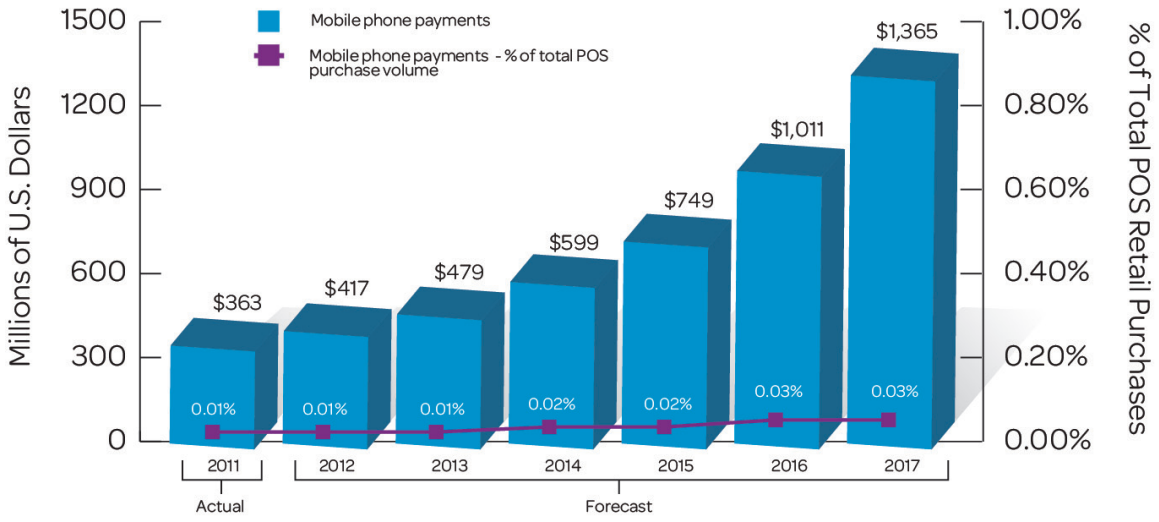
Q5: Does your company currently accept payments through any of the following channels? Please carefully select all that apply.

July 2010, July 2011, July 2011, n = varies 183 to 1030
Base: All merchants, international merchants, large eCommerce merchants

Merchants hoping to prevent fraud through the mobile channel should consider advanced, layered security methods, such as address verification (for physical goods), multifactor identification complete with IP geolocation and other mobile-specific solutions to battle the many expected new mobile risks. Because consumers shopping with mobile devices will typically have a stronger technology competence, merchants and issuers alike can increasingly include customers in active protection methods specific to the mobile channel. Figure 13 shows the expected trend in mobile retail sales through 2017.

Mobile POS Sales Expected to Increase More than Threefold in The Next Five Years

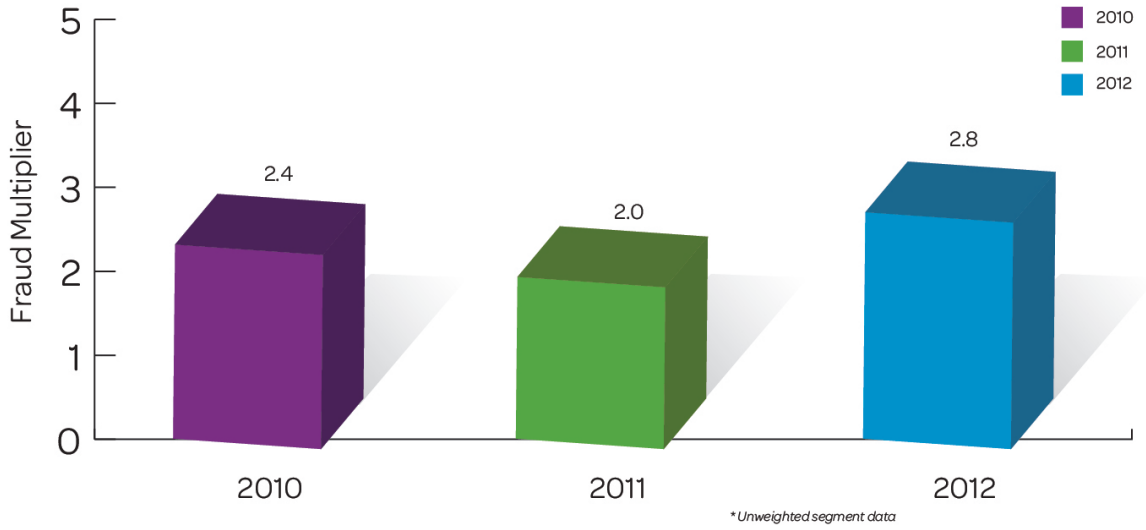
Figure 13. Volume of Mobile Retail Sales, 2011–2017[2]



Mobile-accepting merchants, whose fraud multiplier has historically been surprisingly lower than average, have seen a steep increase in this metric. In 2011, mobile-accepting merchants paid $2.00 for every $1.00 lost to fraudulent transactions, and this year they pay over 40% more, or $2.83 per dollar lost (see Figure 14). This study's researchers believe that this increase shows that criminals are shifting more attention to merchants that use a broader array of sales interaction methods, apparently with renewed impact, as merchant acceptance has opened just enough to finally attract real fraudsters.

Fraud Multiplier Spikes Among Mobile Merchants this Year

Figure 14. Mobile Merchants' Fraud Multiplier, 2010–2012

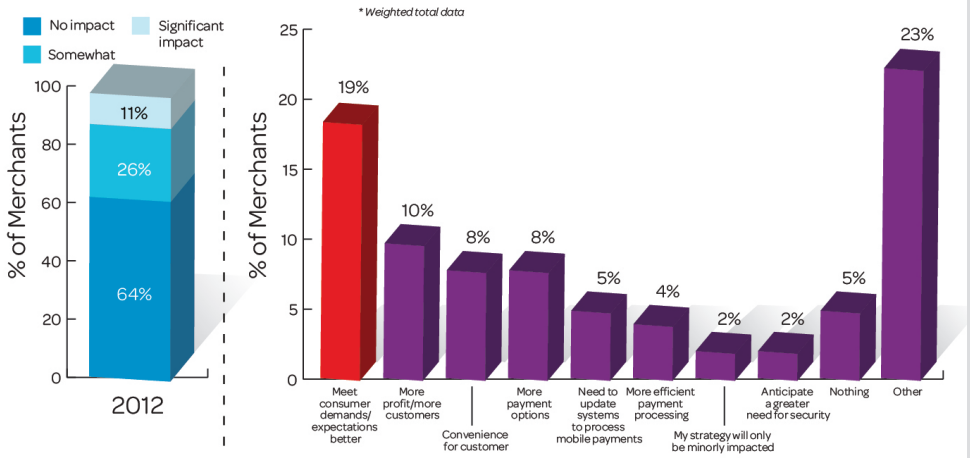


July 2010, July 2011, July 2012, n = 85, 78, 118
Base: Mobile Merchants
Caution: Low Base

The diversity of mobile devices and their operating systems, plus the variety of methods for m-commerce and m-payments (including browser, apps, text and evolving near-field communication (NFC) methods) represent near-future challenges for the industry. Concerns were expressed over reported vulnerabilities in some of the mobile card acceptance devices now populating the small merchant environment. However, mobile devices can also help improve security by providing consumers with increased personal account-monitoring capability, serving as one-time-password tokens and being an out-of-band authentication device for online transactions.

Thirty-seven percent of merchants do expect some or significant impact on their business strategy as a result of mobile commerce and mobile payments, as Figure 15 shows. Of the 37% that did expect to be impacted, 19% cited meeting customer demands/expectations and 10% cited increasing profit and/or customers as the most common ways they would be affected. Curiously, only about 2% expressed concerns about mobile security. This is not entirely atypical of the introduction of new, emerging platforms for which functionality ("does it work?") assumes primacy over security questions, and this study predicts that merchants will increasingly shift from inattentiveness to concentrated focus on mobile security.

Figure 15. Impact of Mobile Payments Evolution on Overall Business Strategy, 2012



Q11a: To what extent do you expect the evolution of mobile as a payment device or a payment channel to impact your overall business strategy? Q11b: In the space provided below, please briefly describe your reasons

July 2012, n = 1030, 375
Base: All merchants, merchants believing mobile will impact business strategy

International and large eCommerce merchants continue to adopt mobile payments channels at a higher rate than do all merchants and are much more likely to expect the evolution of mobile payments to affect their overall business strategy (31% and 43%, respectively, vs. 11% for all merchants). This rate is in part due to their greater access to resources for developing mobile platforms and in part because these businesses rely on remote purchases, believing that their customers are more likely to expect the most current remote payments options. According to one large eCommerce merchant, "Mobile is a key component of our strategy to offer our consumers the range of payment choice that they will come to expect in upcoming years. We think mobile wallets will be huge."

"[Mobile is] the fastest-growth payment in my company."

—Senior vice president of risk and fraud, hotel/ travel industry

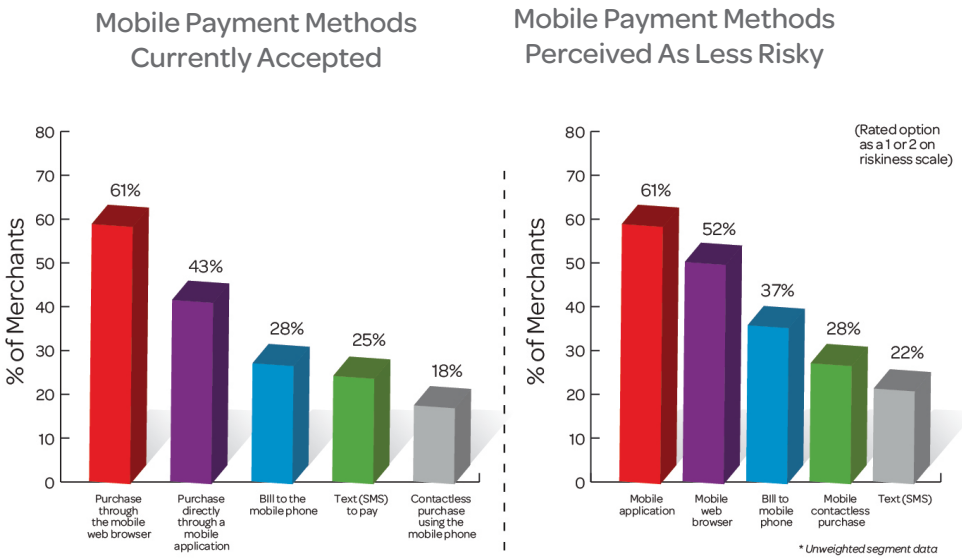
"...Customers will soon expect to pay their bills via mobile."

–Loss prevention manager, textile/ apparel/clothing industry

Mobile-accepting merchants adopt the methods they perceive to be least risky

As mobile gains prevalence as a payment channel, risk perceptions are guiding merchants' decisions about the mobile payment methods they adopt. The methods mobile-accepting merchants are currently accepting map very closely with the methods they perceive to be least risky, as Figure 16 shows. Figure 17 shows merchants' losses by fraud type.

Figure 16. Mobile Browser and App Considered Least Risky



Q9: You previously indicated your company currently accepts payments over the mobile phone. Which of the following mobile payment methods do you currently accept? Q29: Of the following mobile payment methods, please rank the level of fraud risk you associate with each method from least risky to most risky

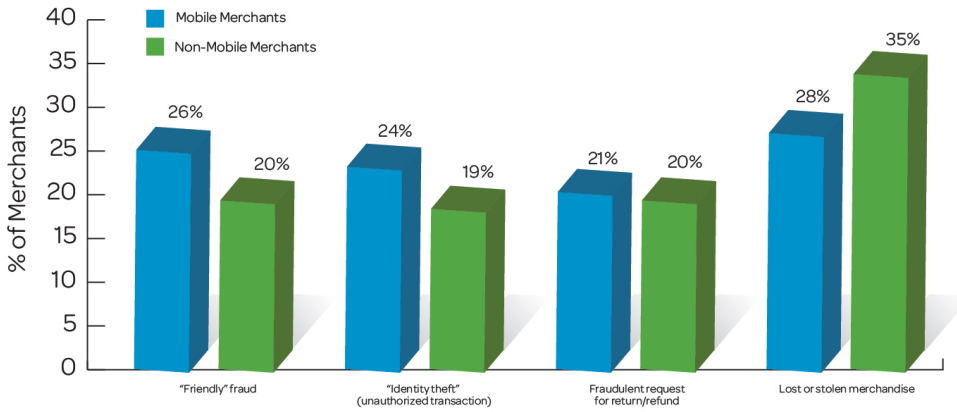
July 2012, n = 118
Base: Mobile Merchants

"... With mobile and tablet, you have to actually put an application on the customer's device. With a PC, you would never do that; they just [click on] the URL. [I] don't put anything on my machine ... but with mobile/tablet, that's exactly what you do, and as a result, it allows you to do things differently and potentially better than [the] security you [are] provided on a PC."

–FI executive

Mobile Merchants at Increased Risk for "Friendly" Fraud

Figure 17.Fraud Type by Mobile and Non-Mobile Merchants



**Unweighted segment data*

Q16: 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:

July 2012, n = 118, 912
Base: Mobile-accepting merchants, non-mobile-accepting merchants

Mobile-accepting merchants have a higher percentage of fraud losses in total revenue than nonmobile-accepting do. In particular, their rates of friendly fraud and identity theft are higher. Friendly fraud may be emerging as a key fraud type for the mobile channel; 1 in 5 mobile-accepting and less than 1 in 10 nonmobile-accepting merchant indicates that friendly fraud has increased in the past year. Although it is impossible to definitively attribute responsibility to device sharing, mobile-accepting merchants should remain on guard for that possibility.

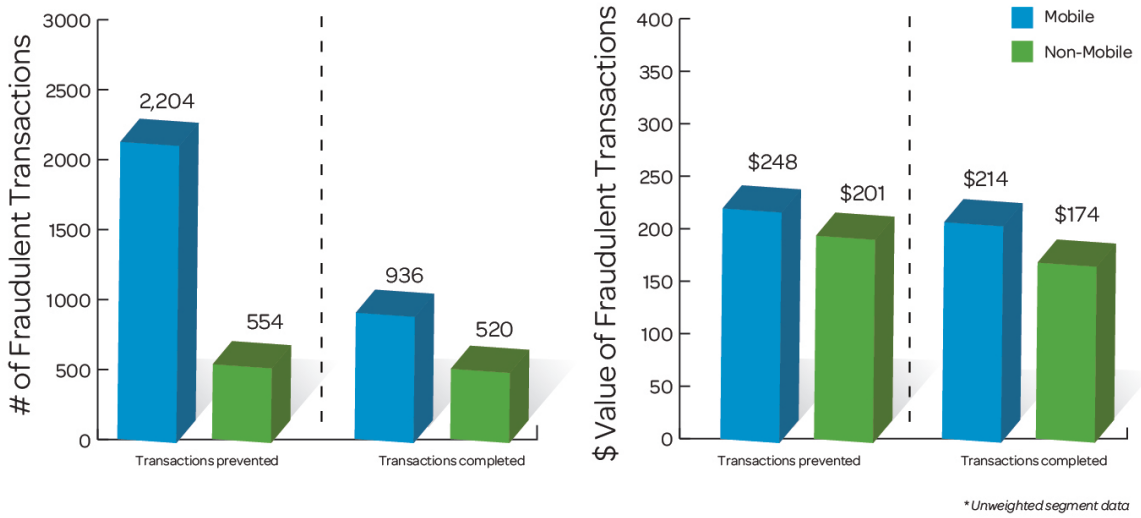
"I think the mobile arena is what's going to bring us the 'what's new' next. If you look at what we're seeing now—everybody introducing wallets, you have Visa, you have seen MasterCard making announcements, everybody from the issuer level, the overall bank community beginning to issue their respective wallets—I think that will create the critical mass for account takeover scenarios there in the future. Mobile will represent a sufficient asset to make them now appealing to the bad guys."

–Executive at a large issuer and acquirer

In 2011, mobile-accepting merchants prevented almost 2.5 times as many fraudulent transactions as were successfully completed at their company, whereas nonmobile-accepting merchants prevented less than 10% more fraudulent transactions than were completed (see Figure 18). Although both mobile and nonmobile-accepting merchants estimate that they prevent more fraudulent transactions than are successfully completed, mobile-accepting merchants report a higher value of both prevented and successful fraudulent transactions than do nonmobile-accepting merchants. This finding suggests that mobile-accepting merchants are more sophisticated at fraud mitigation, even if more criminals still eventually succeed with them.

Mobile Merchants Prevent a Far Higher Number of Fraudulent Transactions than are Successfully Completed Against Them

Figure 18. Prevented and Successful Fraudulent Transactions Against Mobile and Non-Mobile Merchants



** Unweighted segment data*

Q20: In a typical month, approximately how many fraudulent transactions are successfully completed at your company? Q21: Thinking of the fraudulent transactions that are prevented, what is the average value of such a transaction? Q22: In a typical month, approximately how many fraudulent transactions are successfully completed at your company? Q23: Thinking of the fraudulent transactions that are successfully completed, what is the average value of such a transaction?

July 2011, n = 118, 912
Base: Mobile merchants, non-mobile merchants

Merchants that include mobile among their acceptance channels have a dramatically different pattern of fraud types and must therefore adapt accordingly. It is likely that the significant differences in fraud types are largely explained by the types of merchants that venture into mobile channels in these early days of m-commerce rather than by mobile-specific transactional threats. Yet as merchants' acceptance of actual mobile payments grows, merchants must monitor such threats to assess their loss patterns among similar merchants.

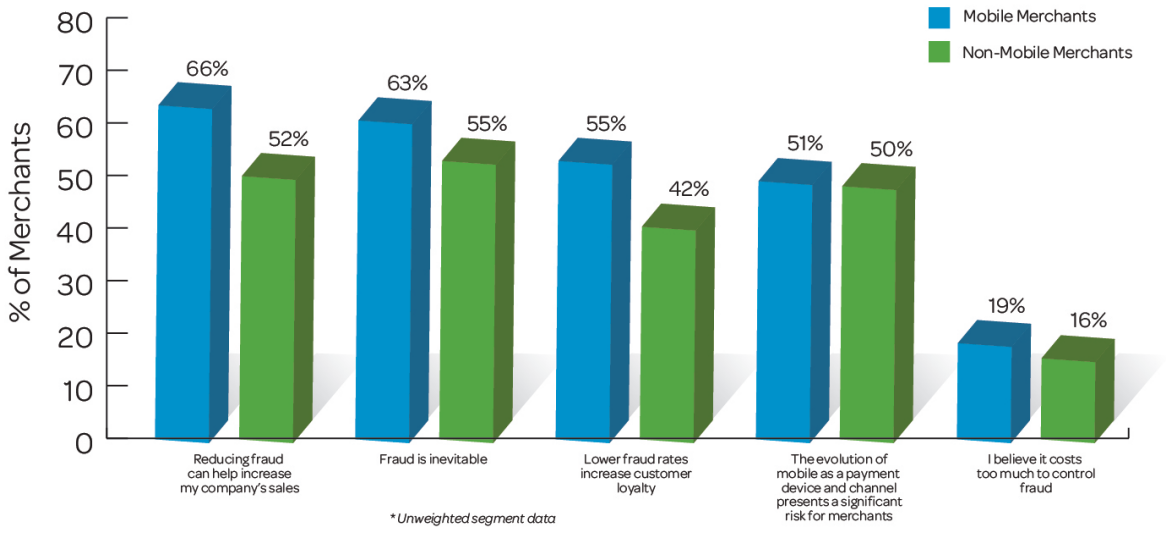
Mobile-accepting merchants are likely to see fraud as an issue of revenue and customer retention

Mobile-accepting merchants are more likely than merchants without mobile capabilities to see fraud prevention as an opportunity to increase revenue and retain customers. Although they are also more likely to take a fatalistic outlook toward fraud (63% agree that fraud is inevitable vs. 55% of nonmobile-accepting merchants), mobile-accepting merchants are more likely to believe that lower fraud rates will increase customer loyalty (55% vs. 42%) and to agree that reducing fraud will help to increase sales (66% vs. 52%). See Figure 19.

Thus, just as many mobile-accepting merchants have adopted the channel in an effort to meet customers' expectations, mobile-accepting merchants may be better than their nonmobile counterparts at recognizing customers' needs and managing relationships.

Mobile Merchants More Likely to Tie Fraud Prevention to Sales and Customer Loyalty

Figure 19. Merchant Attitudes Toward Fraud by Mobile and Non-Mobile Merchants



Q35: Please indicate the extent to which you agree or disagree with each statement listed below:

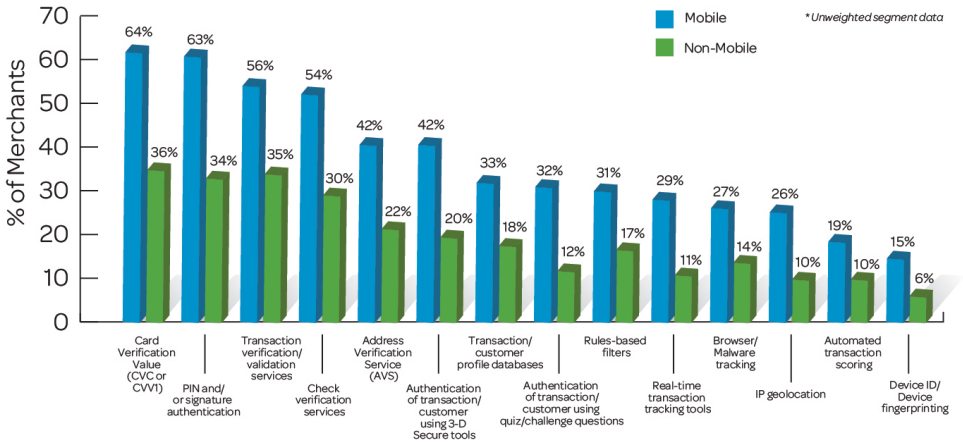
July 2012, n = 118, 912
Base: Mobile merchants, non-mobile merchants

Consistent with their perceptions that fraud will affect both revenue and customer loyalty, mobile-accepting merchants are significantly more likely than nonmobile-accepting merchants to use multiple fraud solutions.

Asked to name the top three factors that could help their company control fraud, mobile-accepting merchants were more likely than nonmobile-accepting merchants to list implementing fraud technology solutions as number one (9% vs. 4%). Figure 20 shows the methods that the two groups use.

Mobile Merchants More Likely to Use Anti-Fraud Solutions Across the Board

Figure 20. Current Users of Anti-Fraud Solution



CQ30: Which of the following best describes your awareness and use of the fraud solutions listed below: Current Users

July 2012, n = 118, 912
Base: Mobile merchants, non-mobile merchants

"[The top factor that could help my company prevent fraud is to] be aware of new technology which can be adapted to prevent fraud."

– IT director at a computers/electronics/ software retailer

"...Confirming customers are logged into their own accounts."

–Partner at a social networking enterprise

III. Spotlight: Large eCommerce merchants

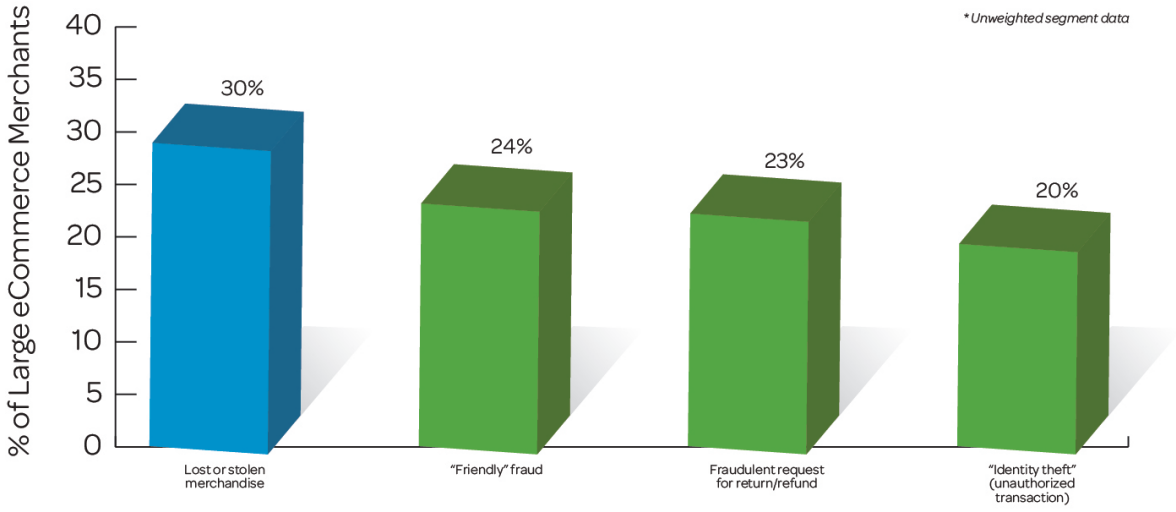
Large eCommerce merchants' fraud multiplier reverted to 2010 level

After large eCommerce merchants' Fraud Multiplier dipped last year, this measurement rose again to its 2010 level. Given the dynamic trends in merchant fraud over the past few years (which are closely correlated to retail spend and economic health), this fluctuation is unsurprising—but now this rise must be viewed as a renewed call to action.

Large eCommerce merchants continue to incur a lower-than-average fraud multiplier this year (2.5), likely because their rates of lost and stolen merchandise as a percentage of fraud losses are lower than those of all merchants. However, large eCommerce merchants' rates of friendly fraud, identity theft and fraudulent requests for return are higher than those for merchants overall. The fraud types large eCommerce merchants tend to suffer disproportionately often occur as CNP transactions, to which online merchants are particularly vulnerable. See Figure 21.

Friendly Fraud, Identity Theft and Fraudulent Requests Higher Among Large eCommerce Merchants Than All Merchants

Figure 21. Fraud Types by Large eCommerce Merchants



Q16: 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.

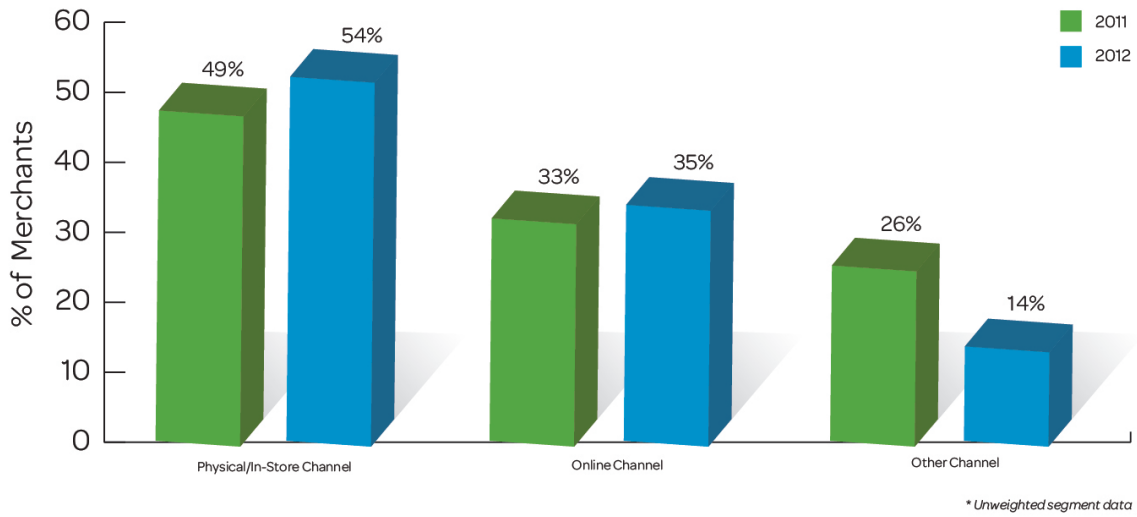
July 2012, n =183
Base: large eCommerce merchants

Large eCommerce merchants struggling with in-store channels

Large eCommerce merchants report a greater percentage of fraud through online channels than total merchants overall. However, despite the online component of their sales presence, in-person fraud still constitutes the majority of fraud for this segment and has actually increased since last year, accounting for 54% of fraudulent transactions compared with 49% last year. See Figure 22.

Physical/In-Store Fraud Increasing Among Large eCommerce Merchants

Figure 22. 2011 and 2012 Fraud Losses by Fraud Channel



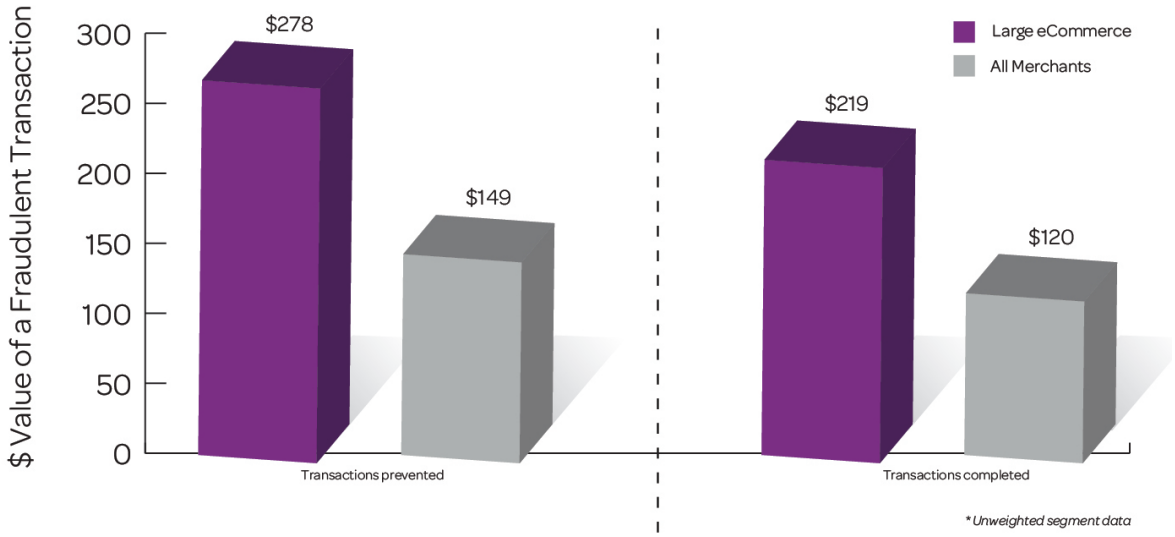
Q19: Thinking about the total fraud losses suffered by your company in the past 12 months, to the best of your knowledge, what is the percentage distribution of fraud over the following sales channels?

July 2011, July 2012, n = 163, 183
Base: large eCommerce merchants

On average, large eCommerce merchants are suffering higher average per-fraudulent transaction amounts than are all merchants ($219 vs. $120 for a completed fraudulent transaction). However, both merchant segments still achieve relative success in preventing fraud involving higher-ticket-value transactions. See Figure 23.

Large eCommerce Suffers From Higher Value of Fraudulent Transactions

Figure 23. Prevented and Successful Fraudulent Transactions Against Large eCommerce Merchants



Q21: Thinking of the fraudulent transactions that are prevented, what is the average value of such a transaction?
Q23: Thinking of the fraudulent transactions that are successfully completed, what is the average value of such a transaction?

July 2012, n = 1030, 183
Base: All merchants, large eCommerce merchants

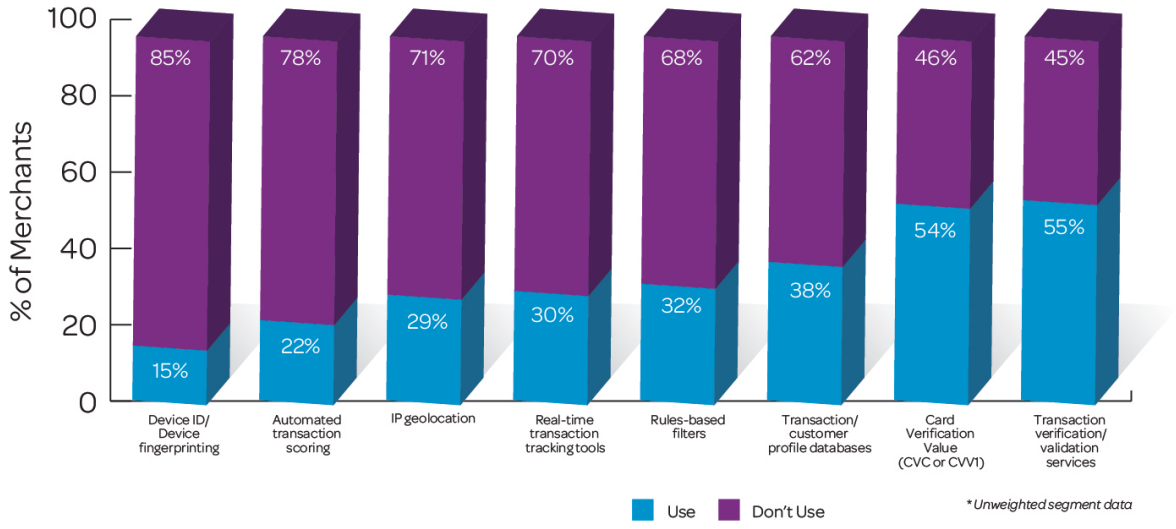
Large eCommerce merchants are also more likely than all merchants to have seen an increase in friendly fraud (19% vs. 5%), ID theft (38% vs. 8%), fraudulent request for return (30% vs. 10%) and lost/stolen merchandise (26% vs. 12%).

Large eCommerce merchants can still improve in adoption of antifraud solutions

Continuing a trend from 2011, large eCommerce merchants adopt the most antifraud solutions across the board (see Figure 24). However, they still lag in adoption of several solutions, such as device fingerprinting, IP geolocation, automated transaction scoring and real-time transaction-tracking tools. Large merchants must benchmark their success on both fraud incidence rates and average ticket amount.

Large eCommerce Still Has Room to Improve in Adoption of Several Anti-Fraud Solutions

Figure 24. Use of Anti-Fraud Solutions by Large eCommerce Merchants



Q30: Which of the following best describes your awareness and use of the fraud solutions listed below. Other response options available.

July 2012, n = 183
Base: large eCommerce merchants

Several of these tools are particularly useful when they are applied to the mobile channel, a payment channel growing quickly among large eCommerce merchants (23% of large eCommerce merchants accept mobile payments, compared with only 6% of all merchants).

Forty-three percent of large eCommerce merchants indicate that the evolution of mobile payments will impact their overall business strategy, compared with only 11% of all merchants. In particular, large eCommerce merchants believed that they would need to adapt their strategy to meet customers' demands and expectations (22% vs. 19% for all merchants). As these merchants adapt to an increasing volume of mobile payments, they would do best to tailor their antifraud strategies to cover this channel as well.

Despite the undeniable long-term growth of fraud among online merchants, adoption of solutions still has the markers of an immature market. Consumers increasingly take their own unique devices to make purchases, yet fingerprinting of the devices is rarely used. Transaction scoring and IP geolocation (which may require network changes) are still nascent, and the rarity of real-time tracking tools makes it difficult to stop rapid criminal purchases. Despite the pattern of shipment to known criminal or nonexistent addresses, many merchants are not equipped to identify this. And, surprisingly, CVV solutions are still not pervasive.

IV. Spotlight: International merchants

International commerce shows signs of future problems

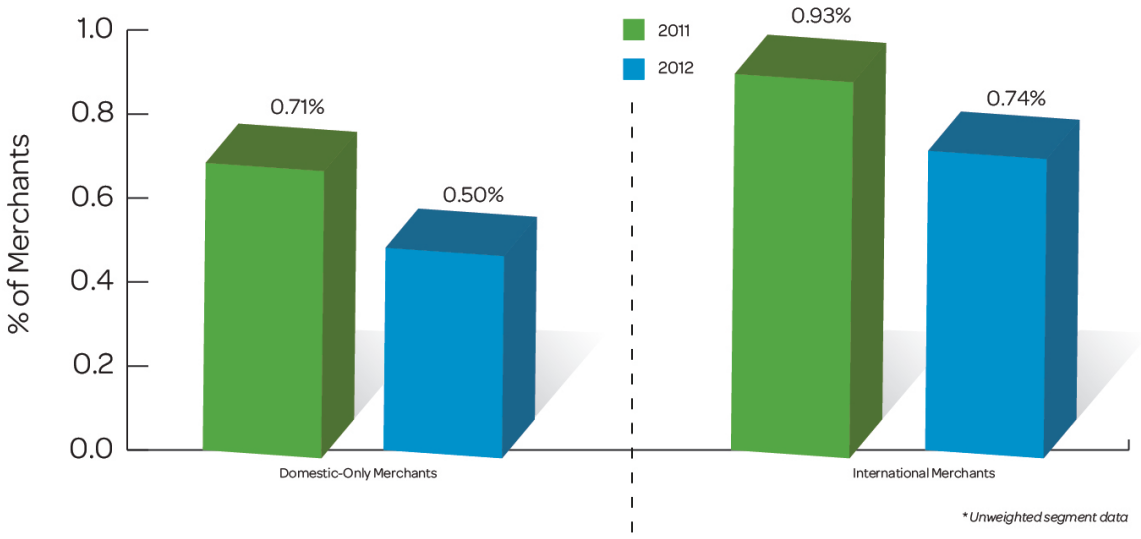
This study finds an increasing cost to merchants from fraudulent transactions in their international activities. The Fraud Multiplier among international merchants has risen from 2.2 to 2.5 since last year, an increase of almost 14% per dollar of fraud. This increase echoes verbal comments made by industry executives who also report the payoff of much more stringent policies in global transactions.

Fraud losses have decreased as a percentage of revenue for both international and domestic-only merchants, although losses reported by international merchants are nearly 25 points higher than those reported by domestic-only merchants (see Figure 25). Fraud losses have decreased at a greater percentage for domestic merchants, however (30% vs. 20% for international merchants). Note that these two trends are not contradictory; one reflects the true cost of fraud (overall financial impact), whereas the other reflects the primary amount of the fraudulent transactions themselves.

Banking leaders interviewed for this study touted methods applicable to dealing with the increased risk of fraud for international merchants, including a dramatic payoff in routinely blocking particular transactions based on the highest-risk profiles of both country and merchant category. FI fraud executives also underscored the need to efficiently conduct detailed analysis in a way that that leads to rapid adjustment following sudden shifts in criminal tactics.

Fraud Losses Falling for International and Domestic-Only Merchants Alike

Figure 25. 2011 and 2012 Fraud as a Percent of Revenue by International and Domestic-Only Merchants



Q14: What is the approximate dollar value of your company's total fraud losses over the past 12 months?

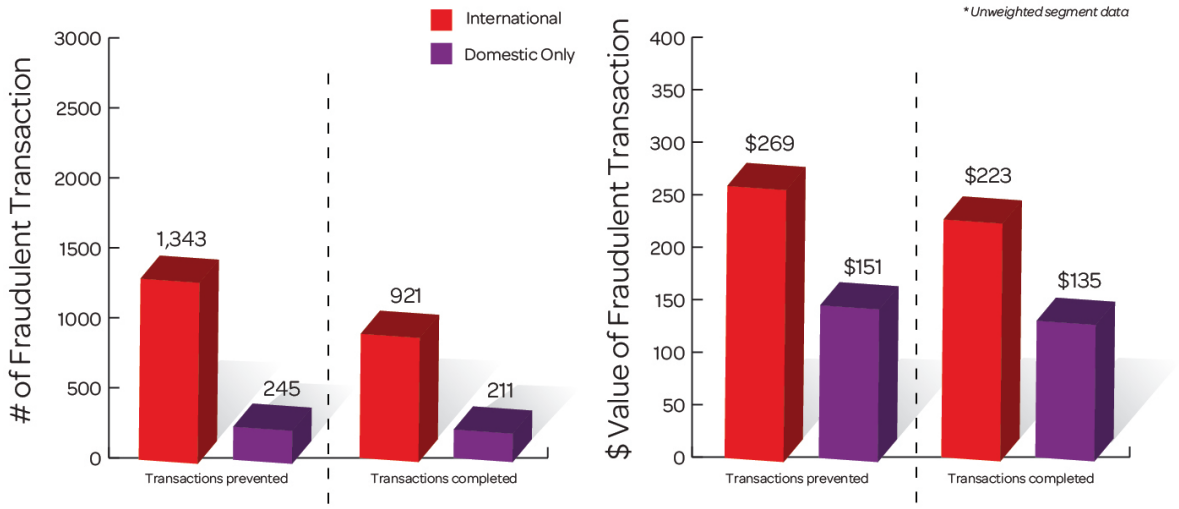
July 2011, July 2012 n = varies 467 to 563
Base: International Merchants, Domestic-Only Merchants

FI executives also cite wire transfer fraud and balance transfer fraud as areas of growth in international fraud. The shift to these channels may be a result of increasing controls on payments methods typically involved in CNP transactions.

International merchants also both prevent and fall victim to a higher number and higher value of fraudulent transactions per month than do domestic-only merchants. See Figure 26.

International Merchants Victim to More Successful Fraudulent Transactions at Higher Ticket Value Than Domestic-Only Merchants

Figure 26. Prevented and Successful Fraudulent Transactions Against Domestic-Only and International Merchants



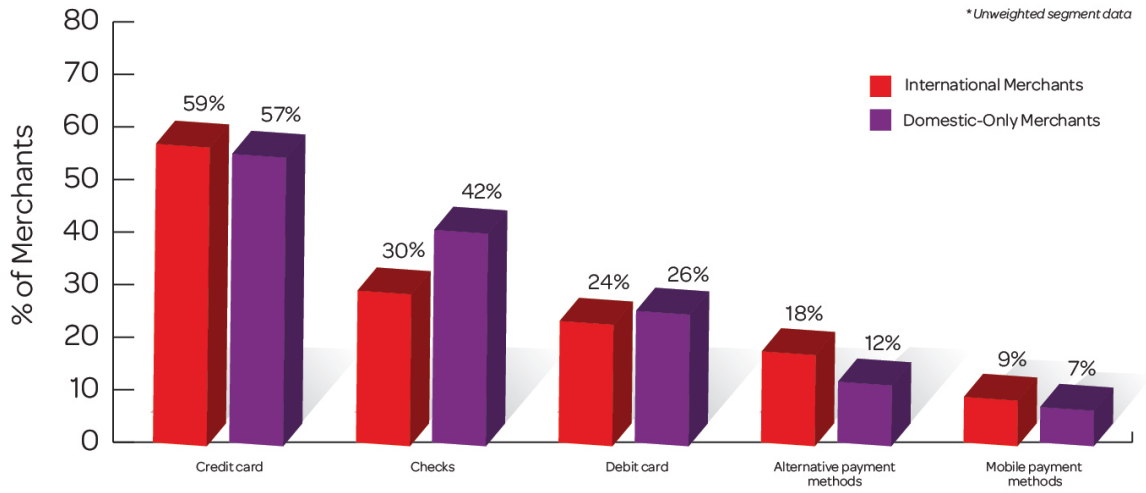
Q20: In a typical month, approximately how many fraudulent transactions are successfully completed at your company? Q21: Thinking of the fraudulent transactions that are prevented, what is the average value of such a transaction? Q22: In a typical month, approximately how many fraudulent transactions are successfully completed at your company? Q23: Thinking of the fraudulent transactions that are successfully completed, what is the average value of such a transaction?

July 2012, n = 467, 563
Base: International Merchants, Domestic-Only Merchants

International merchants are more likely than domestic merchants to see a higher percentage of fraudulent transactions occurring through the channels typically associated with CNP fraud. In particular, rates of credit card, alternative payments and mobile payments fraud are higher for international merchants than for domestic-only merchants, and rates of check fraud are lower. See Figure 27.

International Merchants See More Fraud Through Methods Typically Associated with CNP Fraud

Figure 27. Fraud Distribution Across Payment Methods for International and Domestic-Only Merchants, 2012



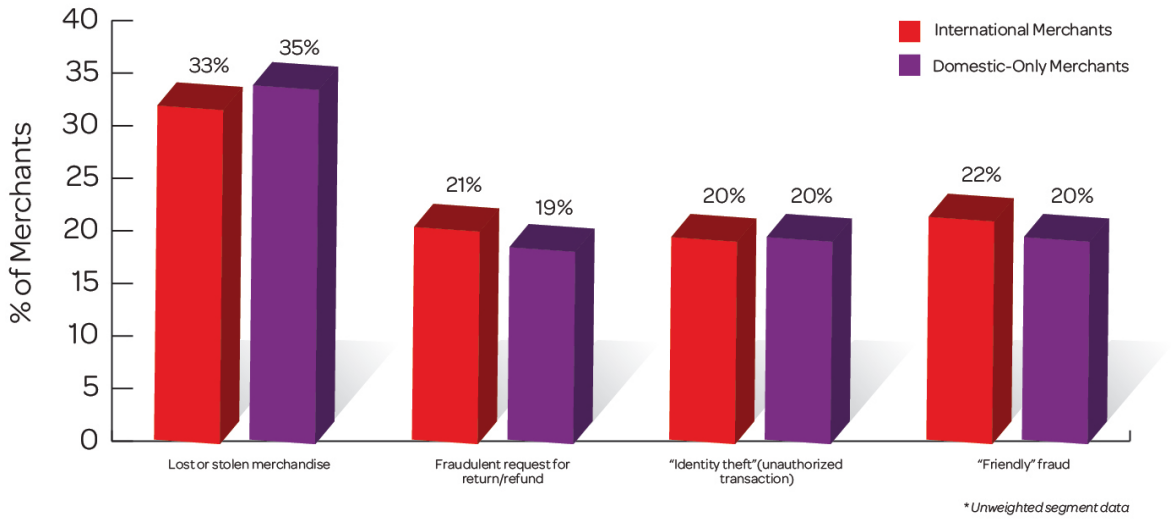
Q25: In thinking about which payment methods are most commonly linked to fraudulent transactions, please indicate the percentage distribution, to the best of your knowledge, of the payment methods used to commit fraud against your company:

July 2012, n = 467, 563
Base: International merchants, domestic-only merchants

An increase in identity theft over the past 12 months is more likely at international merchants than at domestic-only merchants (27% vs. 14%). Nonetheless, international merchants are reporting a profile of the breakdown of fraud losses that is very similar to that of domestic-only merchants. The fraud patterns naturally reflect the predominant tender types that are used by global purchasers. Because both merchant and FI fraud-mitigation specialists reported in interviews that it is increasingly difficult to prevent and follow up on fraud losses, it is clear that companies cannot afford to take a casual approach to global purchases through any payment method or channel. See Figure 28.

Friendly Fraud, Fraudulent Request for Return a Greater Problem for International Merchants

Figure 28. Fraud Types at International and Domestic-Only Merchants, 2012

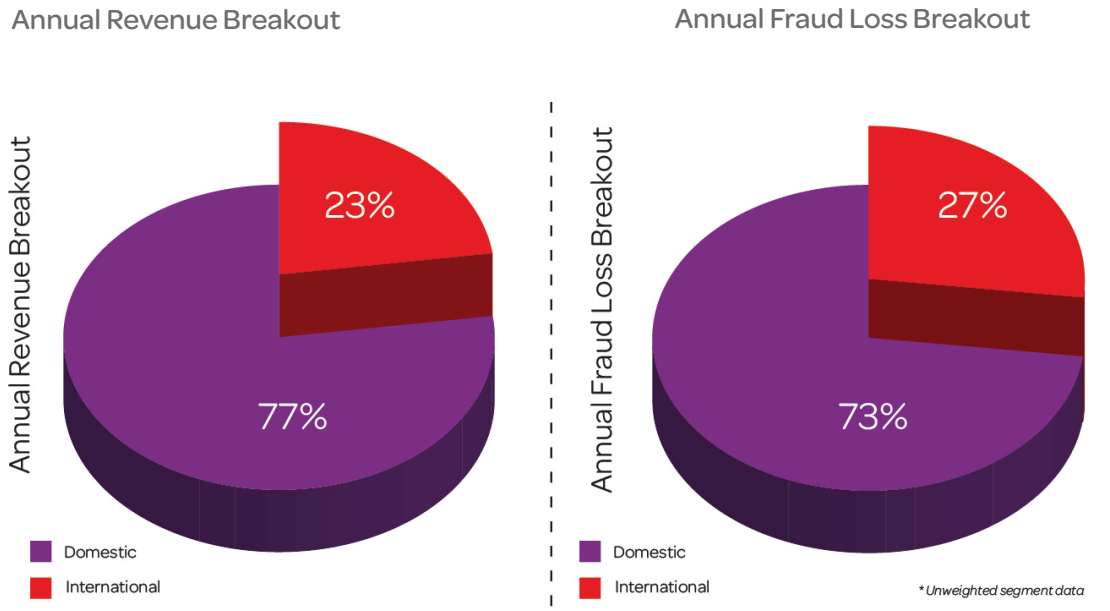


Q16: Please indicate, to the best of your knowledge, the percentage distribution of the following fraud methods below, as they are attributed to your total annual fraud loss over the past 12 months:

July 2012, n = 467, 563
Base: International merchants, domestic-only merchants

Despite international merchants' lower-than-average Fraud Multiplier (2.5 vs. 2.7 for all merchants), this group loses a higher percentage of revenue to fraud than do domestic-only merchants, and loss to international fraud is disproportionate to the amount of revenue merchants generate from international sales. This finding is consistent with one FI executive's claim that foreign transactions on a card are six times as likely to be fraud. See Figure 29.

Figure 29. 2012 International Merchants Snapshot



Q12: Does your company currently sell merchandise to customers outside of the domestic US? Q13: Please indicate the percent of annual revenue generated through domestic compared to international sales in the last 12 months.

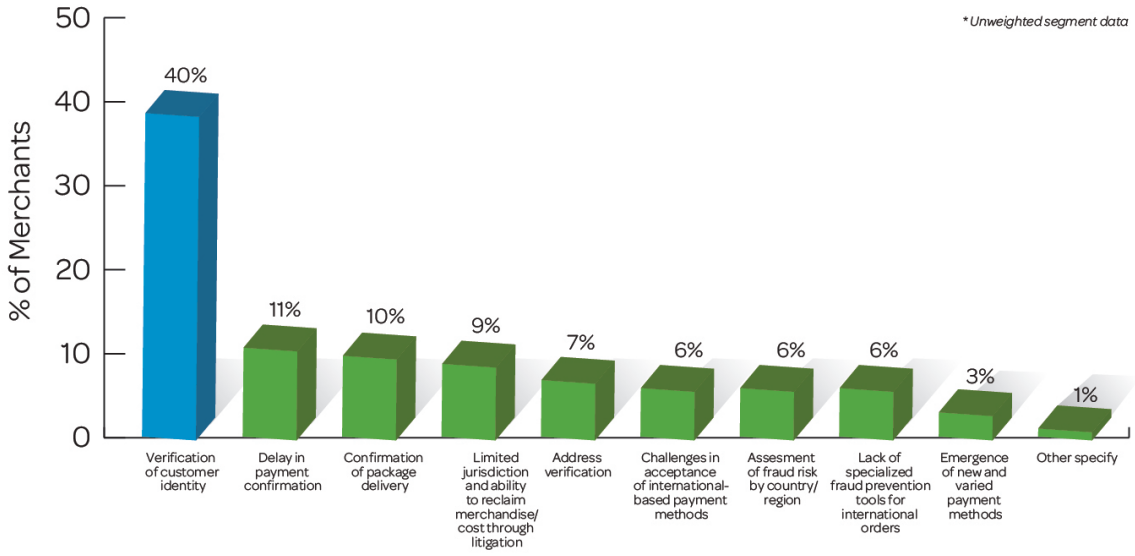
July 2012, n = 467
Base: International Merchants

International merchants struggle to verify customers' identities

Consistent with international merchants' reported increase in identity fraud in the past 12 months, verifying customers' identities emerges as a key concern; two-fifths of them name it as the number one challenge they face when selling internationally. See Figure 30.

Two in Five International Merchants Most Concerned with ID Verification

Figure 30. Top Concerns When Selling Internationally for International Merchants



Q18: Please rank the top 3 challenges related to fraud faced by your company when selling merchandise to customers outside the U.S.

July 2012, n = 467
Base: International merchants

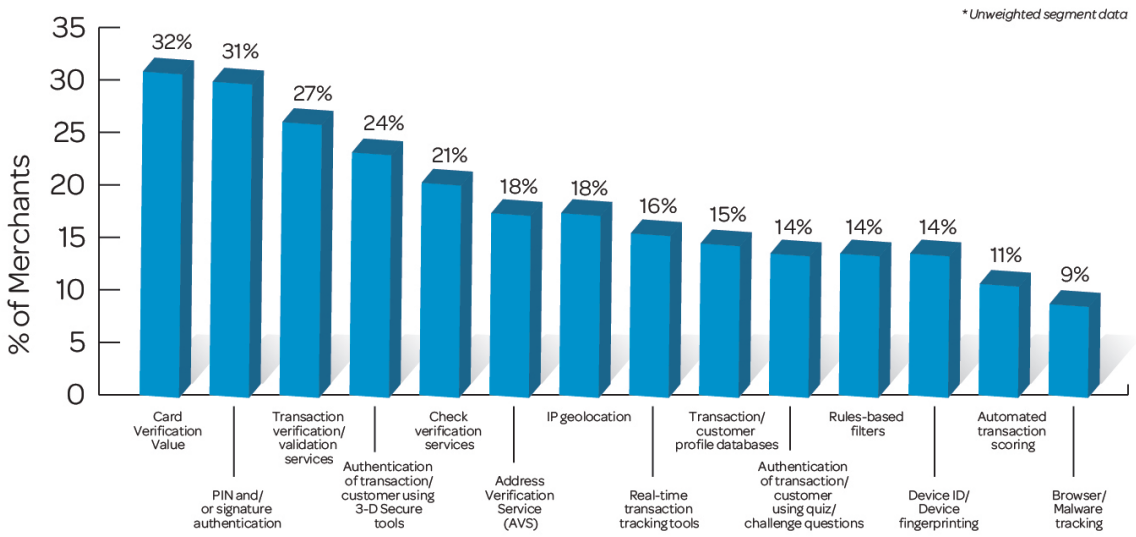
International merchants are more likely than domestic-only merchants to use all types of fraud solutions, probably because they tend to be larger enterprises that must allocate more resources to prevent a variety of fraud methods. Yet despite high rates of use of a wide variety of fraud solutions, international merchants still could be undervaluing several solutions that could help them prevent identity theft.

In particular, IP geolocation and device fingerprinting stand out as underutilized tools for international merchants who see higher rates of fraud through remote payments channels. International address verification and customer profile databases also have great potential to prevent international fraud.

On an unaided basis, global fraud lists and international address verification were listed by international merchants as some of the top fraud solutions. During FI interviews, one issuer also noted that global fraud dropped dramatically when 3-D secure was mandated for particular high-risk international merchant categories. See Figure 31.

International Merchants Rank Card Verification Values and PIN/Signature Authentication as Most Effective in Controlling International Fraud (Aided List From Survey)

Figure 31. Tools Most Effective in Controlling International Fraud



CQ33c: 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

July 2012, n = 467
Base: International Merchants

V. Conclusions and recommendations

The dynamic nature of fraud requires that merchants compare themselves closely with their peers on the basis of size, market channel and more. Because the size and pattern of fraud are significantly impacted by economic conditions, this turbulent time requires merchants to be more vigilant than ever. Merchants often have no choice but to seek global or mobile markets for growth, yet this study shows that an "eyes-open" approach to preparing for the worst (as fraud fatalists do) is likely to predict success against persistent and inventive criminals. Even though increased technology solutions are also vital (and this study identifies several key protective methods that are surprisingly low in adoption), merchants must realize that customer relationships are just as important. Consumer research clearly indicates that customers vote with their feet after fraud, but a surprising majority of merchants surveyed in this study are not aware of this costly after-effect of fraud.

This study's recommendations include:

- Make fraud protection a higher priority. As merchants increasingly do business online, over mobile devices and around the world, they must take advantage of the many solutions available to aid in a battle that will become increasingly pitched and complex. Expect the worst to achieve the best, and use this study to benchmark levels of fraud and implementation of solutions.
- Improve overall profits by allocating more resources to retaining or even attracting customers who have been defrauded. Shoppers are often obsessed with their safety (and in particular, when shopping online), and they increasingly even want to play a role in their own self-protection. Productive engagement requires careful implementation of solutions, education and partnerships.
- Fully train and equip all staff members with the strongest possible policies and technologies. Because large merchants are the subject of higher-value fraudulent transactions, they must ensure that they are prepared to fight fraud at every level .

In short, expect the worst while becoming the best, through a multi-pronged strategy that includes the latest protective measures, customer-engaged communication or solutions and increased prioritization of specific solutions as you grow larger, more mobile and more global.

VI. Methodology

In May 2012, 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 1,030 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 +/- 3.05 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 2012, 2011 and 2010, data was weighted according to the U.S. Census by both employee size and industry distribution. In 2009, totals were weighted only by employee size and used much broader employee size categories than those used in 2010.

Industry was weighted by the following classifications: automotive, housewares, computers, hardware, restaurants, drug/health, gasoline stations, textiles, sporting goods, general merchandise stores, nonstore 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 2012 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-caclculated 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.

2011 Javelin Identity Fraud Survey

The Javelin Identity Fraud Survey Report on a survey conducted in 2011 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 2012 ID Fraud survey was conducted among 5,022 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 Oct. 6, 2011, and ended Oct. 20, 2011. 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 September 2011 CPS and household internet access from October 2010 CPS Supplement.

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 5,022 respondents, the maximum margin of sampling error is +/1.7% at the 95% confidence level. For questions answered by all 818 identity fraud victims, the maximum margin of sampling error is +/3.4% at the 95% confidence level.

Sources

[1] 13 Identity Fraud Survey, subset of 58 out of 5,211 consumers, October 2011.

[2] 2012-2017: Retail Point Of Sale Forecast: Cash is No Longer King; Cards and Mobile Payments Likely to Rise, Javelin Strategy & Research, June 2012.

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

For more information

Call 866.818.0265, visit lexisnexis.com/risk/retail-ecommerce or email us at retailfraud@lexisnexis.com.

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

Our retail solutions assist organizations with protecting revenue, maximizing operational efficiencies, and predicting and preventing retail fraud.

LexisNexis®