

2010 LexisNexis® True Cost of Fraud Study



Research provided by Javelin Strategy & Research

Table of Contents

Introduction	5
Merchant Definitions	6
Key Takeaways.....	7
Overview.....	10
The Impact of Fraud on Consumers	10
Costs of Consumer Fraud	10
Existing Card Fraud Among Consumers	14
The Effects of Data Breaches on Consumers.....	17
The Impact of Fraud on Financial Institutions	18
Components of Financial Institutions' Fraud Cost.....	19
Current Trends in Payments Fraud.....	21
Financial Institutions' Fraud Mitigation Efforts	22
US Retail Merchants: Fraud Losses Overview	24
LexisNexis Fraud Multiplier and Merchant's Cost of Fraud.....	24
Merchant Detailed Findings: Type of Fraud.....	27
Merchant Detailed Findings: Friendly Fraud.....	29
Merchant Detailed Findings: Payment Methods	30
Spotlight on Merchant Segments	32
Merchants Accepting Payments Through the Mobile Channel	33
Large E-Commerce Merchants	35
Online-Only Merchants.....	36
Multichannel Merchants	37
Merchants' Use of Technology to Mitigate Online Fraud	39
Merchants' Level of Satisfaction with Fraud Solutions	41
Prioritizing Merchants' Fraud-Mitigation Needs.....	43
Recommendations.....	44
Methodology.....	47
Appendix	52
Contact	57

Table of Figures

Figure 1: Measures of the Impact of Fraud on Consumers, 2003-2009.....	10
Figure 2: Impact of Fraud on Victims' Behaviors, 2010	11
Figure 3: Consumers' Perceptions of Personal Information Safety While They Shop Online, 2010.....	12
Figure 4: Consumers' Losses by Fraud Type, 2005-2009	14
Figure 5: Existing Card Fraud by Type: Mean and Median Fraud and Consumer Costs, 2009	15
Figure 6: Existing Credit and Debit Card Fraud, 2009.....	16
Figure 7: Top 25 Card Issuers Ability to Meet Javelin's Criteria for Prevention, Detection, and Resolution in Consumer-Facing Security, 2010.....	25
Figure 8: Fraud Multiplier for Merchants by Annual Revenue Size	24
Figure 9: Fraud Multiplier for Merchants By Industry Segment	25
Figure 10: Merchants' Cost of Fraud by Responsibility Type, 2010	26
Figure 11: Merchants Reporting Increases in Major Fraud by Type, 2009-2010	27
Figure 12: Losses for Large E-Commerce Merchants by Fraud Type, 2010	29
Figure 13: Merchants' Average Fraud Losses by Payment Method, 2010.....	30
Figure 14: Merchants Reporting Increases in Fraud by Payment Method, 2009-2010	31
Figure 15: Fraud Transactions for Merchants by Segment, 2010.....	34
Figure 16: Fraud Against Large E-Commerce by Fraud Type, 2010	35
Figure 17: Losses for Online-Only Merchants by Fraud Type, 2010	36
Figure 18: Fraud for Multichannel Merchants by Channel, 2010.....	37
Figure 19: Fraud Against Multichannel Merchants by Fraud Type, 2010	38
Figure 20: Merchants' Use of Outsourced Fraud Technology, 2009-2010.....	40
Figure 21: Merchants' Satisfaction with Fraud Solutions, 2010.....	41
Figure 22: Merchant's Perception of the Effectiveness of Fraud Solutions, 2010	42
Figure 23: Merchant's Greatest Needs for Reducing Fraud, 2010.....	43
Figure 24: Calculation for the True Cost of Fraud, 2010.....	50
Figure 25: Merchant Benchmarks, 2010	53
Figure 26: Multichannel Merchants' Fraud Mitigation Efforts, 2010	56

About LexisNexis®

LexisNexis® is a leading global provider of content-enabled workflow solutions designed specifically for professionals in the legal, risk management, corporate, government, law enforcement, accounting and academic markets. LexisNexis originally pioneered online information with its Lexis® and Nexis® services. A member of Reed Elsevier, LexisNexis serves customers in more than 100 countries with more than 15,000 employees worldwide.

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions is the leader in providing essential information that helps advance industry and society. Building on the legacy of proven LexisNexis® services from the past 30 years, our cutting-edge technology, unique data and advanced scoring analytics provide total solutions that address evolving client needs in the risk sector while upholding high standards of security and privacy. LexisNexis Risk Solutions serves commercial organizations and government agencies and is comprised of several affiliated corporations, each offering premier customer-focused solutions. For more information, visit lexisnexis.com/risk.

About Javelin 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.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright 2010 LexisNexis Risk Solutions. All rights reserved.

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

2010 LexisNexis True Cost of Fraud Study

INTRODUCTION

The 2010 LexisNexis True Cost of Fraud Study is the second 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. Because retail merchants today are suffering exorbitant costs related 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.

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 re-delivering purchased items (including carrier fraud)

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

New to this year's study is the LexisNexis "fraud multiplier", which estimates the total amount of loss a merchant incurs based on the actual dollar value of a fraudulent transaction.

2010 LexisNexis True Cost of Fraud Study

MERCHANT DEFINITIONS

- *Small* merchants earn less than \$1 million on average in annual sales or have 1 to 99 employees.
- *Medium* merchants earn on average between \$5 million and less than \$50 million in annual revenue or have 100 to 999 employees.
- *Large* merchants earn \$50 million or more in annual sales or have 1000 or more employees.
- *Online-accepting* merchants accept payments through various channels including online.
- *Online only* merchants accept payments only via the online channel.
- *Physical* merchants accept payments through “brick-and-mortar” store locations.
- *Digital goods* merchants sell digital goods/services, such as music, games, and other electronic content.
- *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.

KEY TAKEAWAYS

2010 LexisNexis True Cost of Fraud Study

The 2010 LexisNexis True Cost of Fraud Study uncovered the six key findings in the following sections:

1) For every \$100 in fraudulent transaction, merchants are paying a “true” cost of \$310 in total losses (fraud multiplier effect of 3.1)

Merchants are not only suffering the loss from the fraudulent transaction but also shouldering associated costs for fees/interest and costs for replacing lost or stolen merchandise. The actual amount of the fraudulent transaction represents only a percentage of the total loss incurred by the merchant.

2) Fraud loss continues to be one of the most significant problems for large retail merchants

Large merchants saw higher rates of fraud than do medium-sized or small merchants. Large merchants' losses were more than double the average annual fraud loss of their smaller counterparts. Their high transaction volume makes them a prime target for fraud.

3) Planned growth into the mobile channel signals greater risk for merchants, indicating the need for effective fraud solutions covering all channels

Merchants accepting purchases through the mobile device saw the highest volume of fraudulent transactions; in a given month, these merchants are hit with 3,385 fraudulent transactions on average. Many large e-commerce merchants plan to begin accepting payment through the mobile device; 4 in 10 of them are considering accepting mobile payments in the next 12 months. Merchants that accept mobile purchases report more successful fraudulent transactions than do merchants in other channels, indicating a strong need for merchants to establish effective solutions to prevent fraud when they expand into the mobile space.

4) Retail merchants are losing approximately \$139 billion to fraud this year

The true cost of fraud for retail merchants in 2010 is estimated at approximately \$139 billion. A gradual improvement in economic

2010 LexisNexis True Cost of Fraud Study

conditions, a greater awareness of specific fraud threats and at-risk channels, and the increased success of effective fraud prevention solutions, especially among smaller merchants, helped decrease retail merchants' fraud losses in 2010.

5) Fraud not only affects consumer victims monetarily but also alters perceptions and behaviors which can have a significant impact on retail merchants

More than 1 in 3 consumers who were victims of fraud avoid certain merchants, 1 in 4 report they spend less money, and almost 1 in 3 report switching payment methods. Merchants must take an active approach to mitigating fraud to prevent the negative impact on consumer behavior and perceptions.

6) Building on a trend identified in 2009, merchants consider education and industry standards their greatest needs in fighting fraud

Continuing a trend from the 2009 study, improved education and information were specified as the greatest need for fighting fraud; more than 1 in 2 retail merchants consider it important. Merchants ranked industry standards and/or best practices as the second greatest need in reducing fraud losses.

2010 LexisNexis True Cost of Fraud Study

OVERVIEW

The financial impact of fraud is three-fold, affecting consumers, financial institutions and merchants. It is important to gain a holistic view of fraud as it affects each of these segments so as to better understand the cost of fraud for a U.S. retail merchant. The following sections provide a synopsis of the ways fraud affects these three key constituents.










THE IMPACT OF FRAUD ON CONSUMERS

Consumers are the least sophisticated of the three groups affected by fraud, but their success in preventing it is as important to financial institutions and merchants as it is to the consumers themselves.

Costs of Consumer Fraud

Overall, identity fraud caused \$54 billion¹ in losses for financial institutions, businesses and consumers (see Figure 1). Approximately \$5.5 billion is attributed specifically to consumer costs related to identity fraud in 2009. Consumer costs comprise the out-of-pocket costs borne by victims, consisting of unreimbursed losses, lost wages due to the time required for fraud resolution and possible legal fees associated with investigation and prosecution. In contrast to consumer costs, fraud amounts reflect the face value of the crime — essentially, what the criminal was able to obtain.

Figure 1: Measures of the Impact of Fraud on Consumers, 2003-2009

	Trend	Survey Report						
		2009	2008	2007	2006	2005	2004	2003
U.S. adult victims of identity fraud		11.2 M	9.9 M	8.1 M	8.4 M	8.9 M	9.3 M	10.1 M
Fraud victims as % of U.S. population		4.81%	4.32%	3.58%	3.74%	4.00%	4.25%	4.70%
Total one-year fraud amount		\$54 B	\$48 B	\$45 B	\$50 B	\$57 B	\$60 B	\$58 B
Mean fraud amount per fraud victim		\$4,841	\$4,858	\$5,509	\$5,955	\$6,436	\$6,507	\$5,736
Median fraud amount per fraud victim		\$750	\$750	\$750	\$750	\$750	\$750	\$750
Mean consumer cost		\$373	\$498	\$720	\$574	\$467	\$746	\$606
Median consumer cost		\$0	\$0	\$0	\$0	\$0	\$0	\$0
Mean resolution time (hours)		21	30	26	25	40	28	33
Median resolution time (hours)		5	5	5	5	5	5	5

© 2010 Javelin Strategy & Research

¹ 2009 Identity Fraud Survey Report, Javelin Strategy & Research, February 2009. Data from the 2010 Identity Fraud Survey uses consumer trends from 2009, while the LexisNexis True Cost of Fraud Study refers to merchant data from 2009-2010.

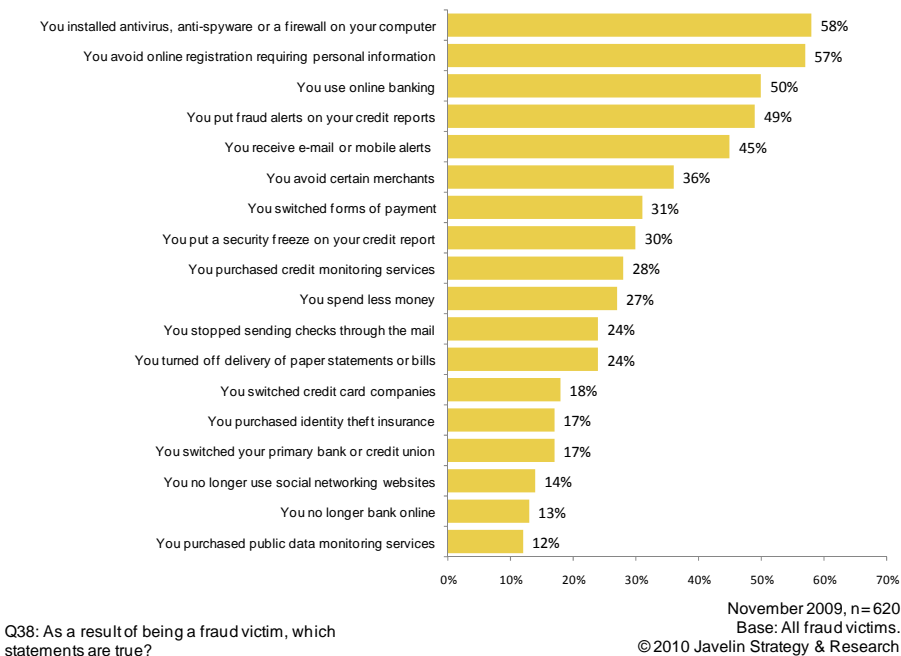
2010 LexisNexis True Cost of Fraud Study

Financial institutions and retail merchants continue to bear the majority of the fraud burden, striving to protect their reputations and brands by covering their customers. Most fraud occurs on existing card accounts; Regulation E of the Electronic Funds Transfer Act limits the liabilities of consumers with regard to unauthorized electronic funds transfers as long as fraud is reported in a timely manner.

Consequently, mean costs of consumer ID fraud continue to decrease, dropping from \$498 in 2008 to \$373 in 2009. Median consumer costs remain at \$0, as they have since 2003 because of zero liability card agreements.

Nevertheless, the impact of retail fraud is not just monetary — it in fact alters consumers' perceptions and behaviors, significantly affecting customers' relationships with merchants and financial institutions.

Figure 2: Impact of Fraud on Victims' Behaviors, 2010



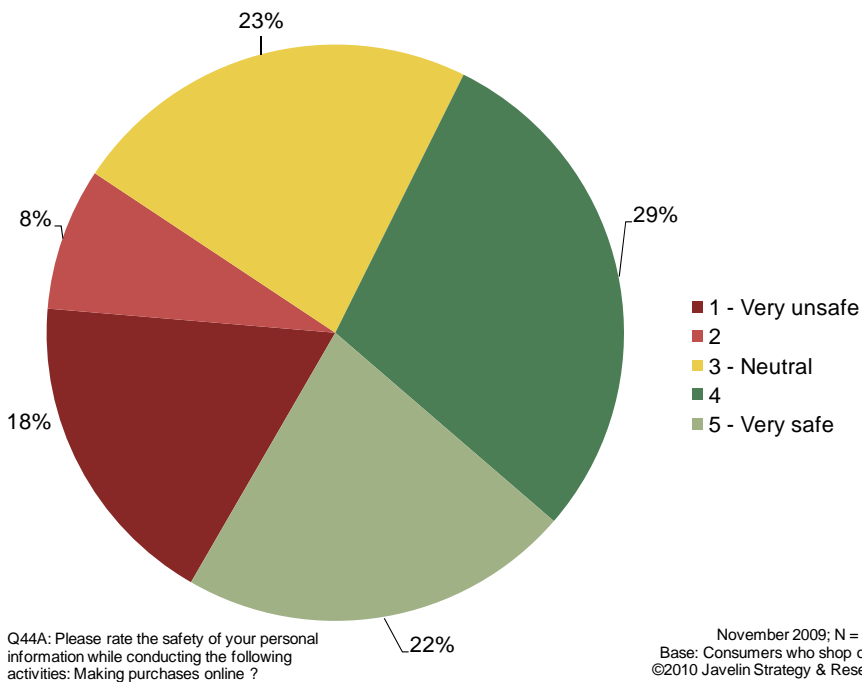
Fraud victims demonstrate a mixture of both positive and fear-driven reactions as a result of their experience (see Figure 2). Approximately 36% of victims report the intent to avoid certain merchants; 17% will change financial institutions (both issuers and primary banks); 27% report they will spend less money; and 31% will switch payment methods.

2010 LexisNexis True Cost of Fraud Study

In reality, criminals' growing focus on manipulating online and mail order/telephone order shopping methods is not necessarily mitigated when consumers simply avoid merchants that sell merchandise through remote channels. Compromised data on cards (credit or debit) as a result of a data breach could be used for fraudulent purchases regardless of the merchants a consumer chooses to avoid.

Fraud victimization also exacerbates existing negative perceptions of the Internet. Data shows that more than one in four consumers view their information as unsafe/very unsafe when shopping online, and another 23% are uncertain of online security.

Figure 3: Consumers' Perceptions of Personal Information Safety While They Shop Online, 2010



2010 LexisNexis True Cost of Fraud Study

The negative perceptions signal the need for merchants not just to educate their customers on how to protect their personal information, but to proactively demonstrate how they are working to secure payment information, especially in the online environment. It is important to note that victims of existing credit card fraud reported a large number of fraudulent online purchases (50% vs. 42% among all fraud victims), indicating elevated risk for fraudulent credit card purchases for merchants accepting purchases through the online channel.

Allowing merchants' web site security to be visibly robust to consumers will help to increase adoption of online shopping and improve consumer comfort levels with using payment methods online.

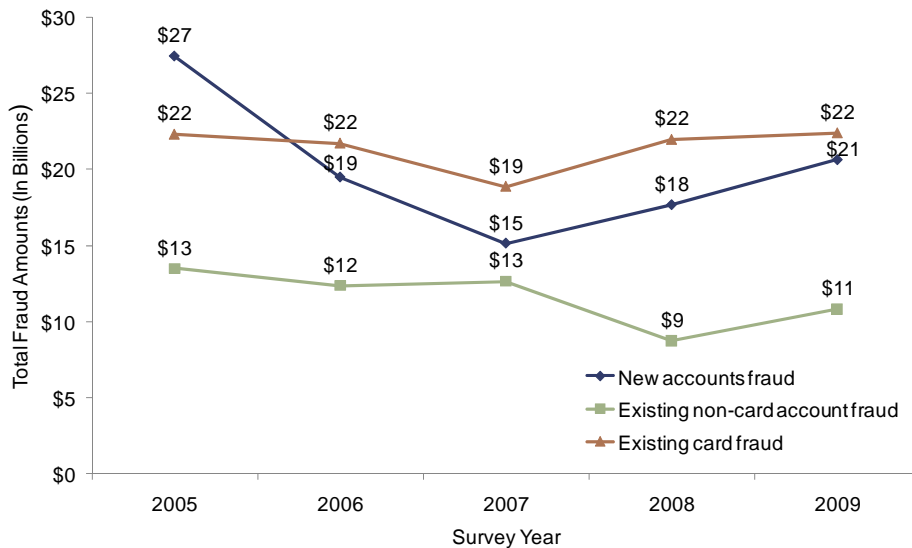
Merchants therefore have an opportunity to lessen the impact of fraud on consumers in a more hands-on manner, not only by implementing back-end fraud mitigation tools and processes but by engaging in more consumer-facing educational efforts. These include educating customers on ways to safeguard their payment information in the form of tips on web sites and informing customers about tools they can use for enhanced protection when shopping online (e.g., online purchase authentication).

2010 LexisNexis True Cost of Fraud Study

EXISTING CARD FRAUD AMONG CONSUMERS

Mirroring trends among merchants, again which most fraud is perpetrated through credit cards, the majority of fraud among consumers also occurs on existing card accounts (with an overall incidence of 2.8% among consumers). Therefore, this payment method becomes important to evaluate among consumers and merchants alike. In 2009, the volume of existing card fraud (credit or debit card) volume remained constant at \$22 billion, as Figure 4 shows, although sharp increases were observed in new accounts fraud (a type of fraud that more directly impacts financial institutions than retail merchants). The steady threat of existing card fraud points to a fundamental need for merchants to effectively validate card-based transactions at the point of sale.

Figure 4: Consumers' Losses by Fraud Type, 2005-2009



Q9: Did the perpetrator use your personal information to obtain new credit or debit cards, new bank accounts or loans in your name, or otherwise commit theft, fraud, or some other crime? Q8: Did the perpetrator use any of your existing accounts other than a credit or debit card account without your permission to run up charges or to take money from your accounts? Q5: Did the perpetrator misuse your existing credit, or debit card or account numbers to place charges on your account without your permission? Q3: Have you, yourself, ever been a victim of identity theft?

November 2009, 2008, 2007, 2006, 2005, 2004,
n= 5,000, 4,784, 5,075, 5,006, 5,000, 5,004
Base: All consumers.
© 2010 Javelin Strategy & Research

2010 LexisNexis True Cost of Fraud Study

As stated earlier, the majority of consumer fraud occurs on existing card accounts which hold the most benefit for criminals. The measures of impact are further analyzed below by card type: credit card fraud vs. debit card fraud.

Although the total amount for existing card fraud held steady last year, consumer costs (the out-of-pocket costs incurred by victims) for credit and debit cards signaled strong improvement from 2008 to 2009, dropping significantly from \$521² to \$314 for credit and \$545 to \$243 for debit (see Figure 5). This decline is the result of better monitoring of accounts by accountholders and FIs and the subsequent shorter periods of misuse (54 days) and detection (31 days).

Figure 5: Existing Card Fraud by Type: Mean and Median Fraud and Consumer Costs, 2009

	Mean fraud amount (dollars)	Mean consumer cost (dollars)	Mean resolution time (hours)	Median consumer cost
Debit	\$3,677	\$243	24	\$0
Credit	\$4,290	\$314	20	\$0
Existing Card Fraud	\$3,861	\$329	21	\$0

© 2010 Javelin Strategy & Research

Consumers habitually use debit cards more frequently than credit cards, although the differences are slight. When asked about the transactions conducted within the past seven days, 44% reported using a debit or prepaid card compared with 42% who reported using a network-branded credit card.

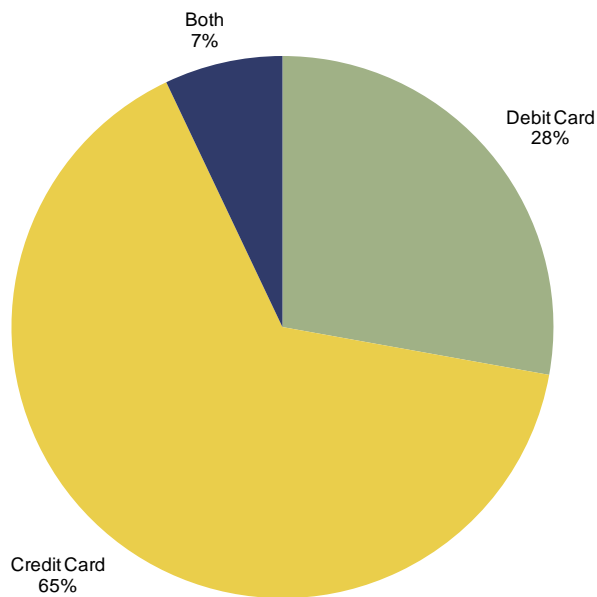
² Prior years' figures have been adjusted for inflation.

2010 LexisNexis True Cost of Fraud Study

Despite greater overall usage of debit cards, the incidence of existing credit card fraud showed a greater increase in 2009 to 2.8% from 2.1% in 2008. This is nearly twice as much as the incidence of debit card fraud, which rose slightly from 1.3% to 1.5%.

In 2009, there were 6.5 million victims of existing credit card fraud and 3.5 million of existing debit card fraud, representing 65% and 28%, respectively, of all existing card fraud (see Figure 6). These numbers further point to the continued fraud risk for retail merchants accepting these payment methods, a figure that will likely rise. Currently, 67% of all merchants accept credit cards, and 17% accept debit cards.

Figure 6: Existing Credit and Debit Card Fraud, 2009



Q6. Was the existing card or card number a credit, or debit card?

November 2009, n=389, 166, 42
Base: Existing card fraud victims.
© 2010 Javelin Strategy & Research

2010 LexisNexis True Cost of Fraud Study

The Effects of Data Breaches on Consumers

Before ending the discussion on consumer fraud, it is important to mention data breaches and their impact. Data breaches have also taken their toll on consumers, financial institutions and merchants; several high-profile compromises have resulted in tens of millions of misused accounts.

Data breaches can directly affect retail merchants as stolen payment card information is circulated, often through criminal organizations or rings, which use the stolen data in fraudulent transactions. Customer-authentication solutions provide an extra layer of security in helping detect and stop this type of fraud.

Criminals continue to become increasingly sophisticated and organized in their efforts to obtain payment card information and perpetrate fraud on a larger, more damaging scale. The LexisNexis True Cost of Fraud Study aims to encourage a similar level of synergy among the industry members that are responsible for resolving fraud, which include merchants, acquiring and issuing banks, payments networks, law enforcement agencies and regulators.

2010 LexisNexis True Cost of Fraud Study

THE IMPACT OF FRAUD ON FINANCIAL INSTITUTIONS

Financial institutions typically reported mean fraud losses of 2% to 3% of total payment card volume based on two years of research projections. These reports suggest financial institutions could be absorbing \$5 billion to \$11 billion in total fraud losses associated with resolving unauthorized retail transactions. Overall, in addition to the actual loss write-offs, FIs incur large operational costs from conducting investigations and communicating with customers as well as with blocking accounts and reissuing cards.

Financial institutions and retail merchants often have conflicting goals that get in the way of collaboration – a merchant's priority is achieving a hassle-free checkout process while a bank's priority is ensuring strong security - but both parties can benefit from sharing information to help reduce fraud.

Fraud losses would be lower for both merchants and financial institutions if they established a partnership for identifying payments security trends, improving merchant security practices, and sharing information on emerging fraud patterns.

FIs play two major roles in securing the flow of payment transactions: as the issuer of the payment card used by the consumer and as the merchant's payments "acquiring" bank. It is therefore important to understand the processes and perspectives of FIs in the fraud arena.

2010 LexisNexis True Cost of Fraud Study

Components of Financial Institutions' Fraud Cost

Existing association rules are mostly structured so that merchants win in card-present situations, and issuers win in mail order/telephone order (MOTO) and Internet situations. Although financial institutions absorb significant costs for several types of transactions, large card-not-present merchants generally do not. Losses associated with fraudulent transactions are absorbed by financial institutions in cases involving counterfeit cards, fraudulent applications, and any unauthorized activity that cannot be charged back to the merchant (namely, card-present transactions).

The card associations are responsible for establishing the fees related to chargebacks, and merchants accept less than the full value of the goods they sell due to the sales interchange process. Interchange discount rates typically range from 2% to 3%, depending factors such as sales volume and authorization practices. A portion of this interchange revenue goes to issuers to help absorb credit and fraud losses, a portion goes to acquirers to absorb their processing costs, and a portion goes to the associations (MasterCard, Visa and American Express) to absorb their infrastructure and processing costs. If merchants do not have the necessary fraud controls in place, they may face excessive chargeback penalties under association rules. However, penalties are usually not levied unless high chargeback rates continue for an extended period of time.

2010 LexisNexis True Cost of Fraud Study

According to financial institutions, the volume of chargebacks has grown so significantly in the past few years that issuing the chargeback amount back rather than process them all is a less costly option. The chargeback process can be arduous for both retail merchants trying to recoup fraud losses and the financial institutions that are trying to cover their customers. As more consumers make purchases online, both merchants and FIs must be prepared to handle the ever-growing frequency of chargebacks.

In addition to chargeback losses, retailers must grapple with the likelihood that customers who are victims of fraud will not return to their store or website. FIs face a similar cost that has just recently begun to be studied in the banking industry: customer attrition resulting from frustration with the fraud resolution process. This is typically categorized as a typically non-quantifiable loss because it focuses on customer loyalty. Most consumers have access to multiple credit cards, so it is important for issuers to provide good customer support and service when billing disputes and fraud disputes arise. Data showed that 18% of consumer fraud victims leave their issuer after becoming fraud victims. Most FIs have special processes in place for more timely dispute handling for high-value customers, and cardholders have the option of using their secure e-mail process for providing dispute documentation.

“Looking at the cost of processing charge backs over the last three or four years – the individual costs haven’t necessarily gone up. It has probably gone down, but the volume is getting so great that we do have to monitor those that we are almost letting go through because it does become sort of cost prohibitive to process them all” – Head of Fraud Operations, Top 20 FI

2010 LexisNexis True Cost of Fraud Study

Current Trends in Payments Fraud

According to FIs, the fastest growing card fraud types are counterfeit and card-not-present (MOTO/Internet). Counterfeit fraud is growing mostly because hackers are breaking into credit card information from merchant systems that are not secured (e.g., hacks from hotels, restaurants gas stations, and other merchants). All of the financial institutions interviewed unanimously highlighted data breaches as a major pain point and reported that data leakage incidents occurred at an alarming rate in the past year. Card-not-present fraud is another problem area for banks; Internet and MOTO fraud continue to grow because fraud perpetrators can operate remotely with limited risk of prosecution by law enforcement agencies.

Fraud perpetrators value gift cards because they can easily convert them to cash. Although gift cards are increasingly purchased and used by consumers and therefore targeted by fraudsters, prepaid card fraud is not measured through a unique merchant category code and is therefore difficult to quantify.

"I think consumers will get frustrated if they continue to be frauded on the same account or inconvenienced based on the amount of external data compromises that issuers have had to endure over the last couple of years. A lot of these people have their cards reissued two, three, four or five times and their angst and frustration gets levied on the issuer. "

– Head of Fraud Operations, Top 20 FI

2010 LexisNexis True Cost of Fraud Study

Financial Institutions' Fraud Mitigation Efforts

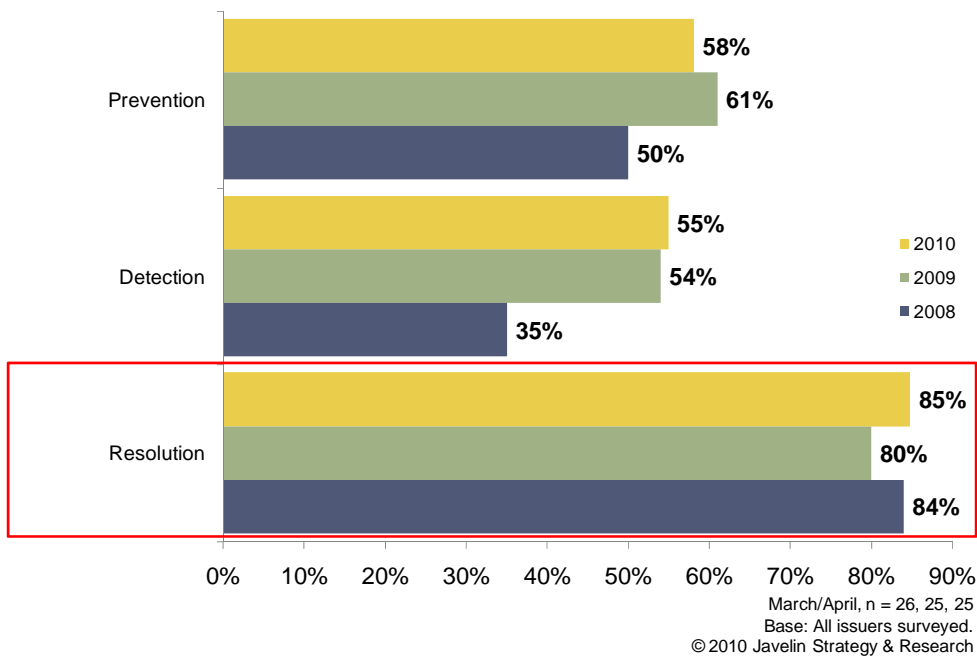
FIs have become increasingly effective at detecting fraud earlier in the process and have largely driven the reductions in fraud seen in the past year. Banks are mitigating fraud through four primary approaches: prevention, which comprises establishing technology and process controls to pinpoint fraud before it occurs; detection, which involves identifying suspicious and high-risk transactions and verifying activity with customers; resolution, which builds on payment network rules to reduce net fraud losses; and investigation, or working collaboratively with law enforcement to prosecute identity criminals.

Javelin research indicates the majority of banks excel at resolving fraud (see Figure 7), providing comprehensive services in customer care and making the fraud victim whole again. Zero-liability, 24x7 fraud reporting, dedicated resolution assistance and next-day replacement of cards are among the many recovery features offered to customers. Although FIs met only over half of the prevention and detection capabilities tested in Javelin research,³ they have in fact made vital strides on the *back-end*, proactively notifying customers of fraudulent activity on their accounts and seeing tremendous improvements in detection.

"Banks are real-timing more, utilizing other tools, getting better at analytics, and reducing the run-time. This is what's been driving the decrease in fraud. Although the case volume is going up, the dollars are going down." – Card Fraud Manager, Top 10 Issuer

2010 LexisNexis True Cost of Fraud Study

Figure 7: Top 25 Card Issuers Ability to Meet Javelin's Criteria for Prevention, Detection, and Resolution Criteria in Consumer-Facing Security, 2010



Financial institutions continually look for fraud prevention/identification tools that they can use to minimize fraud losses. Issuers are also enlisting the help of associations to manage counterfeit losses through improved merchant data security and other account data compromise initiatives and card-not-present fraud by adding more data elements (e.g., repeat customer, shipping cost, gift card use) to the authorization process to improve assessments of fraud risk.

2010 LexisNexis True Cost of Fraud Study

U.S. RETAIL MERCHANTS: FRAUD LOSSES OVERVIEW

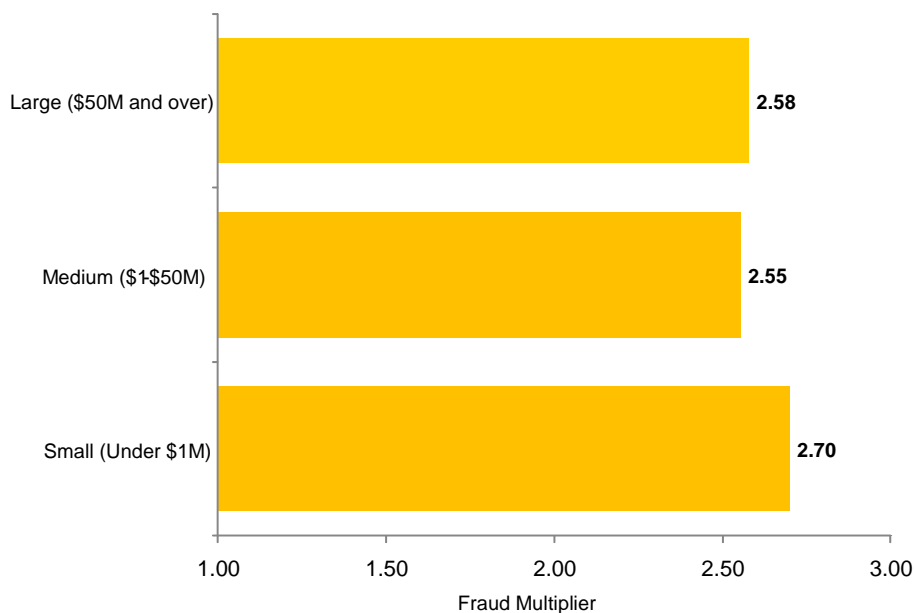
Retail merchants form the group that is most impacted by fraudulent transactions. The extent of their losses varies by size, business types, type of payments they accept, and other factors. LexisNexis has devised ways to measure the real cost of fraud to their bottom line.

LexisNexis Fraud Multiplier and Merchant's Cost of Fraud

New to this year's True Cost of Fraud Study is the "fraud multiplier", which indicates the actual financial impact of a fraudulent transaction for a retail merchant. On top of the dollar value of the fraudulent transaction, merchants shoulder additional costs: fees and interest as well as costs for replacing lost or stolen merchandise. The total cost of fraud for merchants in 2010 is \$139 billion; merchants can now use the fraud multiplier to calculate their individual estimated total fraud losses or the "true" cost of fraud. For every \$1 of fraud, merchants on average are paying more than \$3.

The multiplier for small merchants is slightly higher at 2.70 than large or medium-sized merchants because they pay more to replace lost or stolen merchandise (see Figure 8). Larger merchants typically enjoy lower costs to replace merchandise based on lower inventory pricing.

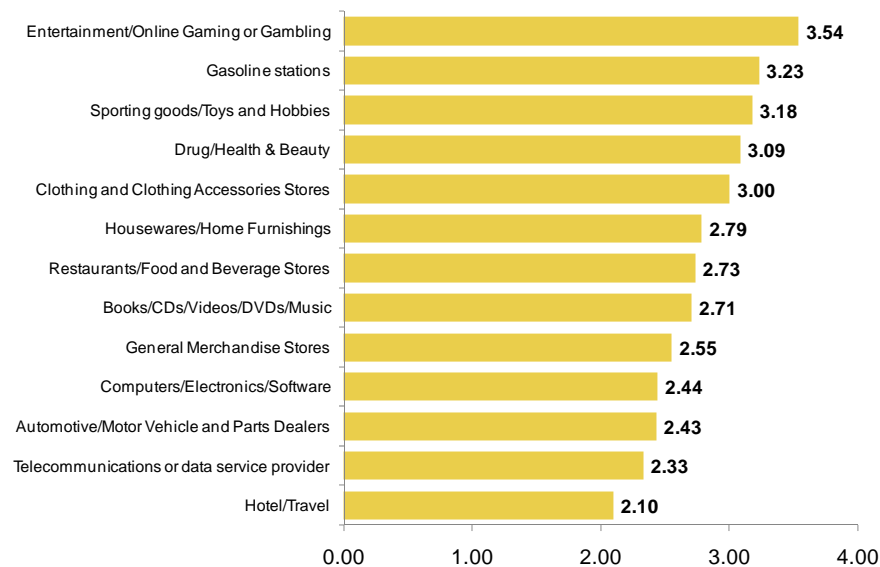
Figure 8: Fraud Multiplier for Merchants by Annual Revenue Size



2010 LexisNexis True Cost of Fraud Study

The multiplier does vary across industry segments, primarily because of the varying costs to replace lost or stolen merchandise for certain higher cost industries. Figure 9 shows the multipliers in various industries.

Figure 9: Fraud Multiplier for Merchants by Industry Segment



Q9: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud costs over the past 12 months. Note that the total must add up to 100%.

n = base varies by industry.
*industries with n < 30 shown
Base: All merchants experiencing fraud.

The following example illustrates the way the fraud multiplier helps determine loss from fraud: a merchant in the clothing industry, which has a fraud multiplier of 3.00, that suffers a fraudulent transaction of \$50 would have an estimated financial loss as a result of that fraud of $3.00 \times \$50$, or \$150. The additional costs result from paying to replace lost or stolen merchandise as well as paying fees and interest to financial institutions due to the fraudulent purchase.

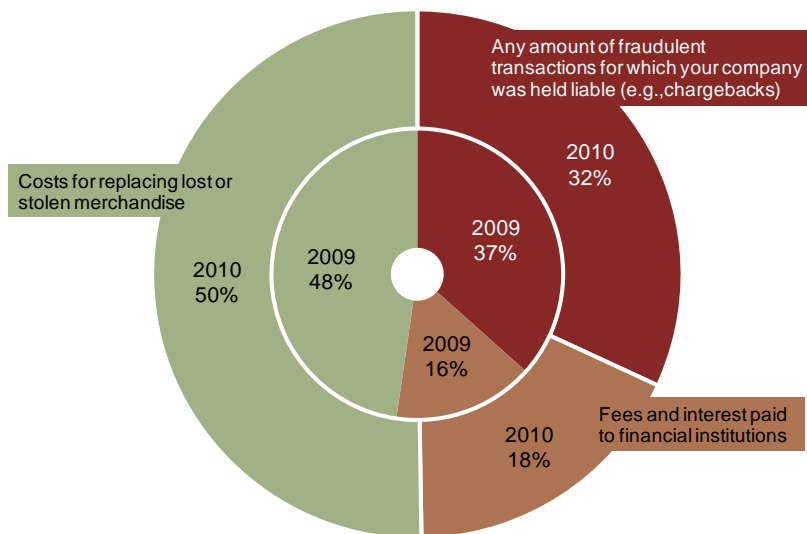
Merchants in the entertainment/online gaming or gambling sector and gasoline stations report the highest fraud multipliers at 3.54 and 3.23 respectively, while merchants in the hotel and travel business report the lowest multiplier at only 2.10. Data indicates that the online gaming industry has high losses because of the easy conversion to cash from fraudulent bets or wagers using stolen card information as well as false chargeback claims due to gambling problems; this often results in higher losses compared to the original fraudulent transaction amount. Gasoline stations may suffer disproportionately high losses because of the inability to monitor criminals who generally purchase valuable commodities outside of merchants' physical location, combined with costly problems related to skimming. Merchants reporting the lowest cost ratios include telcos and travel, two categories of merchants that may not need to actually replace a fraudulent purchase when fulfilling the criminal's order.

2010 LexisNexis True Cost of Fraud Study

Overall, retail merchants continue to account for the vast majority of the true cost of fraud because they are absorbing \$139 billion in total losses. Merchants are suffering nearly 25 times the out-of-pocket cost borne by consumer fraud victims. Factoring in the additional cost of covering lost/stolen goods, merchants are facing greater losses because they have the additional costs of reimbursing customers, replacing and/or redistributing merchandise and paying chargeback fees to banks.

On average, unauthorized transactions and chargeback fees/interest accounted for half (50%) of losses attributed to fraud; the additional 50% were attributed to costs for replacing or redistributing lost or stolen merchandise (see Figure 10).

Figure 10: Merchants' Cost of Fraud by Responsibility Type, 2010



Q9: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud costs in 2009.

July 2010, n = 1006, 1009
Base: All merchants.

2010 LexisNexis True Cost of Fraud Study

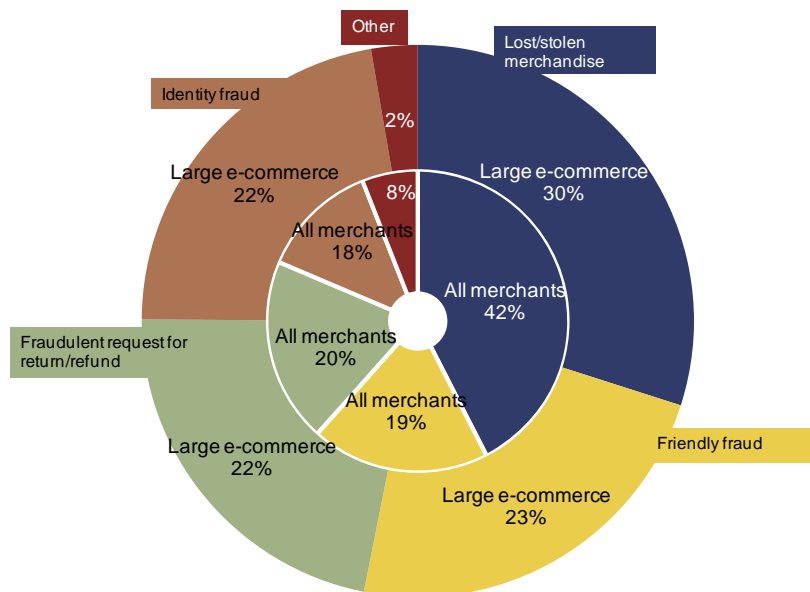
Detailed findings presented in subsequent sections review trends among overall U.S. merchants while maintaining a focus on specific merchant segments, where relevant. This specialized focus is important since overall US merchants' trends often reflect those of smaller merchants, which outnumber their larger counterparts in the US economy. Trends among specific merchant segments (such as large, e-commerce, mobile, multichannel) thus deserve spotlighting to truly portray the various aspects of retail fraud.

Merchant Detailed Findings: Type of Fraud

Results from the 2010 LexisNexis True Cost of Fraud study show that 20% of merchant fraud losses are attributed to friendly fraud, 42% to lost or stolen merchandise, 18% to identity fraud, and 20% to fraudulent requests for a return/refund (see Figure 11).

Overall this year, U.S. retail merchants did not report an increase for most of these fraud types; the most notable drops recorded were for identity fraud and friendly fraud.

Figure 11: Losses for Large E-Commerce Merchants by Fraud Type, 2010



Q10) Please indicate, to the best of your knowledge, the percentage distribution of the following fraud methods below, as they are attributed to your total annual fraud loss in 2009.

July 2010, n= 1006, 269
Base: All merchants, large e-commerce merchants.

2010 LexisNexis True Cost of Fraud Study

However, this decrease mostly reflects fraud trends among smaller merchants (which outnumber the larger merchants in the U.S. retail population). In individual merchant segments, important variations in fraud trends must be noted:

- More than 1 in 4 retail merchants that sell both digital and physical goods reported an increase in identity fraud in 2009.
- Large merchants continued to see identity fraud's impact on their fraud losses as 1 in 3 of them reported an increase in the number of fraudulent transactions
- Thirty-percent of large e-commerce merchants also reported an increase in identity fraud, continuing a trend seen in the previous year's study that large merchants are primary targets for fraudulent retail transactions
- Almost 4 in 10 merchants accepting purchases through the mobile channel reported an increase in identity fraud

The trends listed above illustrate that identity fraud continues to loom as a concern for large, e-commerce, and mobile-accepting retail merchants. Large merchants in particular face higher fraud losses compared to medium-sized or small merchants because large transaction volumes ensure that they will continue to be a prime target for fraud.

As the consumer retail market gradually recovers and the number of transactions increases, merchants (especially the segments highlighted in this section) should take all necessary precautions in streamlining their operations and protect themselves from the constant threat of identity fraud. Use of fraud prevention solutions and stronger authentication at the point of sale are often the most effective mitigation tools to directly combat this constant threat.

2010 LexisNexis True Cost of Fraud Study

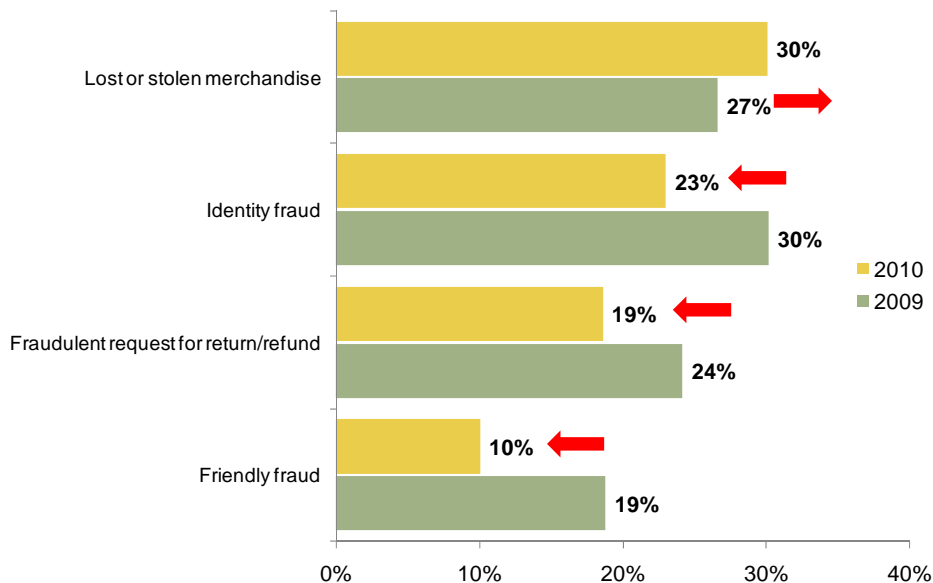
Merchant Detailed Findings: Friendly Fraud

Friendly fraud occurs when a consumer purchases an item online and receives the product but claims not to have received it, requesting a refund or chargeback from the merchant or delivery of a duplicate item. This type of fraud is often difficult to prevent unless the merchant can prove confirmation of receipt of the purchase. Typically, the chargeback requests lead to an investigation process and represent a growing threat for online-accepting merchants, specifically large e-commerce merchants that handle a large number of online purchases.

As shown in Figure 12, only 10% of all merchants reported an increase in friendly fraud in 2010 (compared to 19% in 2009). However, in examining specific merchant segments, significant differences emerge:

- One in five large merchants reported an increase in friendly fraud (compared to only 7% of small merchants and 16% of medium-sized merchants).
- Twenty-three percent of large e-commerce merchants reported an increase in friendly fraud which accounts for 23% of fraud losses for this merchant segment.

Figure 12: Merchants Reporting Increases in Major Fraud by Type, 2009-2010



Q11: Please indicate whether the incidence of each of the following fraud types has increased, decreased, or stayed the same during 2009. (select one only) EXCLUDING THOSE RESPONDING N/A

n = 1006, 1009.
Base: All merchants.

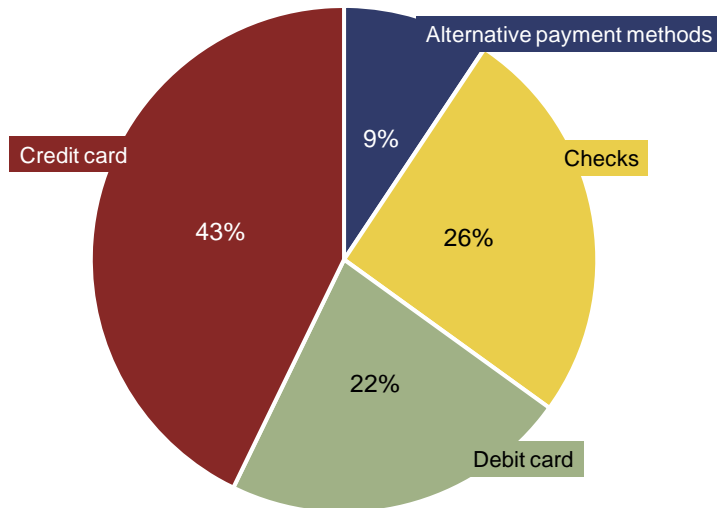
2010 LexisNexis True Cost of Fraud Study

To help prevent friendly fraud, merchants can require signature upon delivery and also use database profiles to determine valid addresses along with authentication solutions such as address-verification services.

Merchant Detailed Findings: Payment Methods

Credit card (followed by checks and debit card) continues to dominate retail payments fraud as in 2009. Credit card fraud accounts for 43% of fraud losses overall, on average, as Figure 13 shows.

Figure 13: Merchants' Average Fraud Losses by Payment Method, 2010



Q20) 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.

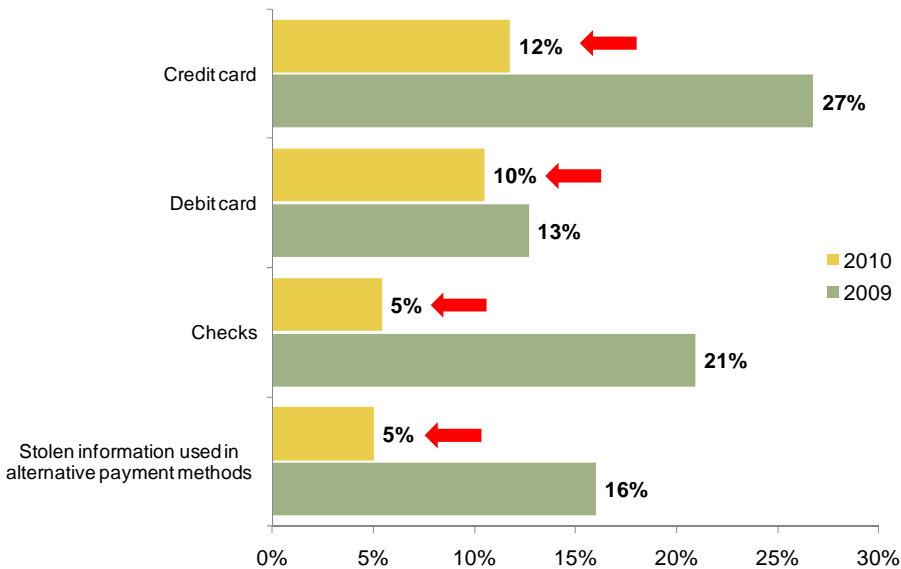
July 2010, n= 1006
Base: All merchants.

Fraud involving alternative payments is emerging as a significant fraud channel for smaller merchants. Although most small merchants as yet do not accept alternative payments, it is important to note that in the small subset that do, approximately 40% of fraudulent transactions are attributed to alternative payment methods.

2010 LexisNexis True Cost of Fraud Study

Although credit card fraud continues to be most pervasive, an important finding is that the incidence for fraud with credit cards, as with other payment methods, has not increased since last year. Only 1 in 10 retail merchants reported an increase compared to the nearly 3 in 10 indicating an increase in the previous year.

Figure 14: Merchants Reporting Increases in Fraud by Payment Method, 2009-2010



Q18: 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?

base varies by payment method accepted.
Base: All merchants.

Although the incidence of fraud related to credit cards and other payment methods does not appear to be on the rise, retailers must not overlook the persistent threat of fraud. Threats such as data breaches and international fraud rings often spring up unexpectedly, requiring merchants to constantly evaluate and improve their solutions for fraud prevention and detection.

SPOTLIGHT ON MERCHANT SEGMENTS

2010 LexisNexis True Cost of Fraud Study

The following sections reveal pertinent findings for four key merchant segments: merchants accepting payments through the mobile channel, large e-commerce merchants, online-only merchants, and multichannel merchants. Data shows these segments to be at the greatest risk of payments fraud.

MERCHANTS ACCEPTING PAYMENTS THROUGH THE MOBILE CHANNEL

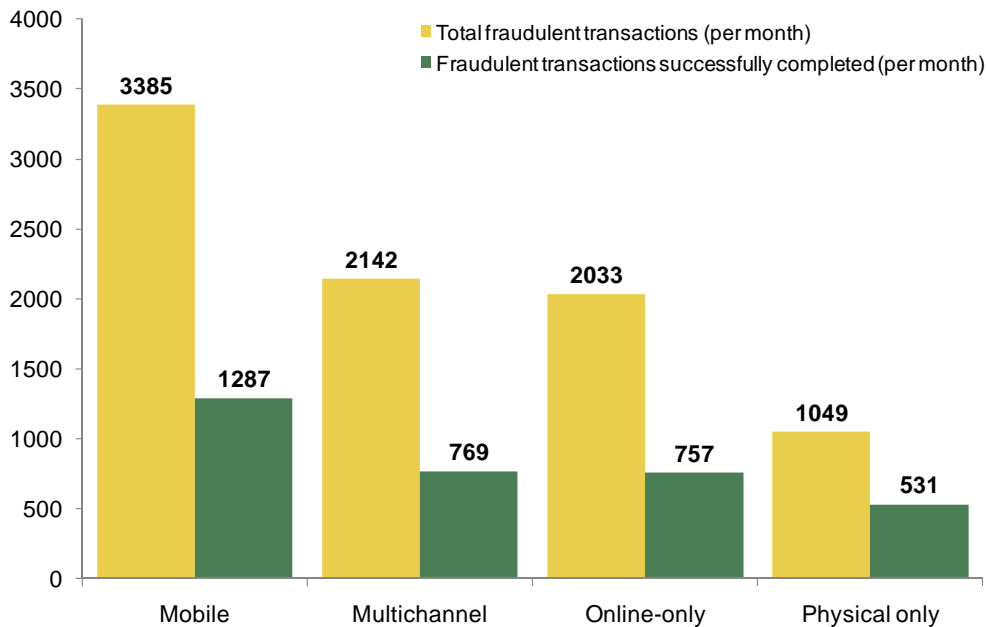
With the growth of smartphones and rapid development in mobile commerce applications, the mobile channel is a prime growth opportunity for retail merchants, especially those already operating an online store because growth into the mobile web is an easy transition. More than 6 in 10 merchants accepting purchases through mobile devices allow for purchases directly through the mobile browser.

However, additional risks accompany this still nascent payment channel because the security vulnerabilities of the mobile channel are not yet fully known. Currently, mobile exists strictly as an emerging fraud channel using traditional payment information (credit card, debit card, information used in alternative payments, etc.). As mobile wallet technology, in which all necessary payment information for purchases is stored on the handset, continues to gain momentum, it may open the mobile channel to greater risk of fraud in the future.

Merchants accepting mobile payment methods attributed 11% of fraudulent transactions to the mobile payments channel; 14% reported an increase in fraud perpetrated through this emerging channel. More than 1 in 4 (28%) merchants overall are considering accepting mobile payments in the next 12 months, indicating the potential for quick growth in this payment channel.

2010 LexisNexis True Cost of Fraud Study

Figure 15: Fraud Transactions for Merchants by Segment, 2010



Q12: In a typical month, approximately how many fraudulent transactions are prevented by your company? Q14: In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

n = 85, 367, 99, 98.
Base: Merchants by segment.

Mobile merchants saw the highest volume of fraudulent transactions; in a given month, they are hit with 3,385 fraudulent transactions on average (see Figure 15), and 38% of these transactions go through undetected - showing a strong need for effective fraud prevention solutions. Fraud losses as a percentage of total revenue were higher (1.13%) for mobile merchants than for online-only accepting merchants (0.83%) and multichannel merchants (0.86%). Although the volume of transactions completed through the mobile channel is small, the threat of fraud remains high for this channel which is primed for fast growth in the next year. Retail merchants must secure their online commerce channels using robust solutions for fraud prevention and detection before considering entry into the mobile channel.

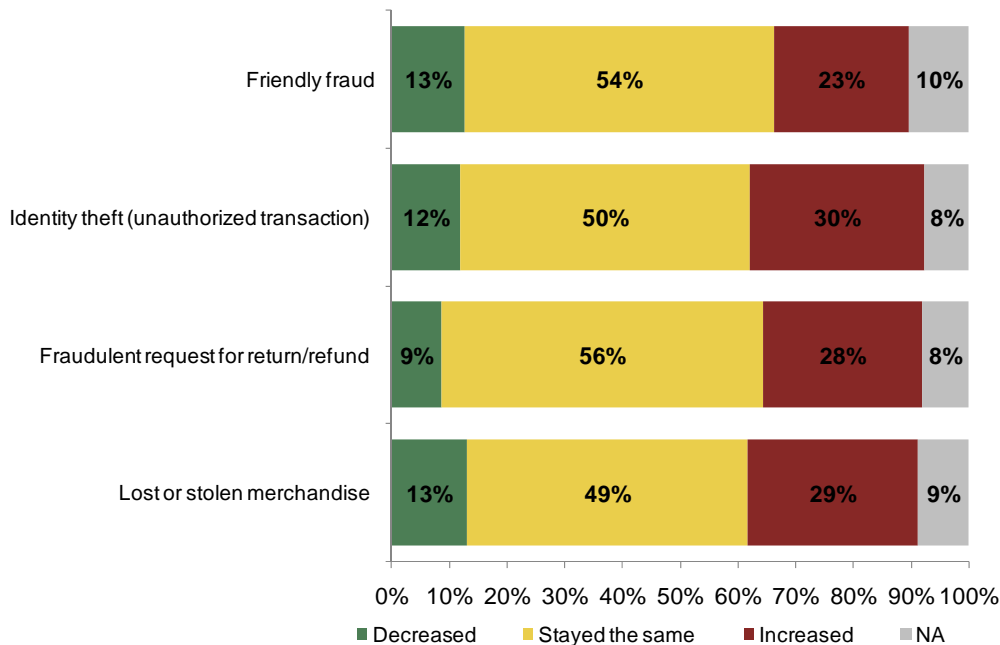
2010 LexisNexis True Cost of Fraud Study

LARGE E-COMMERCE MERCHANTS

Large e-commerce merchants have continued to see a high number of fraudulent transactions in 2010. In a given month, they are hit with 3,161 fraudulent transactions on average, 34% of which are going through undetected.

A significant percentage of large e-commerce merchants indicated an increase in several fraud types. As Figure 16 shows, in 2010, increases were observed in friendly fraud (23%), identity theft (30%), fraudulent request for return/refund (28%), and lost or stolen merchandise (29%). Although fraud decreased overall in 2010, large e-commerce merchants saw an uptick in unauthorized transactions, signaling the need for more robust online efforts in prevention and detection. Growth in e-commerce will continue to nurture criminals' appetite for card-not-present fraud, and large online merchants must be prepared for the growing sophistication of perpetrators' methods for both accessing and misusing stolen payment information on the web.

Figure 16: Fraud Against Large E-Commerce Merchants by Fraud Type, 2010



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

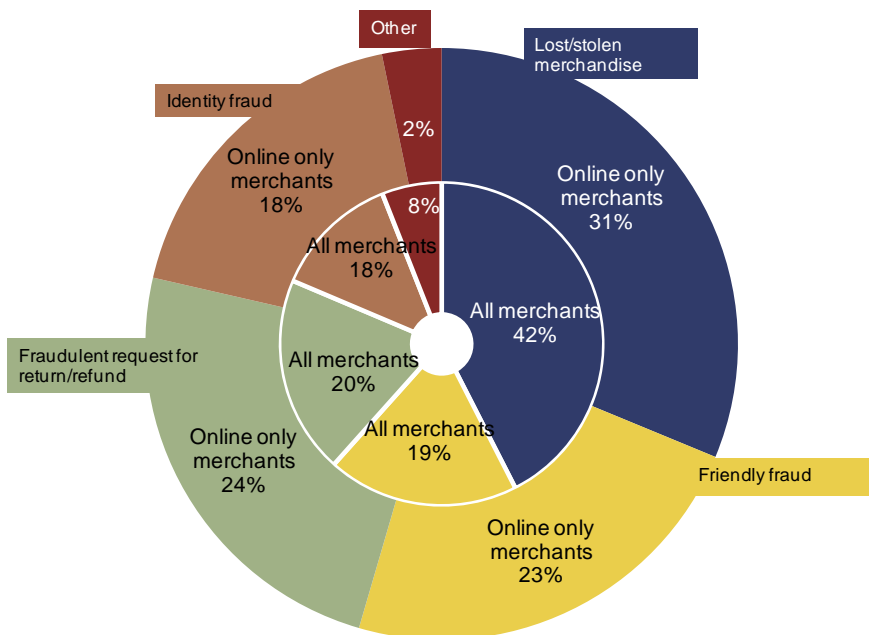
n = 268
Base: Large e-commerce merchants.

2010 LexisNexis True Cost of Fraud Study

ONLINE-ONLY MERCHANTS

Online only merchants incurred fewer fraud losses for lost or stolen merchandise than did U.S. retail merchants overall (see Figure 17) but attributed more losses to fraudulent requests for returns and refunds (24% vs. 20% for all merchants) and friendly fraud (23% vs. 19% for all merchants).

Figure 17: Losses for Online-Only Merchants by Fraud Type, 2010



Q10) Please indicate, to the best of your knowledge, the percentage distribution of the following fraud methods below, as they are attributed to your total annual fraud loss in 2009.

July 2010, n = 1006, 99
Base: All merchants, online only merchants.

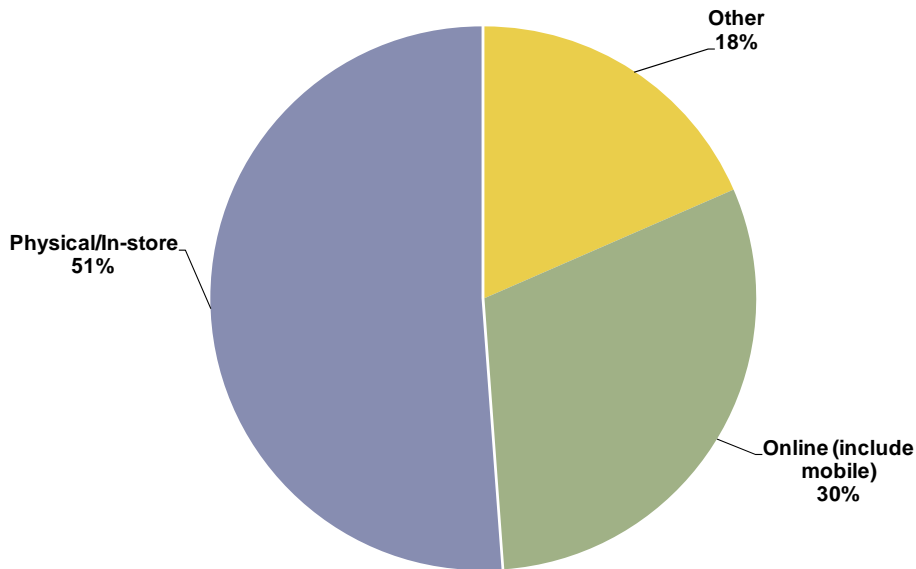
As with U.S. merchants overall, more online-only merchants partnered with external providers for their fraud detection solutions rather than develop an in-house proprietary solution or use a third-party vendor platform. Three in 10 online-only merchants outsourced transaction/customer profile databases, rules-based filters, automated transaction scoring, or online purchase authentication. Improved performance in preventing fraudulent transactions by outsourced solutions may have contributed to lower fraud losses overall while keeping merchants' investment in fraud-mitigation tools low.

2010 LexisNexis True Cost of Fraud Study

MULTICHANNEL MERCHANTS

Multi-channel retail merchants operate in both the physical “brick and mortar” and online channels but can operate through additional channels as well. Physical or in-store fraud accounts for the slight majority of fraud at multi-channel retailers (51%) while card-not-present transactions – both online and through mail/phone – accounts for the remaining 49% of fraud (see Figure 18).

Figure 18: Fraud for Multichannel Merchants by Channel, 2010



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?

n = 338.
Base: Multichannel merchants.

2010 LexisNexis True Cost of Fraud Study

As Figure 19 shows, 1 in 5 multi-channel merchants also observed increases in friendly fraud. Almost 1 in 3 saw an increase in unauthorized transactions, and more than 1 in 4 indicated suffering more fraudulent chargebacks (26%) and lost or stolen merchandise (28%). These numbers are not surprising, considering that multi-channel merchants maintain additional remote channels with which fraudsters can navigate, making them more vulnerable to cross-channel fraud.

Figure 19: Fraud Against Multichannel Merchants by Fraud Type, 2010



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

n = 368
Base: Multichannel merchants.

Retail merchants operating in both the physical and online channels must take all necessary precautions to secure payment channels and protect themselves from various fraud types without overlooking others. As both online and offline security threats continually adapt and evolve, merchants must remain vigilant in order to combat new and emerging fraud types.

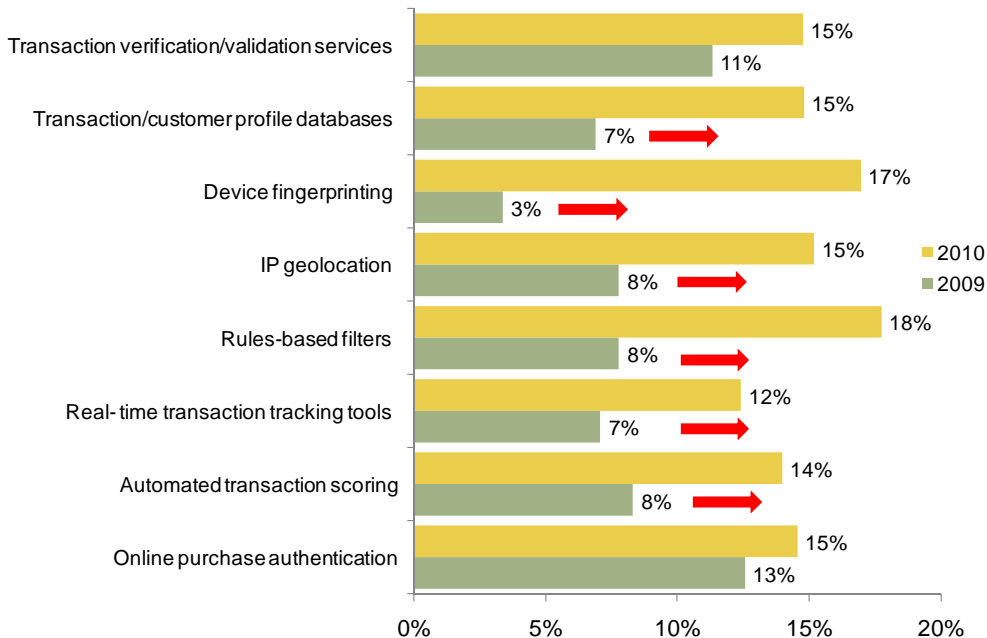
MERCHANTS' USE OF TECHNOLOGY TO MITIGATE ONLINE FRAUD

2010 LexisNexis True Cost of Fraud Study

Retail merchants should consider leveraging fraud solutions by using third-party providers rather than investing in and developing in-house solutions.

More merchants have leveraged fraud prevention solutions in 2010 than did in 2009 (see Figure 20). In 2010, the outsourcing of transaction and customer profile databases doubled (15% vs. 7% in 2009), device fingerprinting increased more than five-fold (17% vs. 3% in 2009), IP geolocation nearly doubled (15% vs. 8% in 2009), use of rules based filters more than doubled (18% vs. 8% in 2009), and real-time transaction tracking tools increased to 12% of merchants (vs. 7% in 2009). This emphasis on prevention, which holds the greatest impact in minimizing fraud losses, is in line with the overall industry-wide reduction in the total cost of fraud.

Figure 20: Merchants' Use of Outsourced Fraud Technology, 2009-2010



Q19: Does your company currently utilize any of the following fraud detection solutions? Please select one only. (We outsource this technology shown only)

n = 446.
Base: All online merchants.

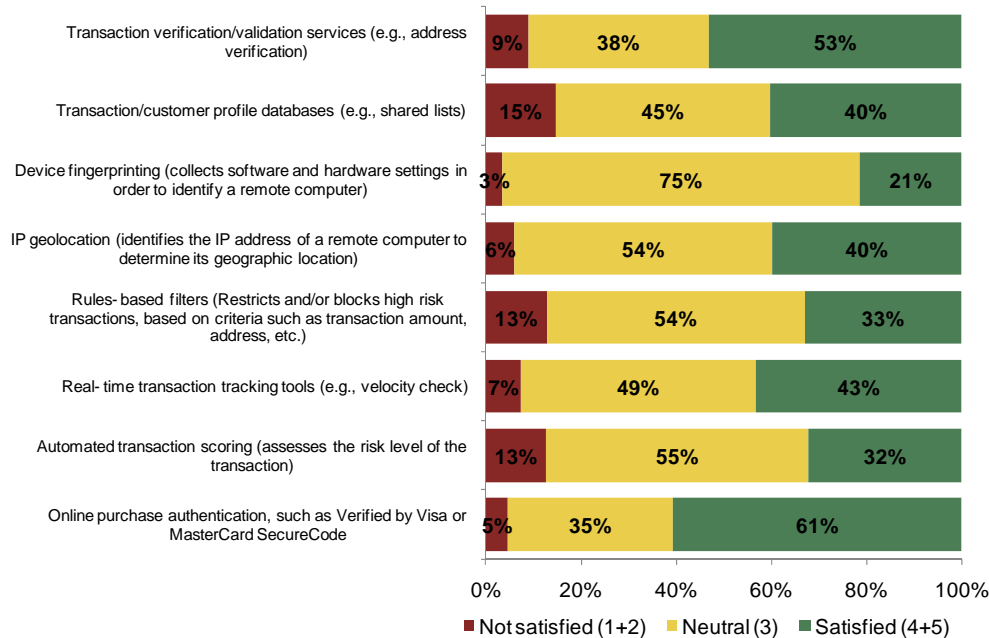
2010 LexisNexis True Cost of Fraud Study

MERCHANTS' LEVEL OF SATISFACTION WITH FRAUD SOLUTIONS

As Figure 21 shows, only two fraud-detection solutions – which also happen to be the two most widely used solutions among merchants – attained satisfaction ratings above 50%: transaction verification or validation (53%) and online purchase authentication (61%).

Merchant satisfaction with device fingerprinting garnered the lowest levels of satisfaction among methods for combating fraud, while other solutions fell into an overall moderate range of satisfaction.

Figure 21: Merchants' Satisfaction with Fraud Solutions, 2010



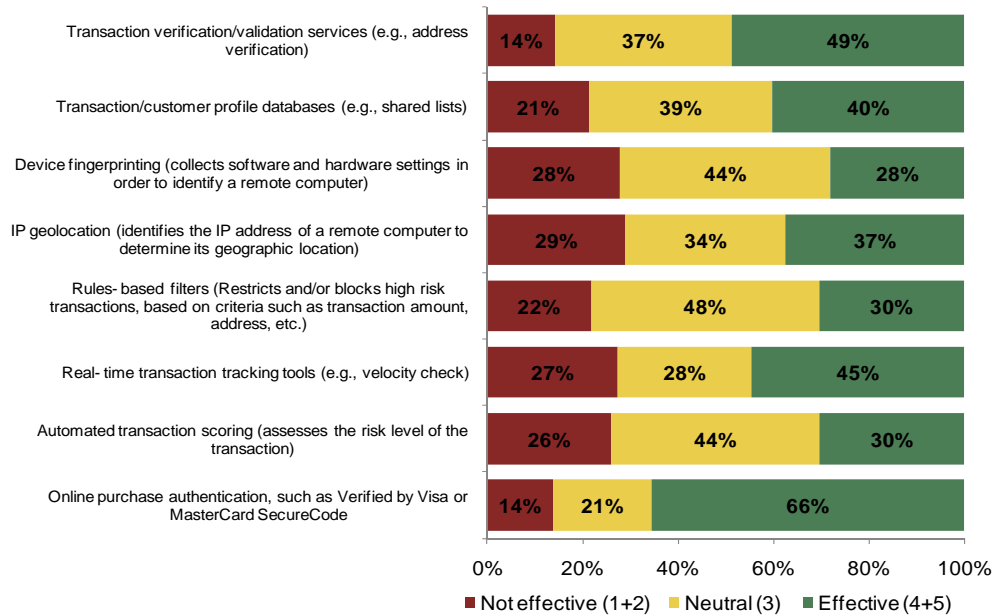
Q22: On a scale of one to five, please indicate your satisfaction level with your current fraud detection solution. Let one represent "not at all satisfied" and five represent "extremely satisfied".

base varies by merchants using the service.

2010 LexisNexis True Cost of Fraud Study

Not surprisingly, merchant ratings for effectiveness are similar to ratings for satisfaction. Only online purchase authentication received an effective rating above 50% (see Figure 22). Retail merchants give online purchase authentication higher marks in both effectiveness and satisfaction than they give to other fraud solutions although it has yet to be widely adopted because it requires an additional step in the purchase process.

Figure 22: Merchant's Perception of the Effectiveness of Fraud Solutions, 2010



Q23: On a scale of one to five, please indicate how effective you feel your current fraud detection solution is in reducing potential fraud losses. Let one represent "not at all effective" and five represent "extremely effective".

base varies by merchants using the service

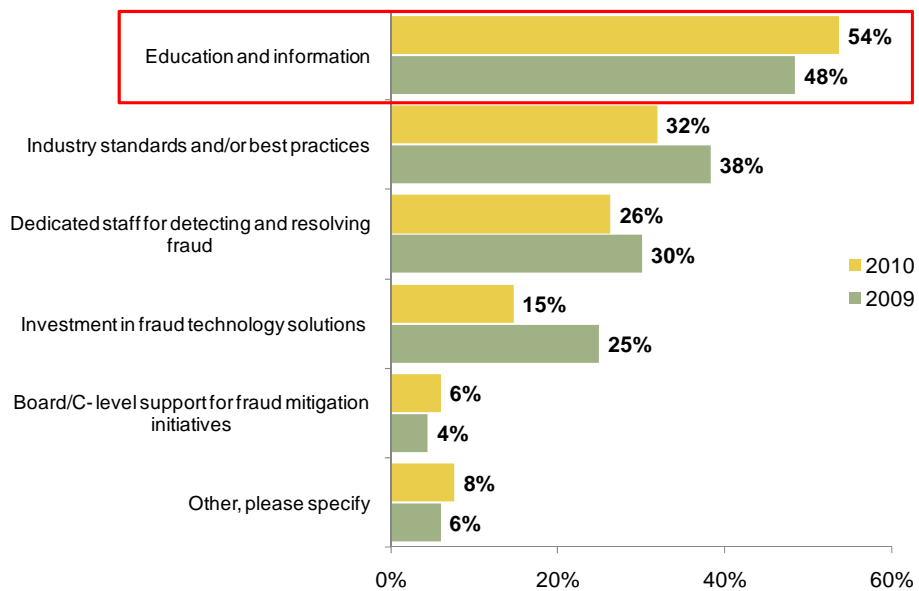
Low ratings in both satisfaction and effectiveness from merchants present an opportunity for solution providers to re-evaluate the performance of their existing solutions as well as partner with merchants to help them identify the most effective and cost-effective fraud-mitigation tools based on their specific fraud risks.

2010 LexisNexis True Cost of Fraud Study

PRIORITIZING MERCHANTS' FRAUD MITIGATION NEEDS

In 2010, 54% of merchants identified education as the primary need for reducing fraud losses (see Figure 23). Industry standards and best practices ranked a distant second as the second highest ranked need at 32%, down from 38% in 2009.

Figure 23: Merchants' Greatest Needs for Reducing Fraud, 2010



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

July 2010, n = 1006, 1009
Base: All merchants.

Although several resources for fraud information exist for consumers, merchants are left with few options in this area. Partnerships with industry trade groups or fraud solution providers could help to fill this gap in the future.

RECOMMENDATIONS

2010 LexisNexis True Cost of Fraud Study

Merchants can reduce their exposure to fraud and decrease losses by following the advice outlined below.

Determine the True Impact of Fraud

Use the LexisNexis fraud merchant multiplier to determine your true cost of fraud (or total financial impact). Based on your industry or the payment methods you offer, losses may be more or less damaging to your bottom line than previously anticipated. Accurately estimating these losses to fraud will allow you to correctly evaluate and address the need for the most effective solutions.

Secure All Other Channels Before Thinking Mobile

Now that mobile is quickly becoming one of the fastest-growing payment channels, merchants need to fully address fraud-mitigation tools present in all channels. Fraud threats from the mobile channel have still not been fully identified, though, so take all necessary precautions in securing all payment channels without overlooking any of them. Fraud threats adapt and evolve; merchants must be vigilant to stay one step ahead.

Look to Outside Fraud Solutions for Assistance

Development of in-house solution can be an arduous and costly undertaking even for the largest merchants. By using third-party solutions or outsourcing, you can save yourself the headache of managing the fraud-mitigation processes while still exploiting effective fraud prevention-measures.

Deputize Consumers in Helping Fight Identify Fraud

Financial institutions and credit card issuers have recently enabled consumers to monitor their personal accounts for any fraudulent activity using tools such as transaction or balance alerts. Security vendors have also joined the battle to fight fraud, offering antimalware software and educating consumers on new fraud threats. Merchants also have an opportunity to engage consumers in fraud education and prevention:

- Advise customers of new fraud threats such as phishing schemes and tell them how to identify non-secure web sites. Promote the use of antimalware such as antivirus software, firewalls, and anti-spyware. Instruct customers to keep their software up to date.

2010 LexisNexis True Cost of Fraud Study

- Inform consumers about the ways you secure their payment information throughout the purchase process.
- Instruct customers to regularly monitor their purchases using online banking and tools such as balance alerts. Advise them to report any irregular activity to their financial institution immediately.

Utilize Education/Best Practices Guidelines

Merchants can take advantage of industry resources for guidelines/standards in customer authentication, transaction verification and security of customer information. Taking a methodical step-by-step approach to preventing fraud can help close any potential loopholes or vulnerabilities across all payment channels.

METHODOLOGY

2010 LexisNexis True Cost of Fraud Study

In June 2010, LexisNexis Risk Solutions retained Javelin Strategy & Research to conduct the second 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 the 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 5000 US adults representative of age, gender, income and ethnicity was also utilized to ascertain the consumer cost resulting from fraudulent transactions.

In 2010, data was weighed according to the U.S. Census by both employee size and industry distribution. In the previous year's study, the 2009 totals were weighted *only* by employee size and used much broader employee size categories than those used in 2010. In 2009, the employee sizes used were as follows: 1 to 99, 100 to 499, 500 to 999, 1000 to 2499, and 2500 or more. In 2010, we divided the first category into four, and the employee sizes were: 1 to 4, 5 to 9, 10 to 19, 20 to 99, 100 to 499, 500 to 999, 1000 to 2499, and 2500 or more. 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. The data set was weighted to match the 2006 US Economic Census in order to better reflect the actual distribution by industry and employee size of the US merchant retail merchant population.

In this year's study, we calculated the true cost of fraud using a two-year rolling average to account for macroeconomic variation and improvements in weighing methodology. In the upcoming 2011 retail merchant study, a three-year rolling average will be applied to the figure for true cost of fraud.

2010 LexisNexis True Cost of Fraud Study

For the dollar calculations of reported fraud loss, outlier values were excluded via a 5% trimmed mean for each employee size category. Overall merchant totals represent both industry and employee size weights. All segment and industry data is reported unweighted, as was done in 2009.

Improvement in the Calculation for True Cost of Fraud

In this year's 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. Smaller 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 when 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 sizes 1 to 99 was aggregated and weighted by the number of merchants according to the U.S. Economic Census. Because the majority of retail merchants in the U.S. are small-scale operators with low average fraud losses, the change to the methodology 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.

Margin of Error/Data Weighting

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. The data set was weighted to match the employment size and industry type distribution from the 2006 U.S. Economic Census to better reflect the actual distribution of the U.S. retail merchant population. In the 2009 study, the data set was weighted only by employment size according to the 2006 U.S. Economic Census. Overall merchant totals represent both industry and employee size weights. All segment and industry data is reported unweighted, as was done in 2009.

2010 LexisNexis True Cost of Fraud Study

2009 Javelin Identity Fraud Survey

The *Javelin Identity Fraud Survey Report* on a survey conducted in 2009 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, 5,000 consumers, representative of the U.S. population, were interviewed via a standardized 50-question telephone survey to develop accurate and actionable insight into this pervasive and costly crime.

Figure 24: Calculation for the True Cost of Fraud, 2010

		NUMBER OF EMPLOYEES							
		0-4	5-9	10-19	20-99	100-499	500-999	1,000-2,499	2500+
TOTAL:	725,577	424,351	149,526	82,491	58,033	8,866	885	606	819
AVG. COST OF FRAUD:		\$436	\$16,871	\$182,057	\$596,606	\$1,820,691	\$3,701,064	\$11,290,057	\$8,733,788
ESTIMATED TOTAL COST OF FRAUD IN BILLIONS OF \$:	\$85.76	\$0.19	\$2.52	\$15.02	\$34.62	\$16.14	\$3.28	\$6.84	\$7.15
Two year rolling average = (\$191.30B + \$85.76B)/2 years = \$138.53B									

The polling yielded interviews with 828 fraud victims. After weighting the responses to standardize them to national demographics, the 2009 survey's computed number of victims interviewed was 703.

Survey Data Collection

Javelin employed Harris Interactive Service Bureau (HISB) for this survey's data collection. HISB, one of the nation's leading data collection providers, is recognized as a reputable data collection service firm with almost 50 years of experience in the industry. HISB was responsible for collecting the data and Javelin was responsible for the survey design, data weighting, data analysis and reporting. Previous studies employed Discovery and Synovate for all phases of data collection using computer-assisted telephone interviewing (CATI) via random-digit dialing (RDD). The study was conducted through interviews administered by telephone with 5,000 U.S.

2010 LexisNexis True Cost of Fraud Study

adults over age 18 and a sample that is representative of the U.S. census demographics distribution. Data collection began September 19, 2009 and ended November 29, 2009.

Margin of Error

For questions answered by all 5,000 respondents, the maximum margin of sampling error is $\pm 1.4\%$ at the 95% confidence level. For questions answered by all 703 identity fraud victims, the maximum margin of sampling error is $\pm 3.7\%$ 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 $\pm 3.7\%$ at the 95% confidence level.

APPENDIX

2010 LexisNexis True Cost of Fraud Study

Figure 25: Merchant Benchmarks, 2010

LexisNexis Fraud Multipliers 2010

	All Merchants	Company size			Large E-Commerce
		Small	Medium	Large	
Fraud Multiplier	3.10	2.70	2.55	2.58	2.53

	All Merchants	Channels				Products		
		Physical Store	Multi-channel	Mobile	Online only	Digital Goods	Physical Goods	Both
Fraud Multiplier	3.10	2.57	2.57	2.38	2.59	2.35	2.68	3.50

Fraud Loss by Company Size, Product Type, Channel and Industry, 2010

Company Size

Total Fraud Loss	Small	Medium	Large
Average annual fraud amount (\$)	\$2,145	\$104,000	\$6,767,000

Digital vs. Physical

Total Fraud Loss	Digital	Physical	Both
Average Annual Fraud Amount	\$952,000	\$2,534,000	\$2,923,000

2010 LexisNexis True Cost of Fraud Study

Channel

Total Fraud Loss	Online Accepting	Physical Store	Both	Other
Average Annual Fraud Amount	\$2,133,000	\$838,000	\$3,556,000	\$398,000

Industry

Total Fraud Loss	Computer/ Electronics	Food/Beverage Stores	Drug/Health & Beauty	General Merch.	Office Supplies	Telecom/ DSPs	Online Gaming
Average Annual Fraud Amount	\$2,006,000	\$3,768,000	\$3,794,000	\$2,302,000	\$5,442,000	\$3,227,000	\$275,000

Fraud Loss by Fraud Type and by Company Size, Channels and Products

Fraud Type/Method	All Merchants	Company size			Channels			Products		
		Small	Medium	Large	Physical Store	Multi-channel	Other	Digital Goods	Physical Goods	Both
Lost or stolen merchandise	42%	37%	35%	32%	41%	34%	39%	27%	38%	32%
Fraudulent request for return/refund	20%	21%	20%	24%	23%	21%	22%	21%	22%	21%
Friendly fraud	19%	21%	22%	19%	16%	22%	14%	24%	19%	22%
Identity theft	13%	13%	21%	21%	19%	20%	13%	21%	17%	21%
Other	6%	9%	2%	4%	0%	3%	12%	7%	5%	4%

Fraud Loss by Fraud Type for Large E-Commerce and Online-Only Merchants

Fraud Type/Method	All Merchants	Large E-Commerce	Online only
Lost or stolen merchandise	42%	30%	31%
Fraudulent request for return/refund	20%	22%	24%
Friendly fraud	19%	23%	23%
Identity theft	13%	22%	18%
Other	6%	3%	3%

2010 LexisNexis True Cost of Fraud Study

ROI

Fraudulent Transactions/Average Value of Fraudulent Transactions	All Merchants Outsourcing Fraud Solutions
Average volume of fraudulent transactions <u>prevented</u> in a given month	1445
Average value of prevented fraudulent transactions	\$247
Average volume of fraudulent transactions <u>successfully completed</u>	963
Average value of successfully completed fraudulent transactions	\$232

Fraudulent Transactions/Average Value of Fraudulent Transactions	Large Ecommerce Merchants
Average volume of fraudulent transactions <u>prevented</u> in a given month	2079
Average value of prevented fraudulent transactions	\$288
Average volume of fraudulent transactions <u>successfully completed</u>	1082
Average value of successfully completed fraudulent transactions	\$259

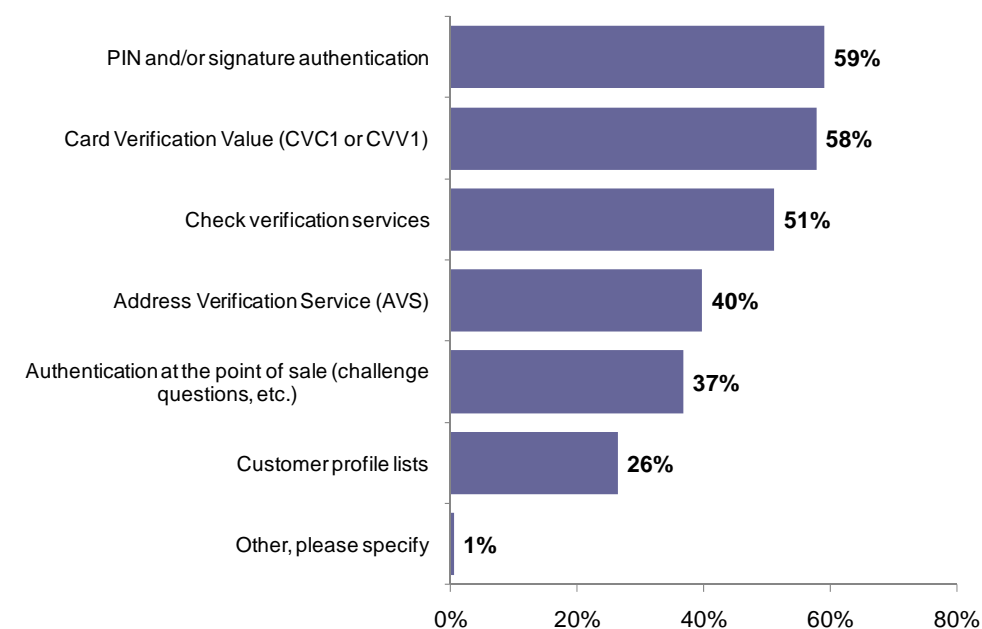
Fraudulent Transactions/Average Value of Fraudulent Transactions	Online Only Merchants
Average volume of fraudulent transactions <u>prevented</u> in a given month	1276
Average value of prevented fraudulent transactions	\$258
Average volume of fraudulent transactions <u>successfully completed</u>	757
Average value of successfully completed fraudulent transactions	\$204

2010 LexisNexis True Cost of Fraud Study

ROI (continued)

Fraudulent Transactions/Average Value of Fraudulent Transactions	Merchants Accepting Purchases Through the Mobile Channel
Average volume of fraudulent transactions <u>prevented</u> in a given month	2098
Average value of prevented fraudulent transactions	\$249
Average volume of fraudulent transactions <u>successfully completed</u>	1287
Average value of successfully completed fraudulent transactions	\$182

Figure 26: Multichannel Merchants' Fraud-Mitigation Efforts



Does your company currently engage in any of the following prevention solutions to mitigate fraud resulting from in-person transactions?

n = 367.
Base: Multi-channel merchants.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license.

Other products and services may be trademarks or registered trademarks of their respective companies. Copyright 2010 LexisNexis Risk Solutions. All rights reserved.