Whitepaper

LexisNexis® 2011 True Cost of Fraud Study

Industry Progress in Fraud Mitigation, But Danger Looms in the E-Commerce Horizon

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, Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of 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 for automated scoring, identity management, workflow management and manual review assist organizations with protecting revenue, maximizing operational efficiencies, and predicting and preventing retail fraud.

About Javelin Strategy & Research

Javelin is a leading provider of nationally representative, quantitative research focused exclusively on financial services topics. Based on the most rigorous statistical methodologies, Javelin conducts in-depth primary research studies to pinpoint dynamic risks and opportunities.

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

Introduction

The 2011 LexisNexis True Cost of Fraud Study is the third annual landmark study conducted on the ways fraud affects U.S. consumers, financial institutions (FIs), and merchants. 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 how fraud may impact the effectiveness of these channels. Because retail merchants today are suffering exorbitant costs related to 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.

Fraud Definition

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

- Fraudulent and/or unauthorized transactions
- Fraudulent requests for 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 insider fraud or employee fraud.

Merchant Definitions

- Small merchants earn less than $1 million in annual sales
- Midsize merchants earn between $1 million and less than $50 million in annual revenue
- Large merchants earn $50 million or more in annual sales or have 1,000 or more employees.
- Mobile merchants accept payments through various mobile phones
- International merchants sell merchandise outside the U.S.
- Domestic-only merchants do not sell merchandise outside the U.S.
- Large e-commerce merchants accept payments through multiple channels but maintain a strong online presence, earning 10% to 100% of their revenue from the online channel and earn $50 million or more in annual sales

Overview

The 2011 LexisNexis study aims to help merchants grow their business safely even as signs in the industry point to a growing risk of fraud. This whitepaper provides snapshots of current fraud trends in the United States and spotlights key pain points merchants should be aware of as they add new payment mechanisms and expand channels into online, mobile, and international. It aims to answer a question critical to the entire merchant community: How do you grow your business safely?

New to 2011 is a deep dive into U.S. merchants selling merchandise outside the U.S. (i.e., a look at the international merchant segment).

Key Takeaways in 2011

- Small merchants show increased interest in adoption of alternative and mobile payments; they also seem most vulnerable and least equipped to handle the threats posed by these emerging channels.
- Large e-commerce merchants and mobile merchants continue to combat a high influx of fraudulent transactions, which tend to also be large in dollar amount.
- A spotlight on merchants with an international presence reveals their lack of control in international arenas and their vulnerability to ID theft and friendly fraud.
- The LexisNexis fraud multiplier declined from being just over $3 in 2010 to $2.33 this year. On average, merchants report they are paying less per dollar of fraud than they were in 2010. However, this decline in the fraud multiplier is not universal — small merchants and certain industries continue to report higher out-of-pocket costs, similar to last year.
- Continuing the downward trend from last year, total merchant fraud losses declined year over year but they continue to be a $100+ billion problem.
- Overall, fraud rates could be poised for an upswing. From the merchant's perspective, although the number of fraudulent transactions went down this year, the nature of transactions is trending to be more severe — the average dollar value of a completed fraudulent transaction is higher this year than what was reported last year.
- 2011 began with some of the largest recorded data breaches in history. Information leaks compromised more than 180 million records, providing fraudsters with a wealth of information through which they can attempt attacks against unsuspecting victims.[1]
- Financial institutions warn of the sophisticated and innovative evolution of fraudster trends that will challenge existing systems.
- Businesses run the risk of growing complacent with a false sense of safety. Merchants report significantly higher levels of satisfaction with existing online fraud detection tools over last year, even though higher-dollar-value fraudulent transactions are seeping through this year. They also report lowered use of these tools overall.
- Risk and fraud executives in the merchant community are calling for greater investment in fraud mitigation technology as well as education on industry standards and best practices.

[1] **2011 Second Annual Antivirus, Browser, and Mobile Security Report.** Javelin Strategy & Research, July 2011.

Conclusions & Recommendations

Fraud Will Likely Increase; Merchants Can Grow Safely with Reduced Risks If They Stay Vigilant

- While the entire industry has made significant strides in reducing fraud;, the current decline in fraud should not be interpreted by merchants to mean "all is OK." Nor should merchants be less vigilant vis-à-vis their anti-fraud and risk mitigation efforts.
- Merchants should take advantage of this lull to stay on top of and improve their security programs in every market, especially as fraudsters become more sophisticated in their security attacks.
- Merchants need to identify specific areas of their businesses that are at risk and use the appropriate fraud prevention, detection, and resolution models, techniques, and tools.
- The most lucrative areas of growth — international, mobile, and e-commerce — also represent high-risk areas for fraud; expansion must be supplemented by additional protection.
- Merchants have an opportunity to build a better relationship with their customers by enhancing their security measures and remaining competitive with other businesses.

5 Steps to a Safe Expansion:

1. Make strategic investments in fraud-prevention tools and technologies to ensure a safe growth into new markets
2. Develop "secure" processes for international transactions by working closely with your issuer or acquirer
3. Ensure your fraud strategy includes solutions that can address the specific risks facing international and mobile orders
4. Develop joint "antifraud" programs with your issuer or acquirer to increase your effectiveness
5. Educate both your employees and consumers about fraud prevention

I. The Lull: Drop in Fraud

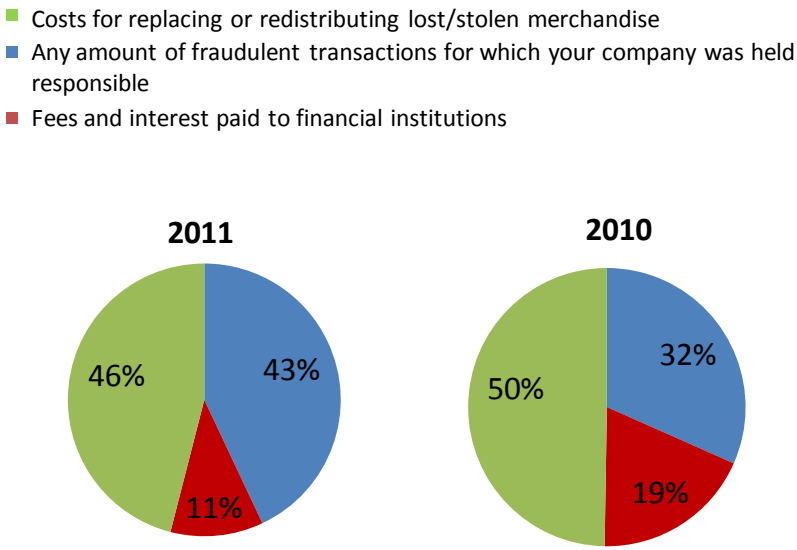
True Cost of Fraud to Merchants – The Fraud Multiplier

U.S. retailers received good news this year. Retail sales actually rose while total reports of fraud declined across the industry. The decline in fraud rates is reported by all players in the industry: consumers, FIs, and merchants.

There is a decline in the LexisNexis "fraud multiplier," which calculates the "true" costs shouldered by merchants. This year merchants report they are paying $2.33 for every $1 lost in fraudulent transactions, signifying a decline from just over $3 in 2010.

The fraud multiplier calculates dollars lost by merchants in paying interest/fees to financial institutions (FIs) and replacing/redistributing merchandise vs. every dollar lost in fraudulent transactions (e.g., for every $1 in chargebacks merchants were also experiencing an additional $2.33 cost from fees/interest and replacement/redistribution costs). The overall drop in the 2011 fraud multiplier correlates with a rise in proportion of fraud losses attributed to any amount of fraudulent transactions for which the merchant was held responsible and a simultaneous drop in fraud losses attributed to cost for replacing or redistributing lost/stolen merchandise and interest/fees paid to FIs (See Figure 1 below). In 2011, merchants attribute 43% of their total fraud losses to fraudulent transactions and 46% to lost/stolen goods. With this shift, merchants are now reporting fraud losses almost equally split over any amount of fraudulent transactions for which their company was held responsible vs. costs for replacing or redistributing lost/stolen goods.

Figure 1: Total Merchant Fraud Losses Broken Out Over Responsibilities/Payments, 2010–2011



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.

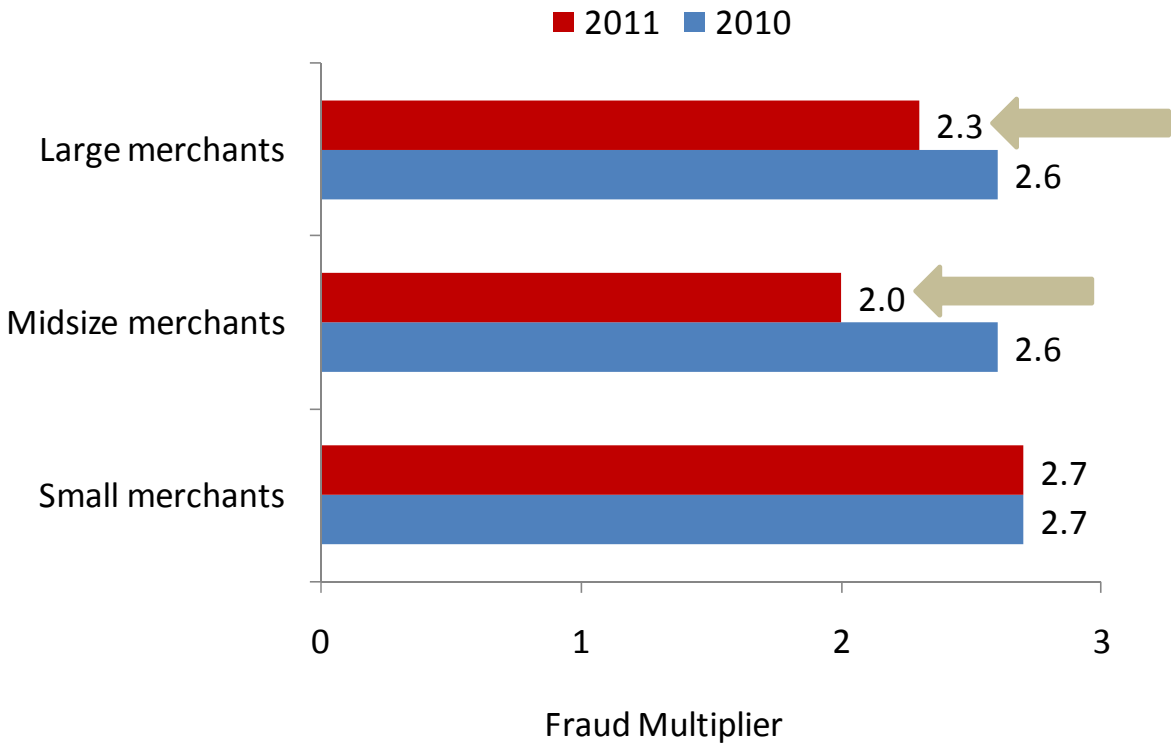
July 2011, n=455; July 2010, n=712
*Base= Merchants willing to provide breakdown (n=78)

Insight

This year the Lexis Nexis Cost of Fraud Study further probes the category of replacing/redistributing goods to reveal that on average, the majority (~70%) of costs are attributed to replacement of lost or stolen merchandise, while ~30% are attributed to redistributing goods.*

However, the story of true "costs" to merchants remains incomplete without delving into an important sublayer of findings. Not all merchant communities report a drop in the fraud multiplier. This drop is largely driven by reports from midsize to large merchants. Smaller merchants remain stable in comparison. In other words, small merchants continue to attribute a high proportion of fraud losses to costs of replacing/redistributing goods vs. chargebacks (53% of fraud losses vs. 37% of chargebacks, respectively), leading to a higher fraud multiplier. In contrast, midsize to large merchants report the opposite (i.e., 37% attributed to replacing/redistributing lost or stolen goods and 44%–50% attributed to chargebacks).

Figure 2: Merchant Fraud Multiplier – by Merchant Segments, 2010–2011



Key behaviors reported by midsize to large merchants reveal trends that highlight their vulnerability to chargebacks:

- These merchants attribute a relatively higher proportion of fraud to ID fraud (unauthorized transactions) than smaller businesses. (Smaller merchants attribute about 12% of fraud losses to ID fraud vs. larger merchants who attribute about 22%.)
- Just under 30% of these merchants report an increase in fraudulent use of credit cards since last year. In comparison, only 15% of small merchants report the same.
- The average dollar value of a completed fraudulent transaction is higher among the larger merchants than their smaller counterparts. This suggests that when a chargeback does occur, larger merchants are losing more dollars in impact
- Fifteen percent to 20% of this merchant community reports it currently does not participate in online authentication programs that are critical to battling chargebacks. Moreover, participation in most other fraud mitigation tools (both online and in-person) also remains varied, with anywhere from 13% to 70% of merchants reporting they currently don't participate in various fraud-prevention programs.

The bottom line: Midsize to large merchants are bearing higher proportions of fraud losses due to chargebacks and also paying an additional $2 for every dollar lost in fraud. Continued vigilance, compliance with industry best practices, and increased participation in fraud mitigation solutions will be critical for these segments moving forward.

Continuing the downward trend from last year, total merchant fraud losses declined but continue to top $100 billion (using yearly rolling averages). Overall, decreases in costs of fraud to merchants in 2011 may be traced to a reduced volume of fraud stemming from several factors:

- The reduction in data breaches in late 2009 and 2010 limiting the amount of personally identifiable information available to fraudsters, impacting the incidence of fraud overall in the industry (especially identity fraud)
- Higher numbers of fraudulent transactions were prevented than successfully completed in 2011 (119 prevented vs. 75 completed each month, on average)
- The average dollar value of prevented fraudulent transactions was higher than the average value of completed fraudulent transactions ($148 vs. $122)

Insight

Reflecting the varied undercurrents prevalent in the merchant community, FIs also express mixed opinions on trends around chargebacks. Some estimate that the dollars have gone up. But as a percentage of sales volume, they have flattened or dropped slightly. One FI executive contends chargebacks are, in fact, on the rise overall. Merchant training is viewed as a fundamental method of reducing chargebacks.

Insight

Consumers also report similar drops in fraud. According to the annual ID fraud survey conducted by Javelin Strategy & Research, approximately 8.1 million Americans, or 3.5% of the total U.S. population, were victims of identity fraud in 2010. Further, at $37 billion, the annual overall fraud amount reported by consumers was also at its lowest point since the survey began in 2003. It dropped significantly from $56 billion in 2009. This downward trend is further corroborated by FIs. In an interview, one executive said, "This last year [we saw] the sharpest one-year drop in identity fraud that we have ever seen in any year."

Cost of Fraud: Consumers and FIs

It is important to note that although overall fraud losses declined among consumers, in a sharp reversal of previous years, mean consumer out-of-pocket costs rose to $631 in 2010, up from $387 in 2009. The average time consumers take to resolve fraud issues also increased 57% this year to 33 hours, from 21 hours in 2009. In summary, customers were shouldering more costs than ever to resolve their fraud and are more severely impacted, although the number of fraud cases was down year over year.

Figure 3: Overall Measures of the Impact of Identity Fraud, 2003–2011[1]

	Survey Report								
	Trend	2010	2009	2008	2007	2006	2005	2004	2003
US adult victims of identity fraud	↑	8.1M	11.1M	9.9M	8.1M	8.4M	8.9M	9.3M	10.1M
Fraud victims as % of US population[2]	↑	3.5%	4.8%	4.3%	3.6%	3.7%	4.0%	4.3%	4.7%
Total one-year fraud amount[3]	↑	$37B	$56 B	$49 B	$48 B	$55 B	$65 B	$70 B	$59 B
Mean fraud amount per fraud victim	↑	$4,607	$4,991	$4,980	$5,865	$6,519	$7,021	$7,603	$5,796
Median fraud amount per fraud victim	=	$750	$750	$750	$750	$750	$750	$750	$750
Mean consumer cost	↓	$631	$387	$511	$767	$580	$472	$754	$606
Median consumer cost	=	$0	$0	$0	$0	$0	$0	$0	$0
Mean resolution time (hours)	↓	33	21	30	26	25	40	28	33
Median resolution time (hours)	↓	6	5	5	5	5	5	5	5

[1] Past years' dollar figures have been adjusted for inflation according to the Consumer Price Index (CPI-U) issued by the Bureau of Labor Statistics, ftp://ftp.bls.gov/pub/special.requests/cpi/cpiai.txt, accessed Nov. 22, 2010.
[2] Based on U.S. population estimates (age 18 and over), http://www.census.gov/popest/estimates.php, accessed.
[3] 2006, 2007, 2008 and 2009 dollar cost estimates have been smoothed through use of three-year averaging — refer to Methodology Section for details.

So why should the merchant community care about the increasing consumer burden? The answer lies in two major areas:

First, the increase in consumer costs reflects the difficulty in monitoring and detecting the types of fraud associated with consumers' preferred payment methods and purchasing behaviors – which is key to protecting your own business. To cite one instance, consumers reported they increasingly turned to debit cards to manage their cash flow in the current economic environment. Thus debit card fraud registered an increase (although credit cards continued to dominate). Debit card fraud takes longer to stop and resolve than credit card fraud, and debit cards have higher average consumer costs related to fraud than credit cards. These factors could influence consumers to switch payment methods and return to credit cards, particularly given the likely forthcoming reduction of debit rewards programs and encouragement by FIs to use credit cards, which will bring higher interchange to these institutions than most debit card products.[2]

Insight

Interchange is the fee paid between banks for the acceptance of a card-based transaction. Usually it is a fee that a merchant's bank (the "acquiring bank") pays the customer's bank (the "issuing bank"). Starting October 2011, new regulations (i.e., the Durbin Amendment) will limit the amount of debit card fees that retailers must pay, fees that will then be absorbed by consumers instead.

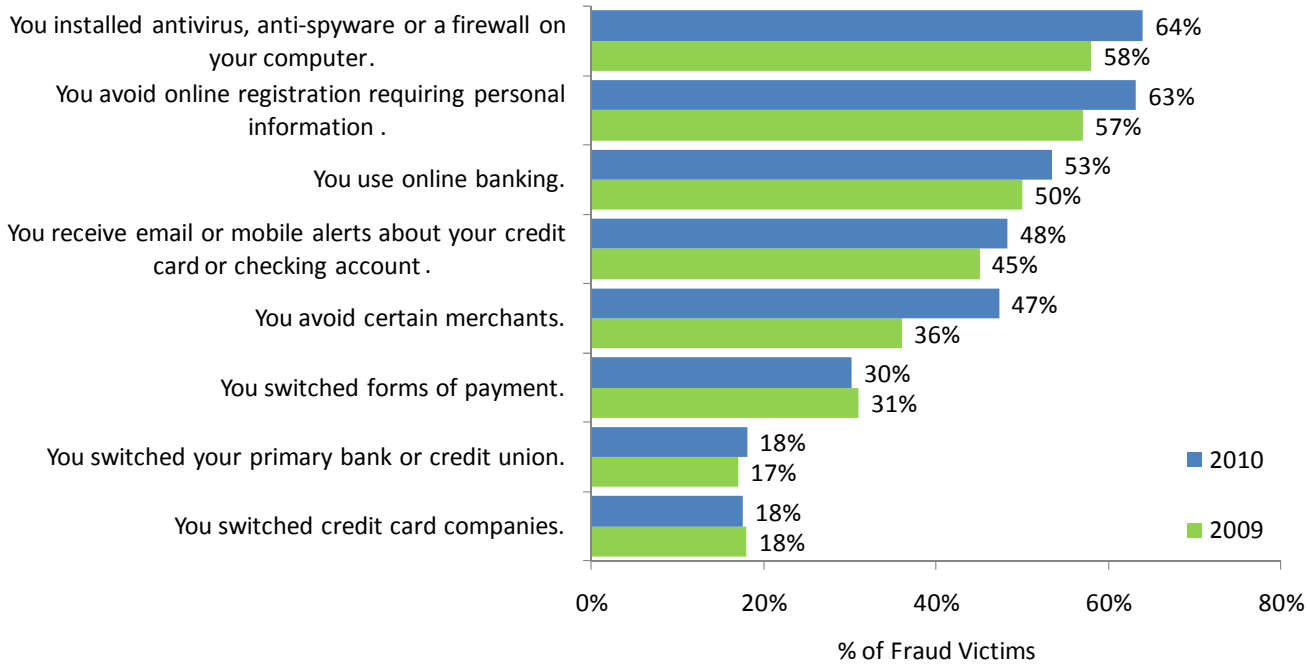
[2] **The Durbin Amendment: Initial Outcomes and Implications.** Javelin Strategy & Research, July 2011.

Credit cards are historically associated with greater risks, and changing consumer behavior could push the pendulum back up on fraud. Such swings in consumer payment preferences can deeply impact a merchant's exposure to fraudulent transactions as well as impact the types of fraud mitigation efforts required, especially since credit cards usually have zero liability and debit cards do not. Retailers must constantly cater to payment preferences even while investing in fraud solutions that work across payment types such as identity-based verification and authentication.

Second: A defrauded customer is a potentially lost customer. In 2010, there is a notable rise in the proportion of victims who state they avoid certain merchants as a result of being defrauded (increased from 36% to 47% of victims). Further, more than 3 in 5 (63%) victims reported they avoid online registration, almost 1 in 3 consumers switch forms of payment methods, and almost 1 in 5 switch FIs. (See Figure 4 below) Each of these behaviors represents significant ramifications for a merchant seeking to maintain and expand a strong business – especially on operational costs of acquiring and maintaining customers.

Merchants must understand how consumers react to fraud and the negative impact on their businesses, so as to take the appropriate steps to resolve and prevent fraud problems and communicate their actions to consumers. Otherwise, merchants could lose customers due to fear.

Figure 4: Fraud Victims' Financial Behaviors, 2009–2010



Q38: As a result of being a fraud victim, which statements are true?

November 2010 n = 470, November 2009 n=620
Base: All fraud victims.

FI executives report they also experienced a drop in fraud losses. They typically report mean fraud losses of less than 1% to 2% of total payment card volume based on three years of research projections. These reports suggest FIs could be absorbing $2 billion to $8 billion in total fraud losses associated with resolving unauthorized retail transactions.

II. The Fraud Swing to Come

More Sophisticated Types of Fraud Are Developing, FIs Warn

Despite the recent drop in fraud, FI executives interviewed this year warn that more sophisticated types of fraud are developing. Cybercriminals are moving from hacking into computers and changing hardware and software to obtaining personal information and using false identities in "bust out" schemes to run fraudulently obtained credit card numbers through shell businesses, collecting money from credit card companies without delivering goods and services. Newer, more complex schemes include:

- Phishing attacks. A phishing attack is a method of trolling for information by sending out authentic-looking e-mails that impersonate the victim's financial institution or another trusted entity to lure the victim to a fake site to collect passwords or other personally identifiable information.
- Spear phishing. A "spear-phishing" attack is a more targeted attack that uses personalized information to make the phishing e-mail seem plausible and trustworthy to the victim.
- Card verification value (CVV) cracking. In this type of fraud, fraudsters gain access to CVV codes on credit cards. They do this by sliding a credit card through a magnetic-strip reader and recovering the large amount of data residing in the magnetic strip that runs lengthwise along the back of the credit card. Or, they can use the multidigit numeral printed flat on the card (separate from the longer, embossed account numeral) to make fraudulent purchases. On a VISA, MasterCard, or Discover Card, the printed CVV contains three digits and is located on the back near the signature area. On an American Express card, it contains four digits and is located on the front near the embossed account numeral.
- ATM skimming. Fraudsters utilize a skimming device that reads all the account information stored electronically on the magnetic strip of the ATM card and, depending on the sophistication of the device, records the PIN as it is punched in on the ATM keypad.
- Botnets. An emerging trend is the use of botnets, a collection of compromised computers used for malicious purposes. Under a hidden identity, the botnet can steal passwords, log keystrokes, and send out spam messages, all in an attempt to gain access to personally identifiable information.

So who is at risk? – FI perspective

- Business-to-business fraud where there are typically higher average tickets
- Goods that are easily sold, the degree to which the item is a commodity, such as electronics and jewelry
- Card-not-present transactions
- Merchants that have $10 million or more in online sales
- International merchants: Particularly in the U.K., as U.S. merchants have improved their tools the fraudsters seek easier targets elsewhere in the world: "The hard data is that [U.K.] fraud rates are two and one-half times that of what we have seen in the U.S."
- Small- to medium-sized merchants who cannot afford to implement risk management

Data Breaches on the Rise

After a relatively quiet 2010 in terms of breaches, 2011 began with some of the largest data breaches ever recorded. More than 180 million records were put at risk. The first major data breach, known as "the Epsilon" and announced on April 1, leaked 77 million customer names and e-mail addresses. Affected companies included Citibank, the Kroger Company, JPMorgan Chase, Capital One, Marriot Rewards, McKinsey Quarterly, US Bank, Citi, TiVo, Best Buy, Ritz-Carlton Rewards, Brookstone, Walgreens, the College Board, and the Home Shopping Network.[3]
Shortly after the Epsilon breach, the state of Texas announced that an unencrypted data file had been left on a publicly accessible server. More than 3.5 million records were exposed, and the state of Texas began the process of sending out "breach letters" (as did Epsilon's clients). In this case, the damage could be considerable as the exposed information included name, address, Social Security number, driver's license number, and date of birth. This represents the jackpot for a fraudster as it allows the creation of new accounts, which are difficult to detect.[4]

In mid-April, Sony's online entertainment networks were attacked, risking the records — including name, birth date, and possible mother's maiden name — of more than 100 million customers. This information can be used to check — and falsify — identities. Another case in point, in spite of being a powerhouse name, Sony was reportedly breached by an SQL injection — a very basic and easy attack to produce.[5]

The impact of these breaches will be felt for years to come. They provide fraudsters with a wealth of information, including awards points balances, which cybercriminals can use to appear legitimate in their requests for personal information, such as PINs, Social Security numbers, and credit card numbers. The Epsilon breach is a part of a troubling trend where providers are not treating certain personally identifiable information with the same care and due diligence that would be applied to more traditional financial data (e.g., bank account number or credit card number).

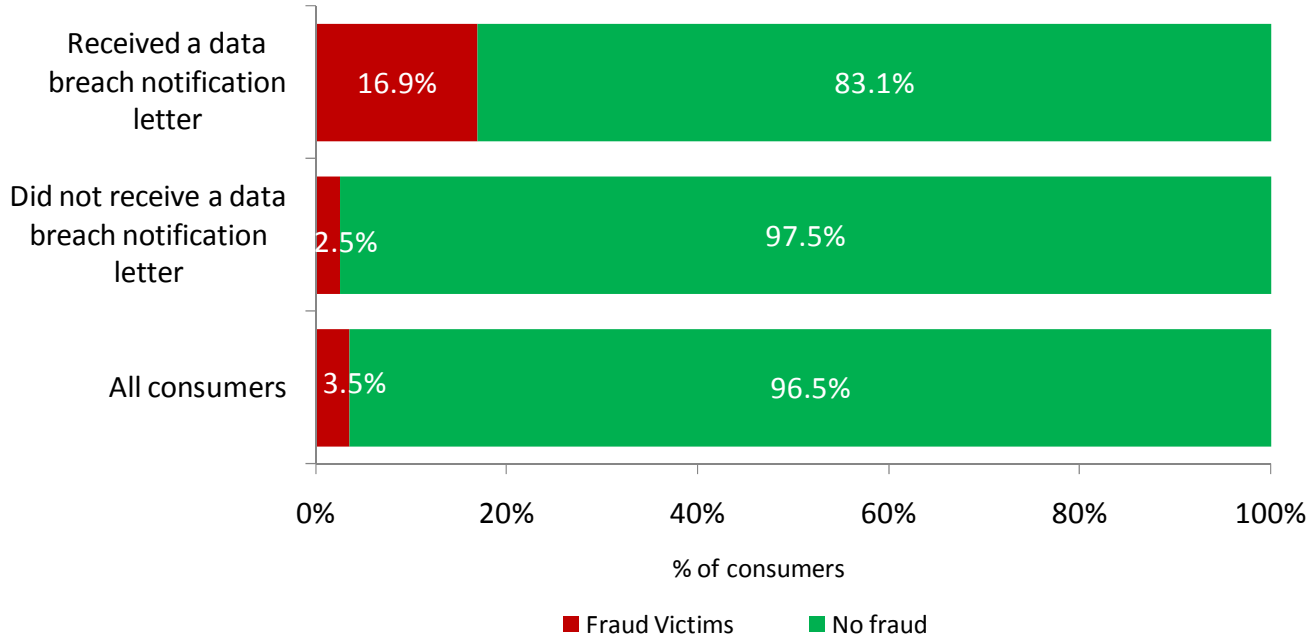
[3] **2011 Second Annual Antivirus, Browser, and Mobile Security Report.** Javelin Strategy & Research, July 2011.

[4] Ibid

[5] Ibid

A look at consumer data further supports the correlation between fraud and data breaches. Seventeen percent of consumers who received a data breach notification also were victims of identity fraud, whereas the victimization rate was only 3% among consumers who did not receive a data breach notification. (See Figure 5)

Figure 5: Identity Fraud Victims Who Also Received a Data Breach Notification, 2010



November 2010; n = 337, 4,667, 5,004
Base: Consumers whose information was compromised, consumers whose information was not compromised, all consumers
© 2011 Javelin Strategy & Research

Q2: In the last 12 months, have you been notified by a business or other institution that your personal or financial information has been lost, stolen or compromised in a data breach? Q4: Have you, yourself, ever been a victim of identity theft?

This finding is particularly important when the cost of fraud is considered in terms of total consumer cost. Victims who received data breach notifications faced higher out-of-pocket costs ($1,108 vs. $510) and more resolution hours (41 vs. 30) than those who did not. Protecting customers will be key in the coming months and play a significant role in stabilized growth through customer loyalty and retention.

III. Merchant Fraud Experience: KEY SNAPSHOTS

The Fraud Multiplier by Industry

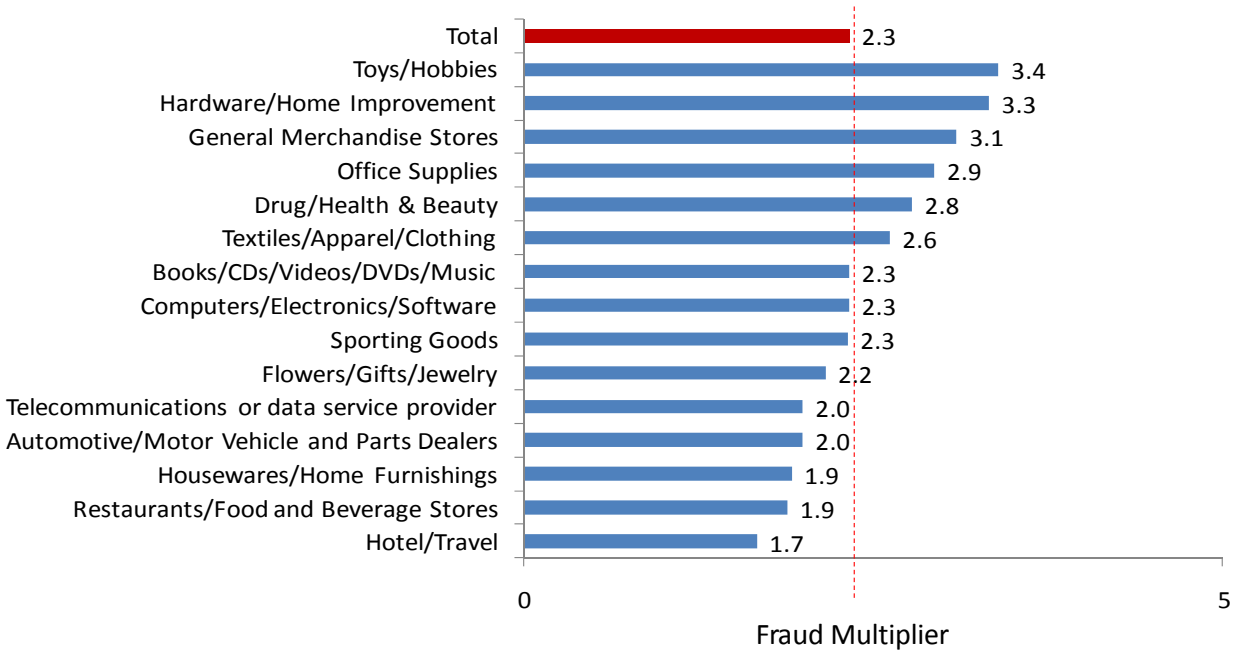
The fraud multiplier varies widely by industry segments, similar to what was seen in 2010. Industries with higher-than-average fraud multipliers are clearly ones with physical goods having higher probability of being lost or stolen, where merchants have to bear the cost of replacing these goods. These industry segments include toys/hobbies, hardware/home improvement, general merchandise, and clothing /accessories.

It is important to note that not all industries report a decline in this metric year over year. There are industries that in fact report an increase (such as toys/hobbies or hardware/home improvement) as well as others that register visible declines (such as hotel/travel, houseware, and home furnishings). Some of this effect may be due to overall economic conditions (e.g., travel.) The key message to walk away with is that not all industries are experiencing lower out-of-pocket costs. Vigilance and greater security measures are still needed, especially if you are a higher-risk merchant selling goods that are easily lost or stolen.

Insight

FIs also agree that they generally see higher fraud rates in industries that sell items that could be easily flipped and resold, such as electronics and computers, jewelry and coins, and merchandise from discount stores. As one FI executive says, "near-cash items, such as gift cards, are also very vulnerable to fraud."

Figure 6: Fraud Multiplier by Industry, 2011



(Note: includes industries with low (i.e., less than 30) base size)

The Nature of Completed Fraudulent Transactions in 2011 vs. 2010

The year-over-year comparison of completed fraudulent transactions reveals warning signs that must be noted by merchants. In 2011 merchants report a drop in the number of completed transactions vs. 2010. This is not entirely surprising when considering the lower incidence of fraud noted by the industry overall.

However, it is important to note that although the number of completed transactions decreased, the average dollar value per transaction increased noticeably since 2010. The average dollar value of a completed transaction was $122 in 2011 vs. $91 in 2010. This signals the entrance of perhaps more sophisticated and invasive fraudsters, costing heavier damage than petty criminals. It is a worry expressed by FIs as well and heralds warning signals for the merchant industry.

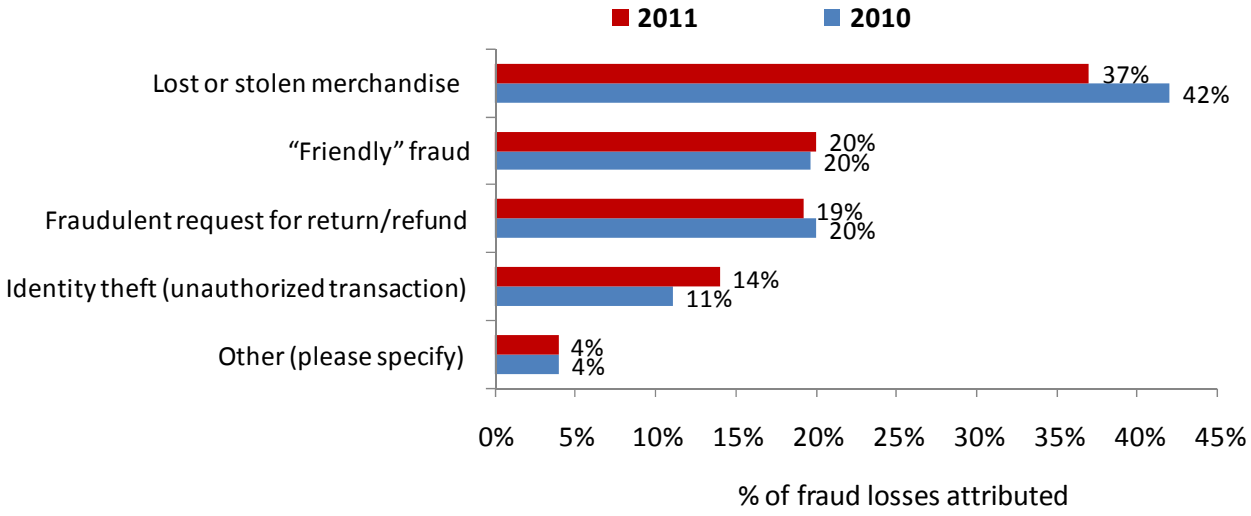
There are newer technologies making their way to the fraudster, which may continue to increase their effectiveness. An excellent example of this is the Zeus Trojan, which was one of the original man-in-the-browser attack Trojans. The source code for Zeus has been made public and has been merged into an even more modern and effective Trojan known as SpyEye. The combination is proving extremely difficult to stop.

As the consumer retail market continues its recovery and the number of transactions increases, retail merchants, especially those moving into new markets such as mobile, alternative payments, or international arenas, can greatly impact transactions and fraud exposure by taking necessary precautions to protect themselves.

Types of Fraud

In 2011 merchants report an overall decrease in fraud losses attributed to lost or stolen merchandise and an upward shift in ID theft. Coupled with a rise in the average dollar value of fraudulent transactions, this trend again highlights a growing threat of more sophisticated, high-impact fraud.

Figure 7: Distribution of Fraud Losses by Types of Fraud, 2010-2011



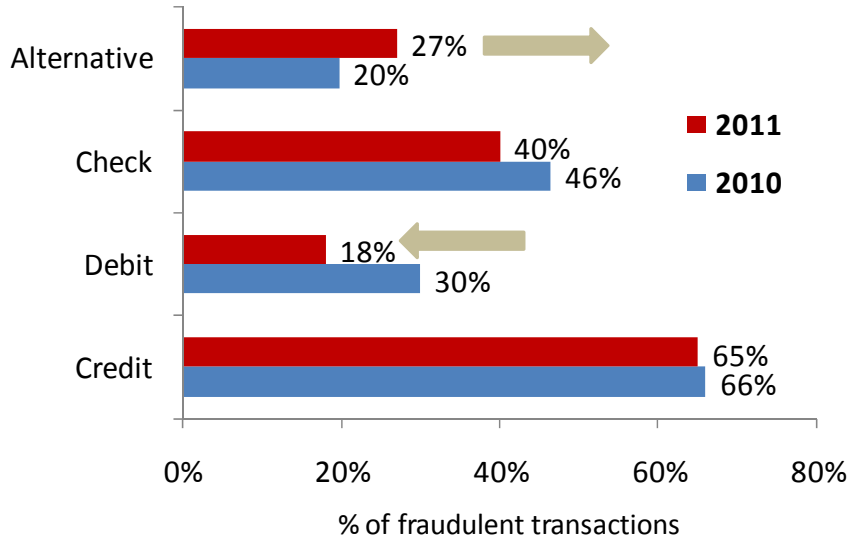
Q16: Please indicate the percentage distribution of the following fraud methods below, as they are attributed to your total annual fraud loss over the past 12 months.

July 2011, n=455; July 2010, n=712
Base: Merchants stating fraud amounts/stating don't know

Payment Methods Used to Commit Fraud

Credit card fraud continues to be the main channel through which fraudulent transactions hit merchants while debit cards record a decrease. The decrease in debit cards is driven mostly by a decrease in mentions by small to midsize merchants rather than large merchants.

Figure 8: Percent Distribution of Fraudulent Transactions over Payment Methods, 2010–2011



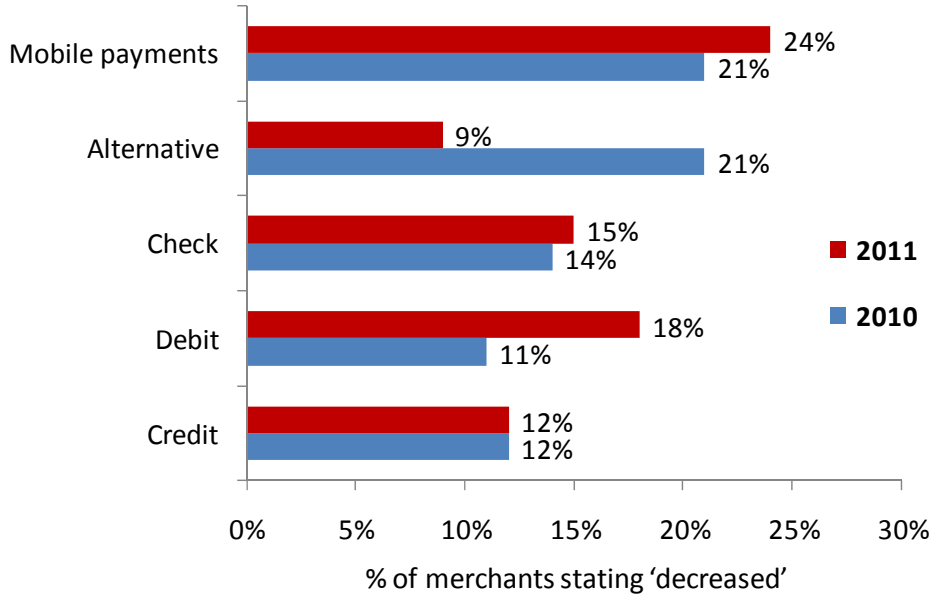
Q25: In thinking about which payment methods are most commonly linked to fraudulent transactions, please indicate the percentage distribution, to the best of your knowledge, of the payment methods used to commit fraud against your company. (Mobile not shown due to small base size)

July 2011, July 2010; n varies: 50-200
Base: Merchants providing fraud amount/stating don't know, accepting method & tracking losses by payment method.

It is key to note that emerging channels such as mobile and alternative payments record an increase. These are the primary areas of growth for businesses – and also the most nebulous areas where security and prevention methods are still growing.

Javelin's consumer research shows about 40% of consumers report monthly use of alternative payments; various factors contribute to the use of alternative payments: consumer reluctance to use credit cards, the economy, consumer debt, consumer convenience, etc. As consumers turn to alternative payments, it will be important for merchants to understand the unique prevention, mitigation, and resolution requirements of this channel and address them.[6]

Figure 9: Merchants Reporting Decreases in Fraud by Payment Method, 2010–2011



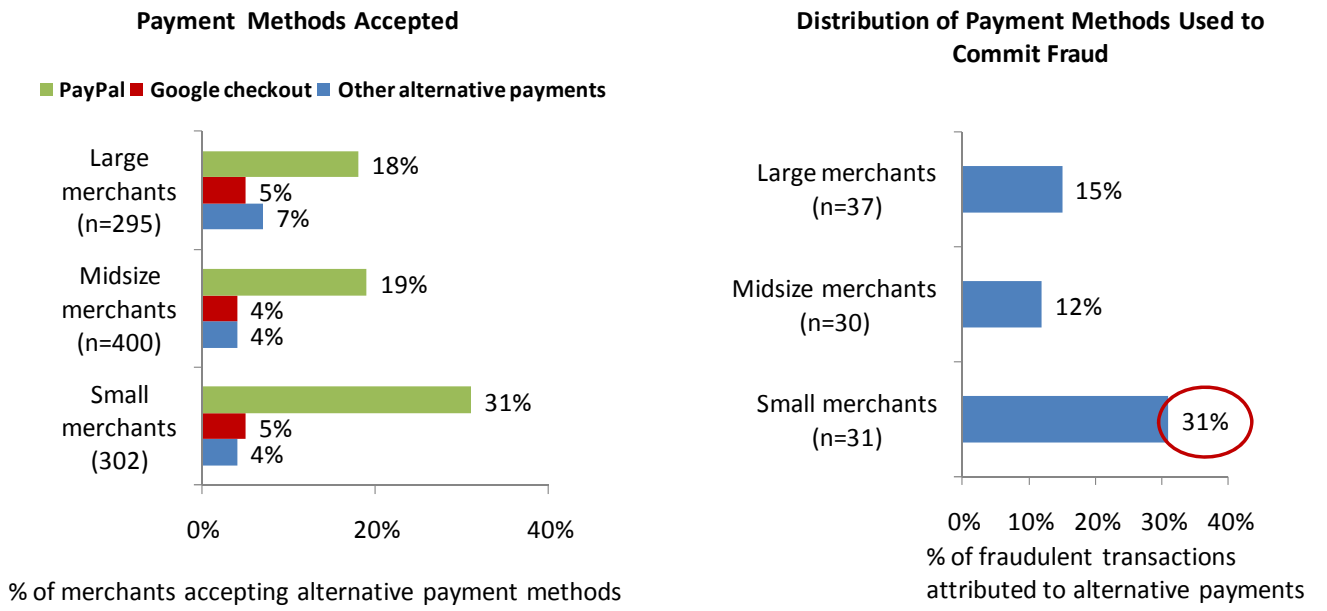
Q26: To the best of your knowledge, over the past 12 months, has the fraudulent use of each of the following payment methods increased, decreased, or stayed the same, for your company? (Shown: Those reporting decrease)

July 2011, July 2010; n varies: 50-800
Base: All merchants accepting payment method & tracking fraud losses

[6] **2011 U.S. Omnibus Consumer Survey.** Javelin Strategy & Research, August 2011.

A deeper look into merchant segments also reveals a key trend for alternative payments (continuing from 2010). Small merchants are active in their use of alternative payments, spurred by their use of PayPal. Overall, 31% of small merchants report they use PayPal, while about 20% of midsize to large merchants report the same. Yet, as seen in Figure 10 below, the proportion of fraudulent transactions attributed to this payment method is far higher among small merchants than their counterparts. Small merchants are less equipped to battle the more sophisticated methods of fraud associated with newer payment methods, and fraudsters are taking advantage of it.

Figure 10: Alternative Payments – by Merchant Segments, 2011



July 2011
Base: All merchants; Merchants providing fraud amount/stating don't know, accepting method & tracking losses by payment method

Key takeaway: As merchants expand into the newer areas of payments in an effort to grow their business, they must also step up their awareness and use of fraud mitigation solutions that help protect them from new risks. Large merchants are already mapping the way toward safer processes. Small merchants must take the time to learn from existing practice, not waste resources in reinventing the wheel, and most importantly, not trivialize the threat presented by these channels.

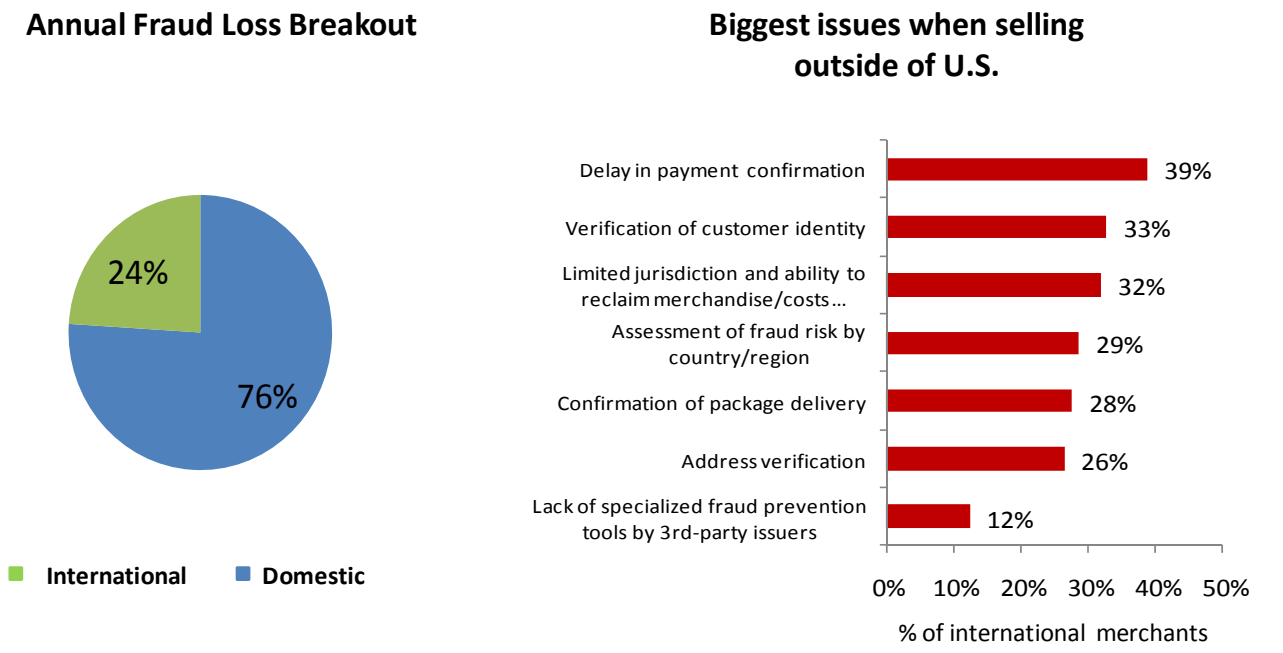
IV. Growth Areas for Merchants and Implied Risks

Unquestionably, today the growth areas for businesses lie in the mobile, e-commerce, and international arenas. As merchants expand into these areas, they will need to guard against the fraud challenges presented by each of these channels. This sections highlights pain points for each key merchant segment to serve as a guide for merchants interested in expanding their business.

2011 SPOTLIGHT: The International Retail Merchants

The 2011 LexisNexis study captures data from 492 U.S.-based merchants who report having an international presence. These merchants report approximately 20% of their revenue stems from international channels and 80% stems from domestic channels. The distribution of fraud losses mirror this breakout, with about 76% of fraud losses attributed to domestic fraud and 24% attributed to international fraud.

Figure 11: International Merchants, 2011



July 2011; n=255, n=492
Base: All international merchants providing fraud amount/stating don't know, all international merchants

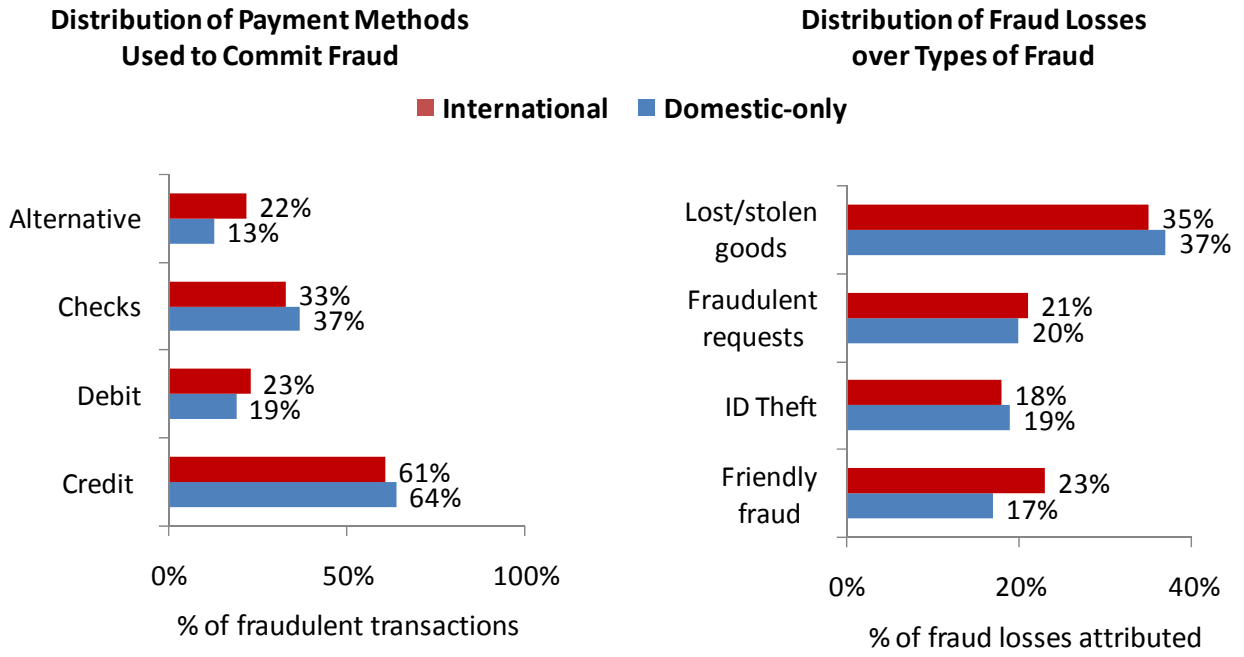
Some of the top issues challenging international merchants are: delay in payment confirmation, verification of customer identity, limited jurisdiction, and ability to reclaim merchandise and costs. This limited control over delivery, payment confirmation, and reclamation partially explains why the proportion of fraud losses attributed to the redistribution of lost or stolen merchandise is higher among international merchants (30%) vs. noninternational merchants (18%).

International merchants also appear more vulnerable to "friendly" fraud than domestic-only retailers (see Figure 12). This aligns with the higher proportion of fraud losses attributed to alternative payments by this segment (than domestic merchants) and reveals the lack of control in international arenas. As merchants expand to new geographical areas with lowered controls, the need for robust security practices becomes more important than ever.

Insight

FIs also agree that they generally see higher fraud rates in industries that sell items that could be easily flipped and resold, such as electronics and computers, jewelry and coins, and merchandise from discount stores. As one FI executive says, "near-cash items, such as gift cards, are also very vulnerable to fraud."

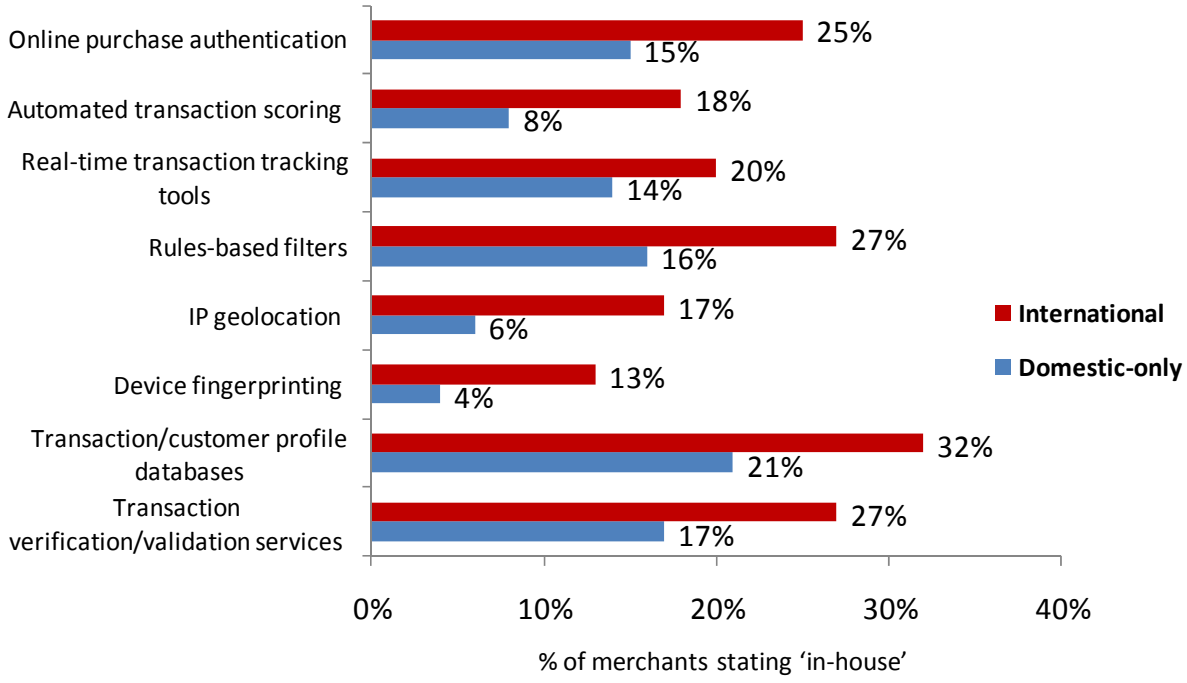
Figure 12: International vs. Domestic-Only Merchants, 2011



July 2011, n varies: 50-300
Base: Merchants providing fraud amount/stating don't know, accepting method & tracking losses by payment method

Compared to domestic-only merchants, international merchants are consistently higher in reporting in-house use of proprietary fraud detection tools (see Figure 13).

Figure 13: International vs. Domestic-Only Merchants: Tools Used In-House, 2011

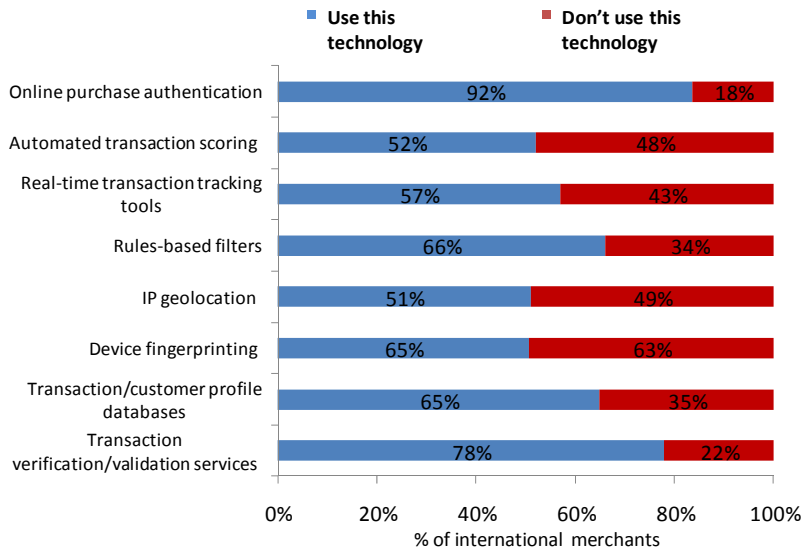


Q30: Does your company currently utilize any of the following fraud detection solutions?

July 2011; International n=334, Domestic n=201
Base: Merchants operating online

Yet, despite this vigilance by some international merchants, there remains a high proportion of international merchants not using these tools currently. For example, 48% of international merchants state they don't use automated transaction scoring, 43% state the same for real-time transaction tracking tools, 34% indicate they don't use rule-based filters, 49% state they don't use IP geolocation, 63% indicate they don't use device fingerprinting, etc.

Figure 14: International Merchants' Current Use vs. Not Use of Online Fraud Detection Tools, 2011



Q30: Does your company currently utilize any of the following fraud detection solutions?

July 2011, n=334
Base: International merchants operating online

Insight

Discussions with FI executives highlight a key difference in international vs. domestic payment fraud. U.S. markets contend with fraudulent transactions from credit and debit cards with magnetic strips. International markets use "chip and pin" technology, where credit and debit cards contain an embedded microchip and are authenticated automatically using a PIN, making fraud a cross-border issue. Merchants must understand the unique environment in international areas as they expand.

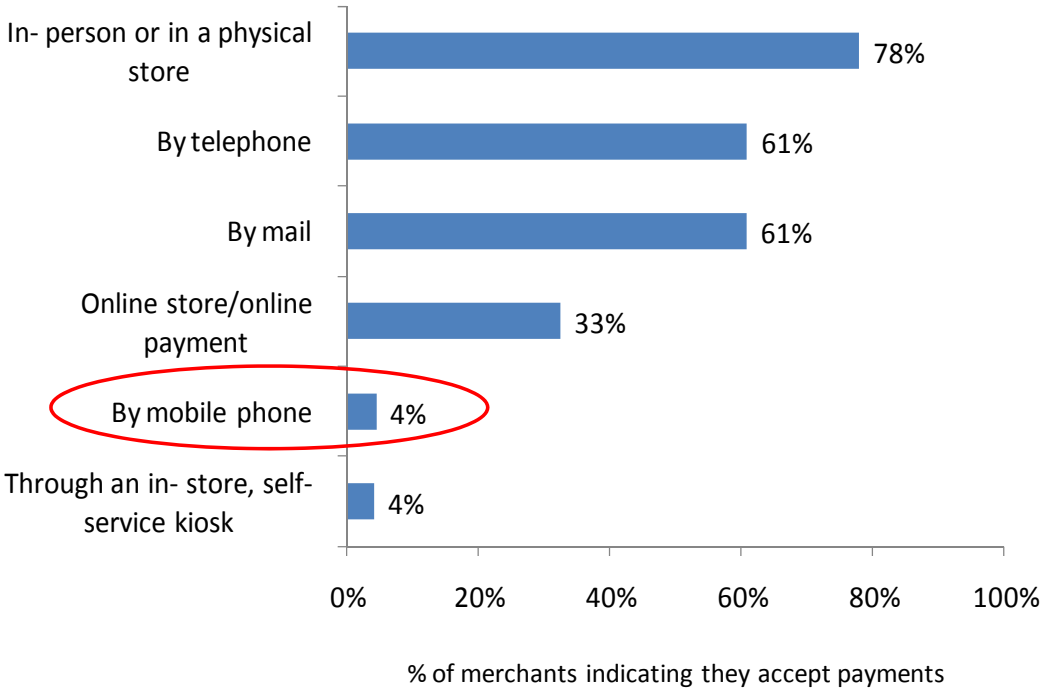
The Mobile Merchants

According to the 2011 merchant data, mobile payments are accepted by 4% of merchants. Although this represents growth since last year (1% in 2010), mobile has a long way to go before it becomes the mainstay of consumer payment behavior. Nonetheless, merchants are preparing to expand – with 20% of current nonusers indicating they intend to accept mobile payments in the next 12 months. Given this interest among merchants as well as the explosion in smartphone adoption among consumers, the growth of mobile payments is imminent.

Insight

Javelin's consumer data shows the end user is a bit hesitant on mobile due to security concerns. By ensuring a safe channel, merchants not only develop a more sticky relationship with the consumer, they also provide positive incentive for that consumer to use the mobile channel.

Figure 15: Payment Methods Currently Accepted by Merchants, 2011



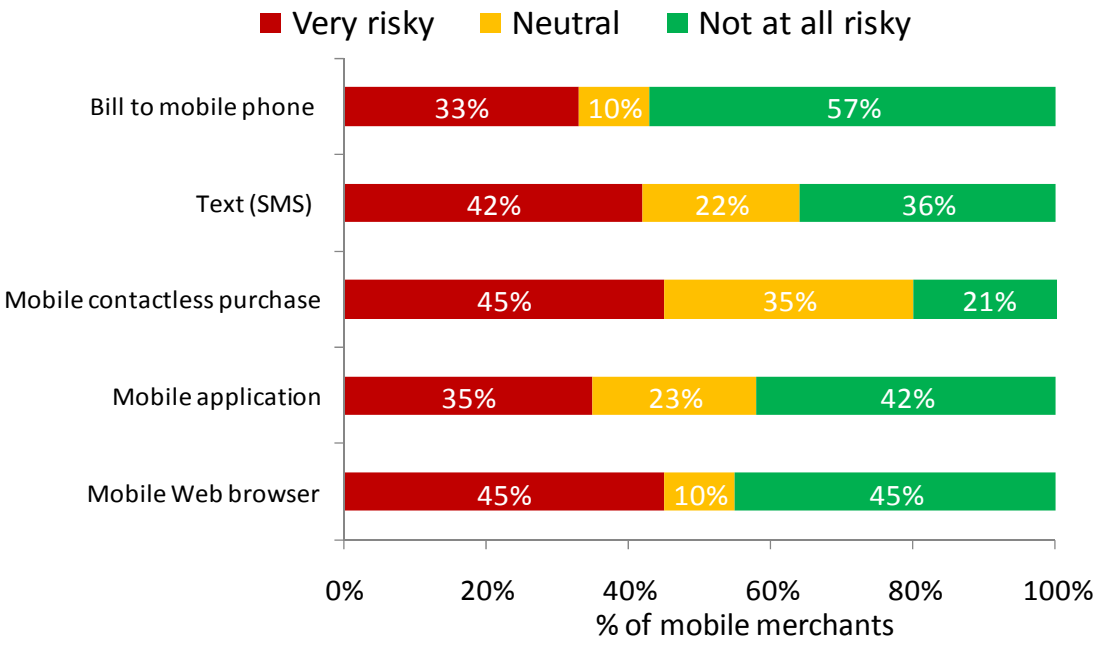
Q5: Does your company currently accept payments through any of the following channels?

July 2011, n=1006
Base: All merchants

Interestingly, this year's growth in acceptance of mobile payments appears to be fueled by a spike in interest among small merchants rather than larger merchants. In 2011, about 7% of small merchants surveyed report that they accept mobile payments, up from 2% last year. Of course acceptance of mobile payments is almost twice as high among large merchants, with 13% accepting mobile payments. Yet this actually represents a stagnated level of interest year over year. As seen by their vulnerability when using alternative payments, small merchants are generally less equipped to expand into new payment arenas. Members of this segment must arm themselves with proper fraud mitigation tools and follow best practices to combat the threats posed by mobile or they will provide easy target for fraudsters.

Currently, the mobile Web browser is the most commonly accepted payment method, followed by applications. Text SMS and contactless payments are least used. Interestingly, no payment method receives a clear vote of confidence from these merchants in terms of safety. (See Figure 16) A deeper look into the fraud experience reported by this segment explains the worry and anxiety evident in the safety ratings.

Figure 16: Risk Ratings for Mobile Payment Methods, 2011

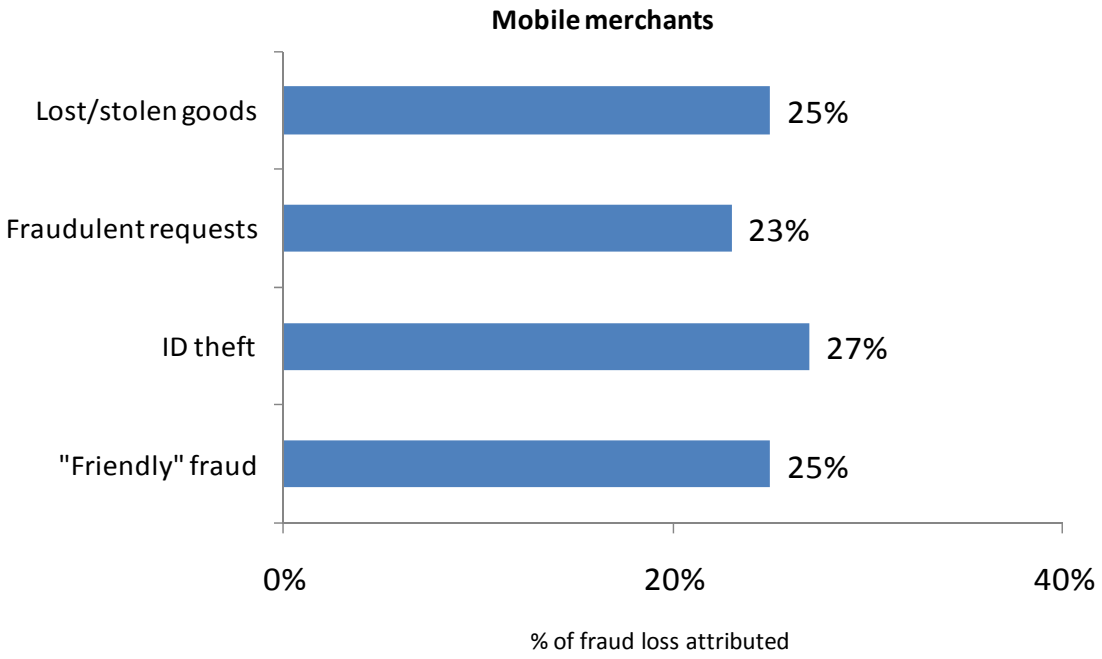


Q29: Of the following mobile payment methods, please rank the level of fraud risk you associate with each method from least risky to most risky.

July 2011, n=78
Base: Merchants accepting mobile payments

Continuing the trend from last year, mobile merchants report a high number of completed fraudulent transactions in a month (about 1,400 fraudulent transactions). The average dollar value of these transactions is also higher among mobile merchants ($167) compared to total merchants ($122). Further, compared to the overall merchant population, merchants accepting mobile payments attribute lower fraud losses to lost and stolen goods but come out higher on all other fraud types, most notably ID theft.

Figure 17: Distribution of Fraud Losses over Types of Fraud – Mobile Merchants, 2011



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 2011, n=37
Base: Mobile Merchants willing to share fraud amounts/stating don't know

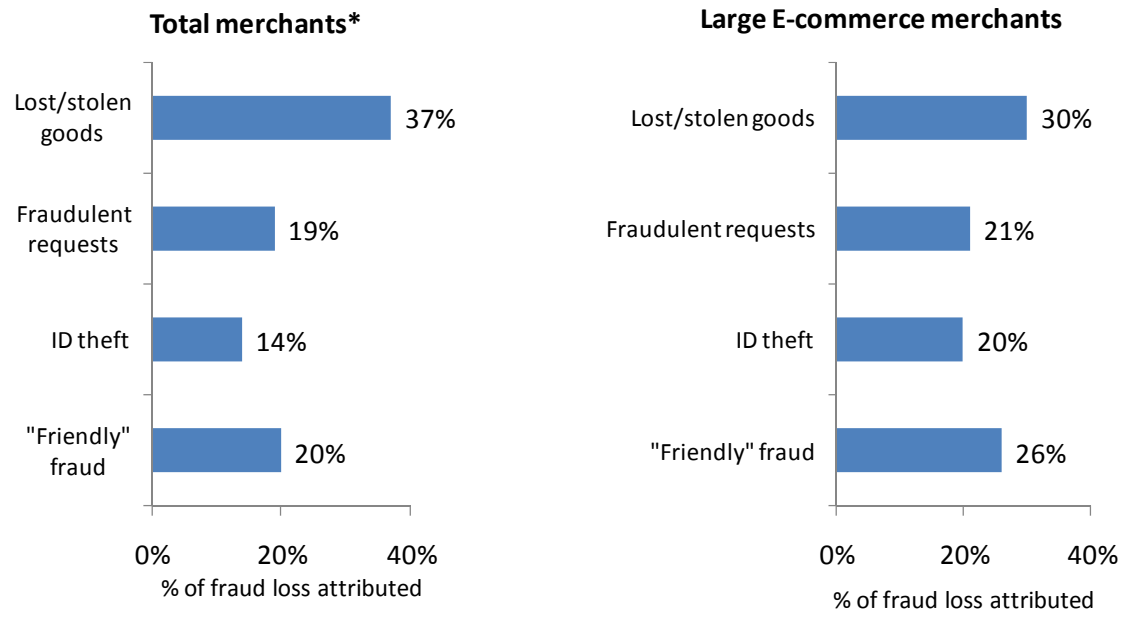
Merchants expanding into mobile payments are at high risk of chargebacks through ID theft, friendly fraud, and fraudulent returns. They also pay $2.0 out-of-pocket for every dollar lost in fraud (fraud multiplier). All in all, the signs are disheartening and as the adoption of mobile payments increases, the vulnerability of this payment method warrants greater vigilance on the merchant's part.

Large E-commerce Merchants

Large e-commerce merchants sell across a variety of channels – in-person/physical store, online, telephone, in-store self-service kiosk, mobile, and mail – to access a wide variety of consumers. The channels merchants most commonly used to accept payments are online (100% of respondents), in-person/physical store (63%), telephone (60%), and mail (53%). Almost 1 in 5 large e-commerce merchants accept payments by mobile phone, and 2 in 5 are considering accepting payments by mobile phone over the next 12 months.

Similar to the mobile merchants, large e-commerce merchants are at higher risk of fraud losses from ID theft and friendly fraud, compared to the average merchant. Both pose significant hurdles. For example, friendly fraud requires the merchant to prove the item was received which can prove to be challenging especially for online purchases. Typically, these chargeback requests lead to an investigation and costs can boomerang to the merchant.

Figure 18: Distribution of Fraud Losses over Types of Fraud – Large E-commerce, 2011



Q16: Please indicate 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 2011; Total n=455, Large e-commerce n=85
Base: Merchants willing to share fraud amounts/stating don't know
* Weighted data

Moreover, FI executives also observe a higher incidence of fraud through e-commerce channels. According to financial institutions interviewed in this research, as consumer use of the e-commerce channel increased, so did fraud. Fraudsters follow the money and have learned that, on average, e-commerce merchants have much higher-priced-ticket items. Crooks can use false identities to purchase large amounts of merchandise without raising suspicion. The data bears this out. The average value of a completed e-commerce fraudulent transaction was $255, higher than the $122 reported by total merchants on average.

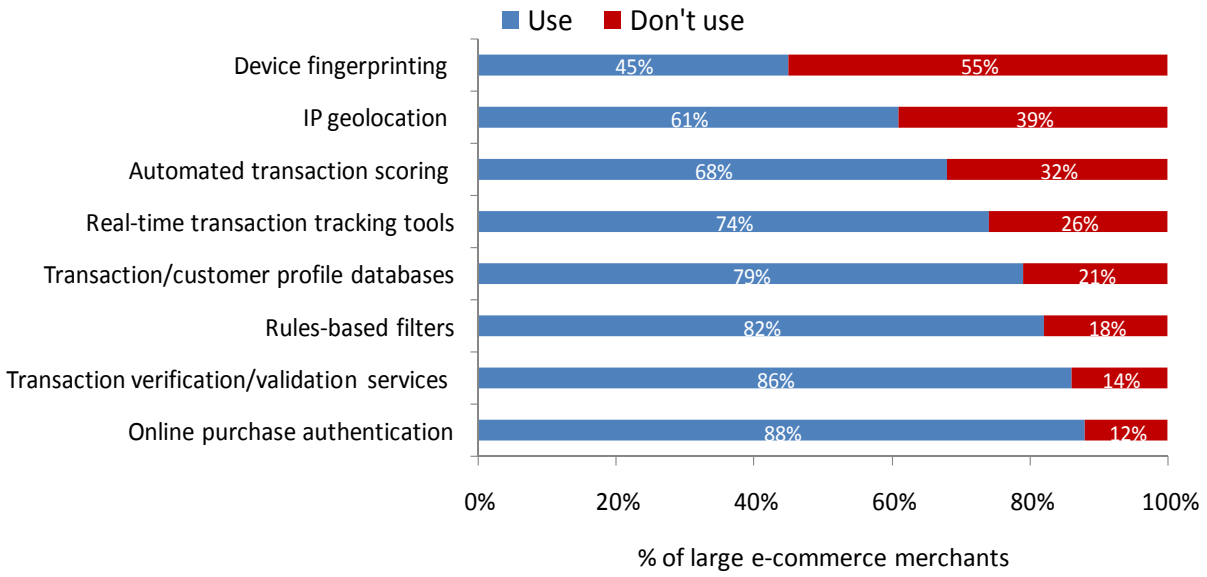
Large e-commerce merchants report their fraud losses continue to be almost evenly split between physical "brick and mortar" and card-not-present situations (including mobile, online, and telephone/mail). With multiple, high-volume channels, large e-commerce merchants need to look to fraud solutions that can effectively work across channels.

One cause for concern: While this segment is most active in using online fraud mitigation tools such as online purchase authentication and transaction verification, it has yet to improve its adoption of other tools such as IP geolocation, device fingerprinting, and automated transaction scoring that could be key to battling fraud threats, especially ID theft.

Insight

Although historically merchant associations have tried to develop best practices to help prevent card-not-present (CNP) fraud, such as monitoring single purchases using multiple cards or tracking unusual customer activity, the reality is that consumers expect to use their cards but are not always vigilant or appreciative of extra security steps. Merchants dealing with CNP are faced with the difficult task of weighing their higher security needs against their customer's comfort and ease. It's a hard balance to maintain, but merchants must continue to tread this line carefully. Security and customer retention loyalty are equally vital to business expansion.

Figure 19: Current Use of Fraud Detection Solutions – Large E-commerce Merchants, 2011



Q30: Does your company currently utilize any of the following fraud detection solutions?

July 2011, n=163
Base: Large e-commerce merchants operating online

New Regulations May Drive Consumers to Higher-Risk Payment Methods

In order to expand productively, merchants must also stay aware of changes in industry regulations and their impact. This is especially relevant now that new regulations may drive the use of certain payment methods that are historically associated with higher fraud rates (e.g., credit cards). Starting October 2011, the Durbin Amendment will limit the amount of debit card fees that retailers must pay, fees that will then be absorbed by consumers. The Durbin Amendment (along with Regulation E) is estimated to create up to a $16.4 billion loss of annual revenue for debit card issuers. In response, FIs may introduce debit card fees to consumers to make up for revenue loss. Three in five consumers said they would switch to another form of payment if FIs imposed debit card fees. Thus fees imposed by FIs may drive consumers back to credit cards, reversing the swing to debit cards that was seen last year. Historically, credit cards are associated with greater fraud rates, which will spike as consumers go back to increasing their usage of this payment method. The somewhat stagnated (yet high!) fraud rates reported for credit cards this year may climb in the coming months if consumers shift back to this payment method (see Figure 8). As businesses focus on growing, they will also have to take care to limit the associated risks from this all-pervasive yet high-risk payment method.[7]

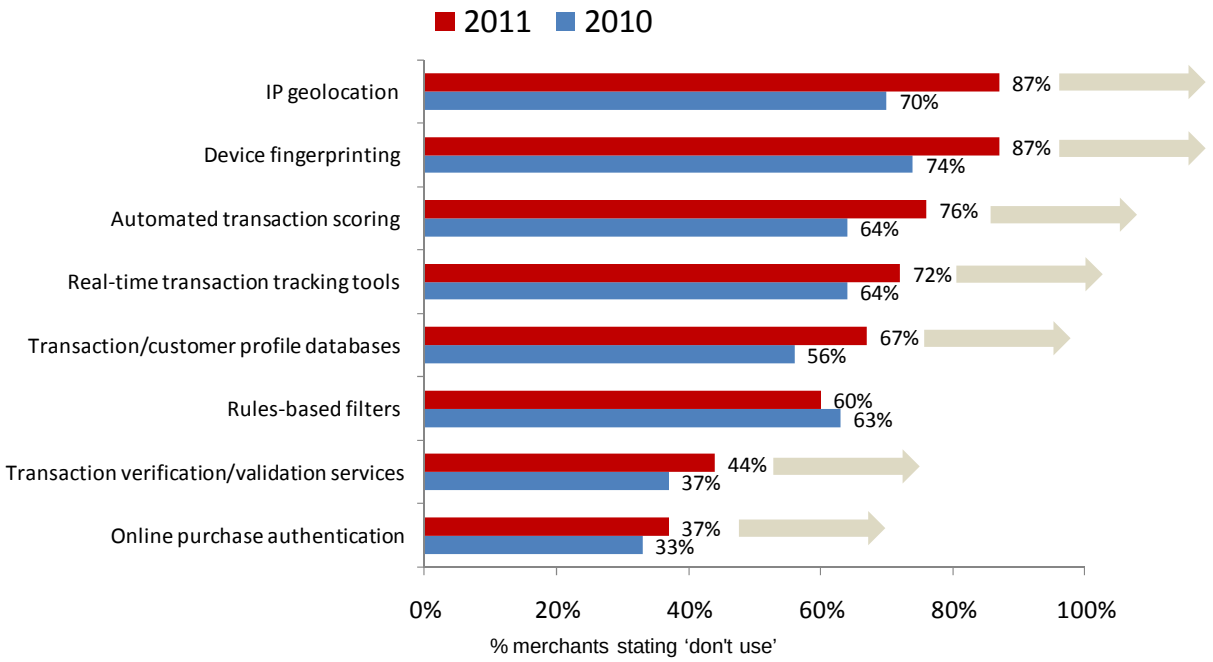
[7] **The Durbin Amendment: Initial Outcomes and Implications.** Javelin Strategy & Research, July 2011.

V. Current Merchant Security Practices – Complacency Settling In?

Current Use and Satisfaction

In a reversal of last year's trends, in 2011 merchants report they are shifting away from outsourcing. Unfortunately, the shift is toward not utilizing technologies rather than bringing them in-house. These are signs of complacency that must be addressed before the impact of data breaches and sophisticated fraudsters makes its combined attack.

Figure 20: Merchants Not Using Online Fraud Detection Tools, 2010-2011



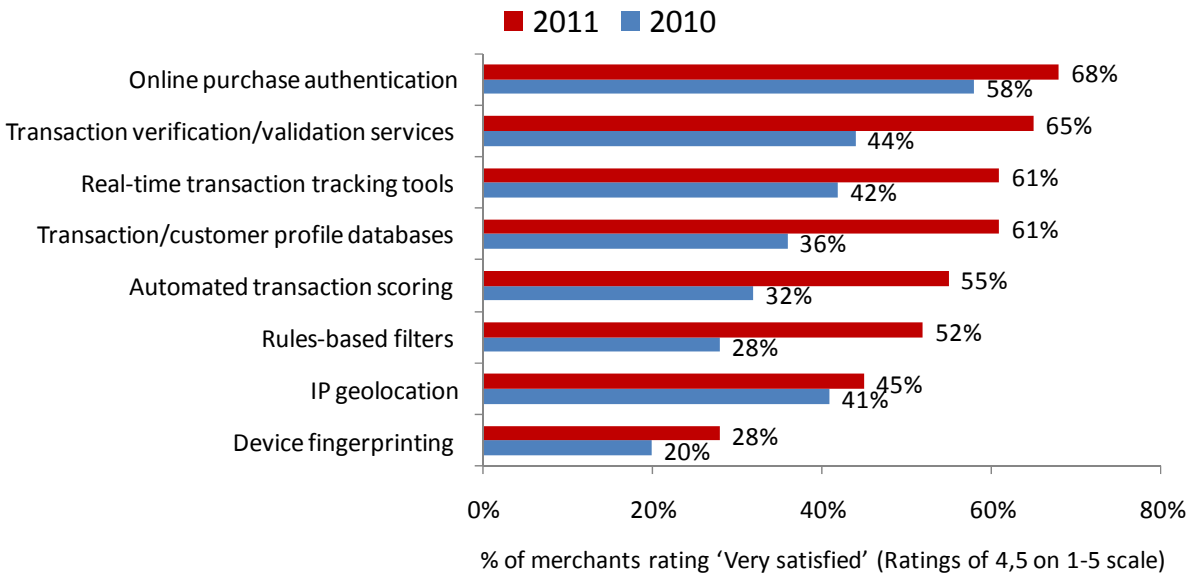
Q30: Does your company currently utilize any of the following fraud detection solutions?

July 2011, n=327; July 2010, n=372
Base: All merchants operating online

Merchants also report fluctuations in use of in-person fraud mitigation tools. They report a decrease for almost all tools except card verification value and PIN/signature authentication.

In 2011, merchants also report significantly higher levels of satisfaction for almost all tools tested. The lull in fraud trends may be boosting perceptions of effectiveness and satisfaction that may be misleading. As the results of this study show, current fraudulent transactions actually have higher-price tickets and high-risk merchant segments such as mobile and e-commerce continue to face a high number of such transactions. Merchants must not confuse the lull in fraud for increased efficiency or safety.

Figure 21: Merchant Satisfaction with Online Fraud Detection Tools, 2010-2011



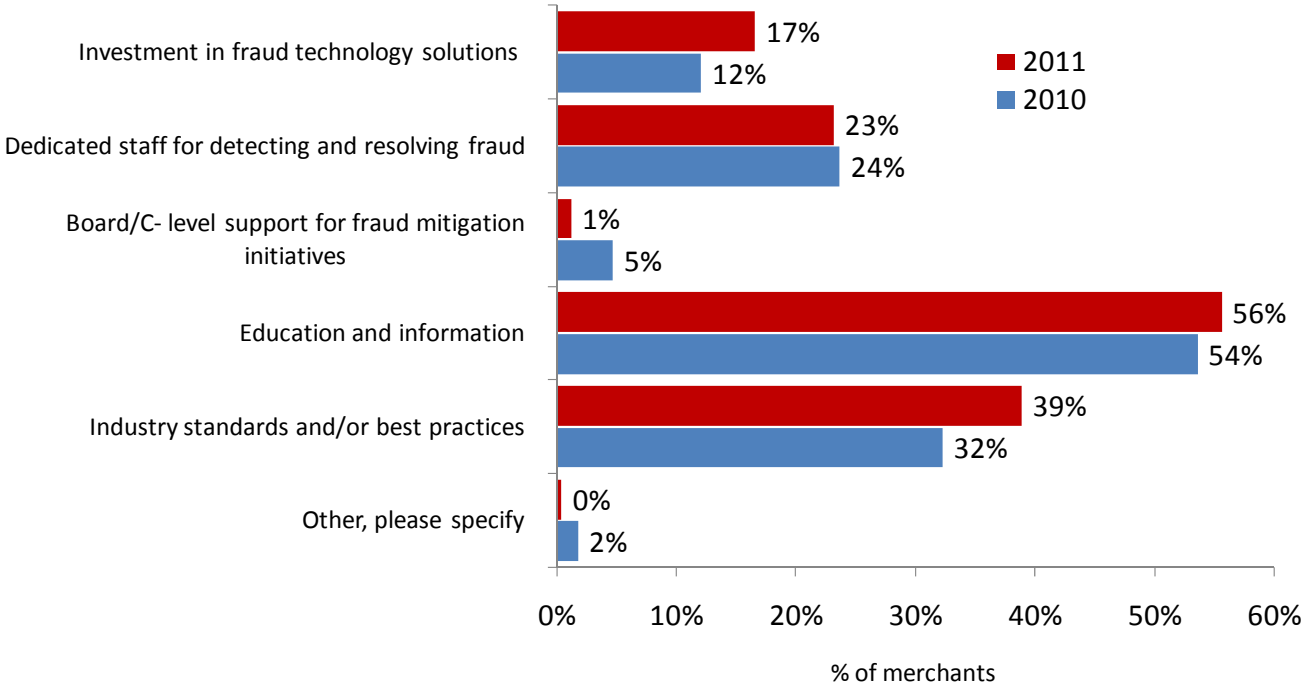
Q33: On a scale of one to five, please indicate your satisfaction level with your current fraud detection solution.

July 2011, July 2010; n varies: 50-250
Base: Merchants using each solution

Prioritizing Merchants' Fraud Mitigation Needs

The need for greater education remains top priority as last year. But in response to the shift away from outsourcing and toward "not using" tools, this year merchant executives are also emphasizing greater investment in fraud technology as well as industry standards and best practices.

Figure 22: Merchants' Greatest Needs for Reducing Fraud, 2010-2011



Q25: Which of the following does your company perceive as its greatest needs areas for fraud reduction?

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

VI. Tips from FIs

FI executives believe that fraud losses would be lower for both merchants and FIs if they could share information on fraud trends and patterns. Recommendations for merchants include:

- Improve security practices to prevent fraud before it happens.
- Monitor their businesses and identify suspicious and high-risk transactions, especially in such vulnerable channels as mobile, online, and e-commerce.
- Educate themselves on the most effective fraud prevention, detection, and resolution technologies and best practices.

FIs' specific recommendations for merchants include:

- Data sharing is key to preventing fraud.
    - "It would be [to] share as much data about the transaction that you can with the issuer and kind of partner better with the issuers."
    - "We have this fear of communication that actually limits our ability to mitigate. So we need to understand each other's processes."
    - "Issuers, acquirers, and the big merchants get together and start to have regular conversations about what they're seeing and really start to talk some of the issues and be able to share each other's points of views and best practices for mitigating losses and then kind of have a commitment to drive an action plan."
- Improving the customer identification process would reduce fraud. "Make sure that the person in front of you is the person presenting the card, check ID, check signatures."
- Merchants need to be proactive about reaching out to their acquirer or issuer and discuss concerns; they need to know when a transaction falls outside their typical parameters.
- Merchants should understand their regulations and know what they are responsible for.
- Merchants must have greater insights into their losses and transactions.
    - "So, I really think that going forward, whoever has the most data wins the game."
    - "Merchants need to be able to quantify their losses and identify root causes."
- A review of the survey data reveals merchants can definitely improve their knowledge of their internal processes and fraud losses:
- Almost 4 in 5 of respondents are unable to identify the allocation of costs to replace lost or stolen merchandise vs. redistributing lost or stolen merchandise.
- More than 3 in 4 respondents do not track the volume or frequency of fraudulent transactions by the payment method that was misused.
- Almost 1 in 10 respondents do not know the average value of fraudulent transactions that were prevented, and almost 2 in 10 don't track this information.

VII. Conclusions and Implications

Fraud Will Likely Increase; Merchants Can Grow Safely with Reduced Risks If They Stay Vigilant

- Much credit is due to the entire industry for fraud reduction. However, the current decline in fraud should not be interpreted by merchants to mean "all is OK." Nor should merchants be less vigilant vis-à-vis their antifraud and risk mitigation efforts.
- Merchants should take advantage of this lull to stay on top of and improve their security programs in every market, especially as fraudsters become more sophisticated in their security attacks.
- Merchants need to identify specific areas of their businesses that are at risk and use the appropriate fraud prevention, detection, and resolution models, techniques, and tools.
- The most lucrative areas of growth — international, mobile, and e-commerce — also represent high-risk areas for fraud; expansion must be supplemented by protection.
- Merchants have an opportunity to build a better relationship with their customers by enhancing their security measures and remaining competitive with other businesses.

5 Steps to a Safe Expansion:

1. Make strategic investments in tools and technologies to ensure a safe growth into new markets.
2. Develop "secure" processes by working closely with your issuer or acquirer for international transactions.
3. Ensure your fraud strategy includes solutions that address the specific risks facing international and mobile orders.
4. Develop joint "antifraud" programs with your issuer/acquirer to increase your effectiveness.
5. Educate both your employees and consumers about fraud prevention.

Methodology

In May 2011, LexisNexis Risk® Solutions retained Javelin Strategy & Research to conduct the third annual comprehensive research study on U.S. retail merchant fraud. LexisNexis conducted an online survey using a merchant panel comprising 1,006 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 +/-3.1 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 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.

In this year's study, we calculated the true cost of fraud using a three-year rolling average to account for macroeconomic variation and improvements in weighting methodology. In last year's 2010 retail merchant study, a two-year rolling average was applied.

For the dollar calculations of reported fraud loss, outlier values were excluded using a 5% trimmed mean for each employee size category. Overall merchant totals represent both industry and employee size weights.

Figure 23: Calculation for 2011 Fraud Losses

		0 to 4	5 to 9	10 to 19	20 to 99	100 to 499	500 to 999	1,000 to 2,499	2500+
		59%	21%	11%	8%	1%	0%	0%	0%
		NUMBER OF EMPLOYEES							
		0-4	5-9	10-19	20-99	100-499	500-999	1,000-2,499	2500+
TOTAL:	693,137	407,203	143,708	77,815	53,521	8,624	849	589	828
AVG. COST OF FRAUD:		$4,438	$2,233	$104,168	$213,325	$548,273	$1,356,774	$968,938	$15,059,782
ESTIMATED TOTAL COST OF FRAUD IN BILLIONS OF $:	$40.6	$1.81	$0.32	$8.11	$11.42	$4.73	$1.15	$0.57	$12.47
Three year rolling average = ($191.30B + $75.04B + $40.6B)/3 years = $102.31B									

2010 Javelin Identity Fraud Survey

The Javelin Identity Fraud Survey Report on a survey conducted in 2010 provides consumers and businesses an in-depth and comprehensive examination of identity fraud in the United States based on primary consumer data.

Survey Respondents

In all, 5,004 consumers, representative of the U.S. population, were interviewed via a standardized 49 question telephone survey to develop accurate and actionable insight into this pervasive and costly crime.

The polling yielded interviews with 466 fraud victims. After Javelin weighted the responses to standardize them to national demographics, the 2010 survey's computed number of victims interviewed was 470.

Survey Data Collection

Javelin employed Opinion Access for this survey's data collection. Opinion Access, one of the nation's leading data collection providers, is recognized as a reputable data collection service firm with over 15 years of experience in the industry. Opinion Access was responsible for collecting the data, and Javelin was responsible for the survey design, data weighting, data analysis, and reporting. The study was conducted through interviews administered by telephone with 5,004 U.S. adults over age 18 and a sample that is representative of the U.S. census demographics distribution. Data collection began Sept. 24, 2010, and ended Nov. 4, 2010.

Margin of Error

For questions answered by all 5,004 respondents, the maximum margin of sampling error is +/ 1.4 percentage points at the 95% confidence level. For questions answered by all 470 identity fraud victims, the maximum margin of sampling error is +/ 4.5 percentage points at the 95% confidence level. For questions answered by a proportion of all identity fraud victims, the maximum margin of sampling error varies and is greater than +/ 4.5 percentage points at the 95% confidence level.

APPENDIX

LexisNexis Fraud Multipliers

Figure 24: Merchant Benchmarks

	All Merchants	Company size			Large e-commerce
		Small	Medium	Large	
Fraud Multiplier	2.3	2.7	2.0	2.3	2.2

	All Merchants	Channels				Products		
		Physical Store	Multi-channel	Mobile	Online only	Digital Goods	Physical Goods	Both
Fraud Multiplier	2.3	2.0	2.3	2.0	2.4	2.1	2.2	2.2

Improvement in the Calculation for True Cost of Fraud in 2010

In the 2010 study, the primary driver for altering the methodology for calculating the true cost of fraud was a concerted effort to more closely measure the comprehensive picture of fraud for merchants overall. Small retailers (those with fewer than 100 employees) were analyzed at a much more granular level than in 2009, leading to greater insight of the fraud losses experienced by even the smallest retail merchants. Because of the addition of more rigorous methods for measuring fraud at smaller merchants, it is now known that this segment suffers 57% fewer fraud losses than estimated under the original methodology.

This year, average fraud losses for merchants of employee sizes 1 to 4, 5 to 9, 10 to 19, and 20 to 99 were weighted individually (see Figure 24). In 2009, the average dollar fraud losses for merchants of employee size 1 to 99 was aggregated and weighted by the number of merchants according to the U.S. Economic Census. Because the majority of U.S. retail merchants are small-scale operators with low average fraud losses, the change to the methodology used in 2010 caused the results to reveal a reduction in total fraud. Weighting by industry distribution was also included in 2010. We excluded outlier values for fraud losses using a 5% trimmed mean for each employee size category.

Your Javelin Contact

Luke Albertalli
Executive Relationship Manager
Javelin Strategy & Research
+1 925 225-9100 x 26 (Office)

For More information

Call: 866.818.0265
Email: retailfraud@lexisnexis.com
Web: www.lexisnexis.com/risk/retail-ecommerce