LexisNexis® Risk Solutions 2018 True Cost of Fraud℠ Study

Retail Edition

July 2018

LexisNexis®
RISK SOLUTIONS

The LexisNexis® Risk Solutions 2018 True Cost of Fraud℠ Study helps merchants grow their business safely even with the growing risk of fraud.

The research provides snapshots of current fraud trends in the United States and spotlights key pain points that merchants should be aware of as they add new payment mechanisms and expand channels into online, mobile, and international sectors.

How do I grow my business and manage the cost of fraud while strengthening customer trust and loyalty?

LexisNexis® RISK SOLUTIONS

The study included a comprehensive survey of 703 risk and fraud executives in retail organizations.

Fraud Definitions

- 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
- This research covers consumer-facing retail fraud methods
  - Does not include insider fraud or employee fraud
- The LexisNexis Fraud Multiplier℠ cost
  - Estimates the total amount of loss a merchant occurs based on the actual dollar value of a fraudulent transaction

Research was conducted in March 2018.

	Merchants with Digital Goods	Large ($50M+) Merchants with Digital Goods	Large ($50M+) Merchants with Digital Goods International	Large ($50M+) w/ e-Commerce	Large ($50M+) w/ m-Commerce	Large ($50M+) w/ e-Commerce International
# Completions	252	114	96	156	104	124

Merchant Definitions:

Earn <$1 million on avg. in annual sales.

Earn between $1 million to <$50 million on avg. in annual sales.

Earn $50 million+ in annual sales.

Merchants with an mCommerce channel

Accept payments through either a mobile browser or mobile application, or bill payments to a customer's mobile carrier.

Large merchants with an eCommerce channel

Accept payments through multiple channels but maintain a strong online presence, earning 10%–100% of their revenue from the online channel and earning $50 million+ in annual sales.

LexisNexis® RISK SOLUTIONS

Executive summary: Initial Key Findings

LexisNexis®
RISK SOLUTIONS

Key Findings

1

Retail fraud continues to increase sharply year-on-year, along with its cost.

- The average volume and value of fraudulent transactions has risen.
- And, the level of fraud as a percentage of revenues has moved upwards (1.58% to 1.80% on average).
- Each of these contributes to a rise in the LexisNexis Fraud Multiplier℠.

2

m-Commerce adoption grew as expected, among mid / large merchants selling digital goods **(from 57% to 70%).**

- Adoption is viewed as a means of growing the business – reaching new customers and providing an additional means for current ones to connect with the merchant.
- Many digital goods sellers also view mobile payments as a way to improve the customer experience and gain efficiencies via a faster transaction process.

3

But there is a cost. Mid / large m-Commerce merchants selling digital goods have higher fraud costs than others.

- Fraud cost represents an average 2.10% of mid/large m-Commerce digital goods merchants' annual revenues.
- And, every $1 of fraud costs these merchants an average of $3.29, which is a 24% increase over 2017.
- This is much higher compared to $2.78 for mid/large m-Commerce selling physical-goods only and mid/large physical-goods only merchants not allowing m-Commerce ($2.30 - $2.54)

LexisNexis® RISK SOLUTIONS

Key Findings (cont.)

4

Identity fraud remains a serious issue for retailers, particularly mid/large m-Commerce merchants selling digital goods.

- A significant degree (39%) of their fraud losses are attributable to identity theft, including from synthetic identities.
- Digital identity verification is a key challenge for these merchants, based on the volume of Botnet orders and rise of synthetic identities which take advantage of the "fast transaction" quality with digital goods.
- e-Gift cards, downloadable SW and digital subscriptions are prime targets.

5

Tracking fraud by both channel and payment method has increased. But, it is still not optimal, thereby contributing to fraud challenges.

- Larger remote merchants have increased their tracking of fraud by payment method; this has been a weak point in the past.
- And while many track successful fraud transactions, fewer are tracking where it has been prevented.
- This weakens the ability to manage fraud in its entirety.

6

Digital-goods selling merchants appear to have been investing in fraud prevention solutions during the past year. Yet, many struggle with identity fraud.

- The average number of solutions has increased most among mid/large m-Commerce merchants selling digital goods.
- Continued challenges are likely related to the types of solutions used. Findings indicate that those who layer identity authentication and transaction verification solutions to meet specific transaction environments have a lower cost of fraud.

The cost of fraud continues to rise.

LexisNexis®
RISK SOLUTIONS

Fraud success continues to outpace prevented fraud attempts.

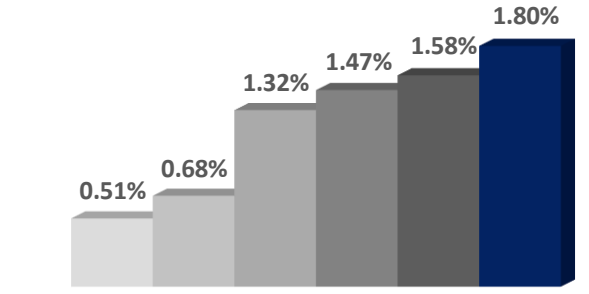
This impacts the degree of fraud losses as a percentage of annual revenue, which jumps by 13.9% over 2017 – continuing a sharp upward trend since 2015.

Key Indicators

Volume of Fraud Transactions

	2012	2013	2014	2015	2016	2017	2018
Avg. Transaction Value / Mo.	$120	$155	$114	$113	$146	$181	$184

Fraud as % Cost of Revenues



All Merchants

13.9% increase since 2017

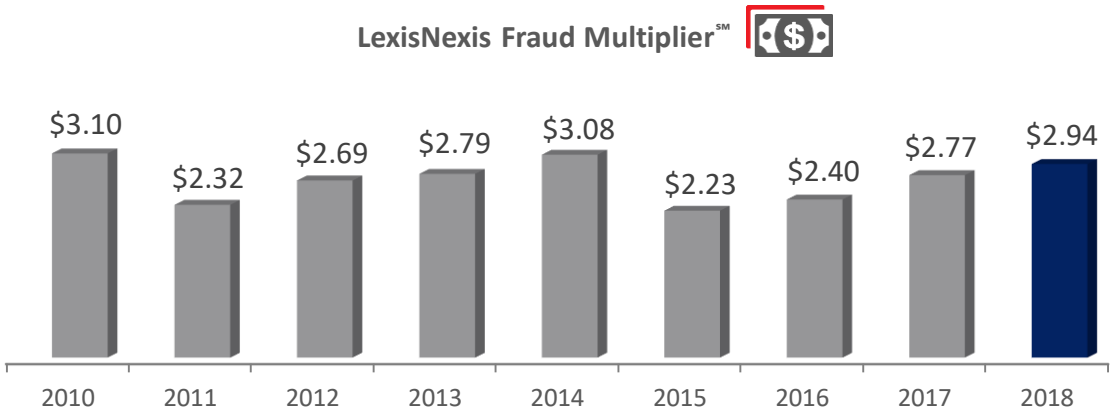
Q10: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud cost over the past 12 months.
Q22/23: In a typical month, approximately how many fraudulent transactions are prevented by your company? What is the average value of prevented transactions?
Q24/25: In a typical month, approximately how many fraudulent transactions are successfully completed at your company? What is the average value of successful fraud transactions?
Q11: What is the approximate fraud losses as a percent of total annual revenue.

LexisNexis® RISK SOLUTIONS

This also impacts the LexisNexis Fraud Multiplier℠, which continues its upward trend.

The cost for each dollar of fraud losses is up 6% from last year, at $2.94, which involves increased expenses related to chargebacks, fees, merchandise redistribution, labor/investigation, legal prosecution and IT/software security.

As shown later, the cost of fraud has risen based on a combination of factors. One, there has been an increase in the volume of fraud attempts / botnet activity. This relates to the second factor, which is an increased use of m-Commerce among digital goods sellers, where fraudsters have found success. And, thirdly, merchants using these remote channels have not optimally layered solutions to protect against unique threats from different channels (online, mobile) and transaction types.



Q16a: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.

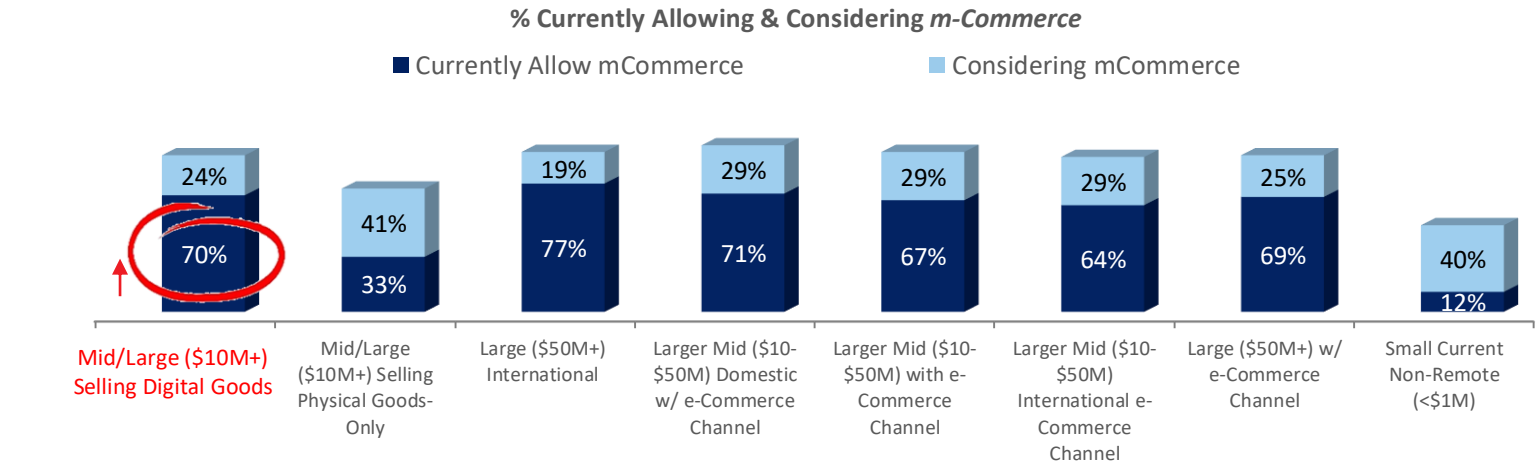
LexisNexis® RISK SOLUTIONS

The cost and volume of fraud is more severe for m-Commerce merchants that sell digital goods.

LexisNexis®
RISK SOLUTIONS

As predicted in previous waves of this study, m-Commerce growth continues to be driven by larger merchants selling digital goods.

This continues a trend of year-over-year double-digit adoption among mid/large digital goods merchants since at least 2016. In effect, these larger online merchants are now synonymous with mobile. Those selling only physical goods lag with m-commerce adoption.



2017	35%	30%	28%	20%	18%	14%	24%	41%
	57%	38%	70%	72%	70%	71%	72%	0%
2016	34%	44%	19%	55%	50%	38%	18%	23%
	35%	13%	63%	13%	29%	40%	62%	0%

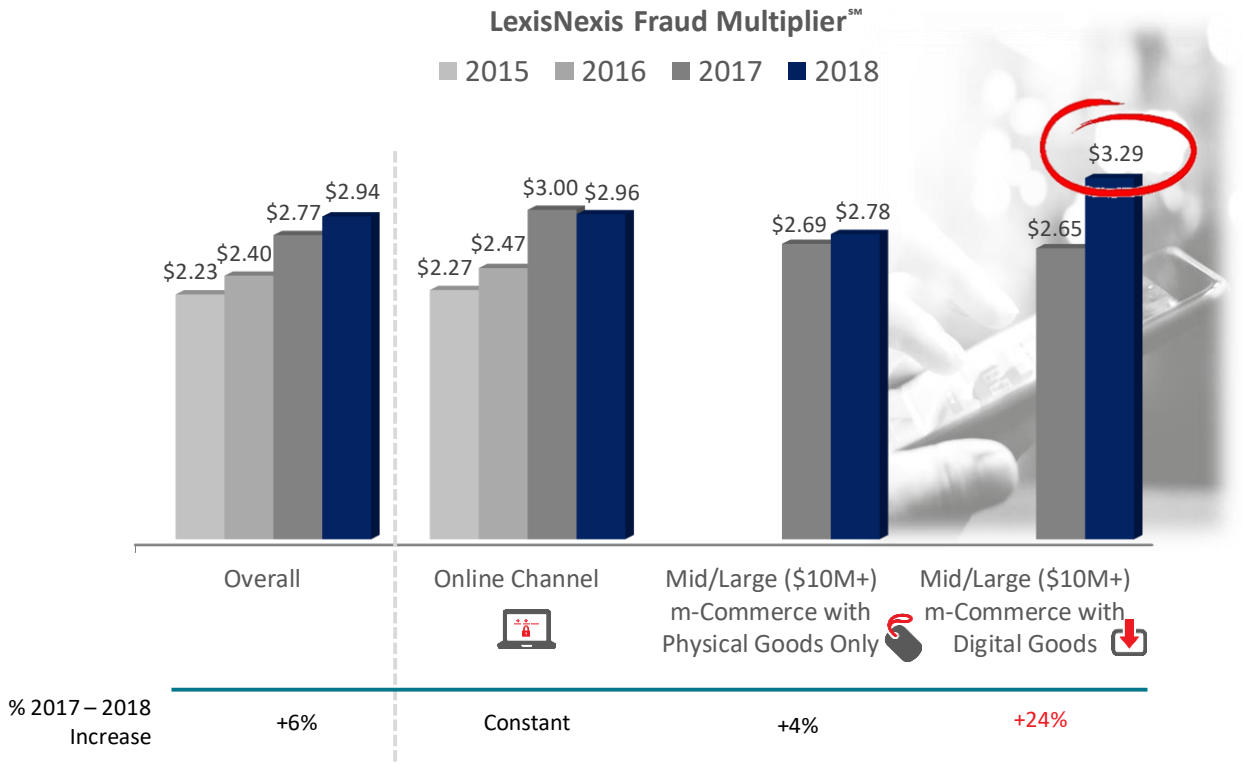
There has been a directional increase in adoption among large merchants selling internationally as well. This leaves smaller merchants as the next segment with the potential for m-Commerce growth. That said, they have been slower to adopt it during the past two years, even though they are considering it.

LexisNexis® RISK SOLUTIONS

*Not all who say "likely in next 12 months" may actually be able to do so in that timeline. Budgets and other unforeseen factors could delay adoption.
Q4: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment channels currently accepted by your company.
Q6: Is your company considering accepting payments by mobile device over the next 12 months?

↑ Significantly different than 2017 within Segment

But m-Commerce growth=fraud. The LexisNexis Fraud Multiplier℠ has risen most sharply among those selling digital goods through the mobile channel.



The LexisNexis True Cost of Fraud℠ study has highlighted the risk of mobile channel fraud during recent years – particularly where digital goods and "fast fraud" can occur more easily. And as more adoption has occurred, this trend has emerged.

For every $1 of fraud, **mid/large m-Commerce merchants selling digital goods are hit with an average cost of $3.29**, as opposed to their physical-goods only counterparts at $2.78 (which is high nonetheless).

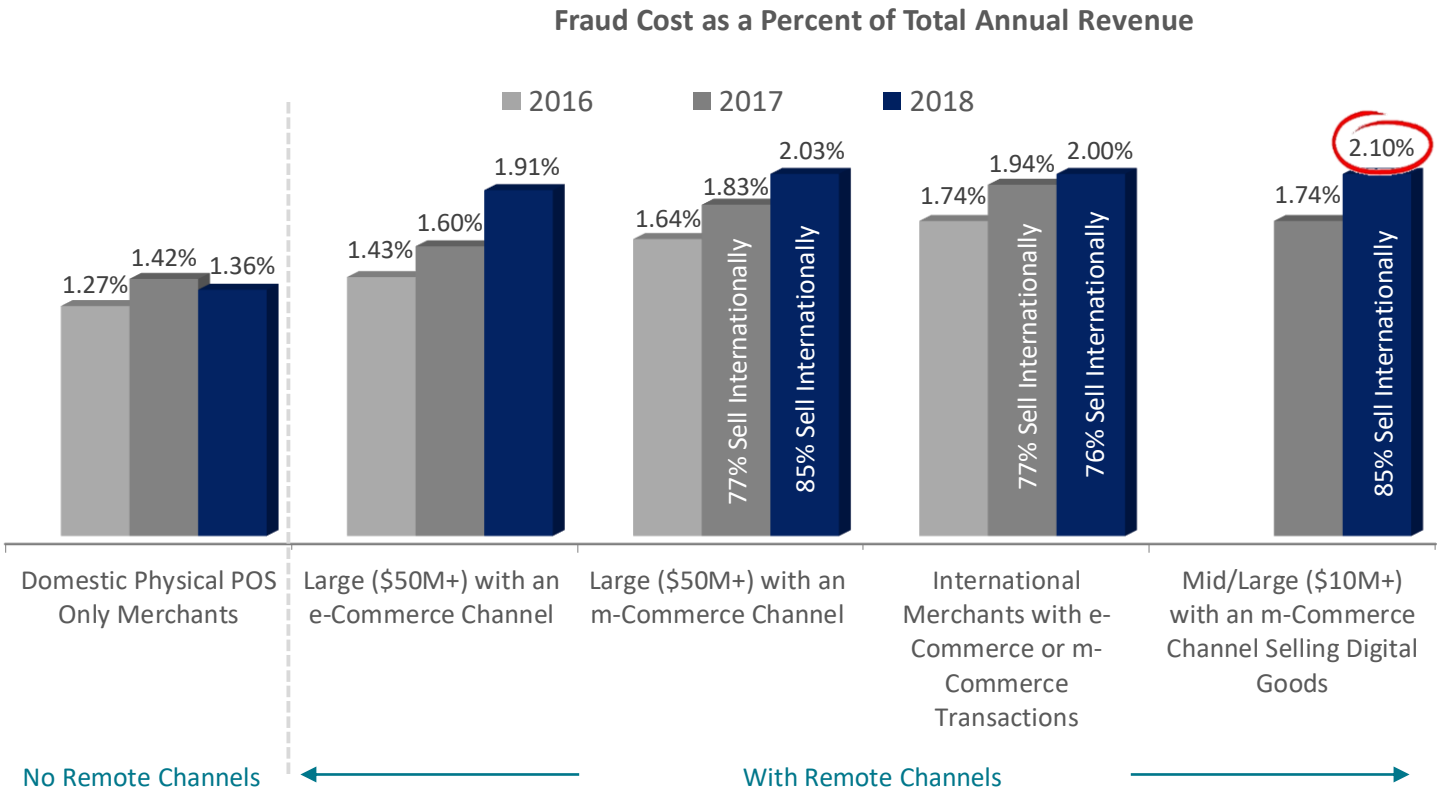
Mid/Large not allowing m-Commerce and selling only physical goods realize a cost of $2.30 - $2.54 for every $1 of fraud loss.

LexisNexis® RISK SOLUTIONS

Q16a: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.

And, the bottom line impact to larger m-Commerce merchants continues to be higher than others.

Fraud cost as a percent of total annual revenues has risen sharply over 2017 for m-Commerce merchants selling digital goods.



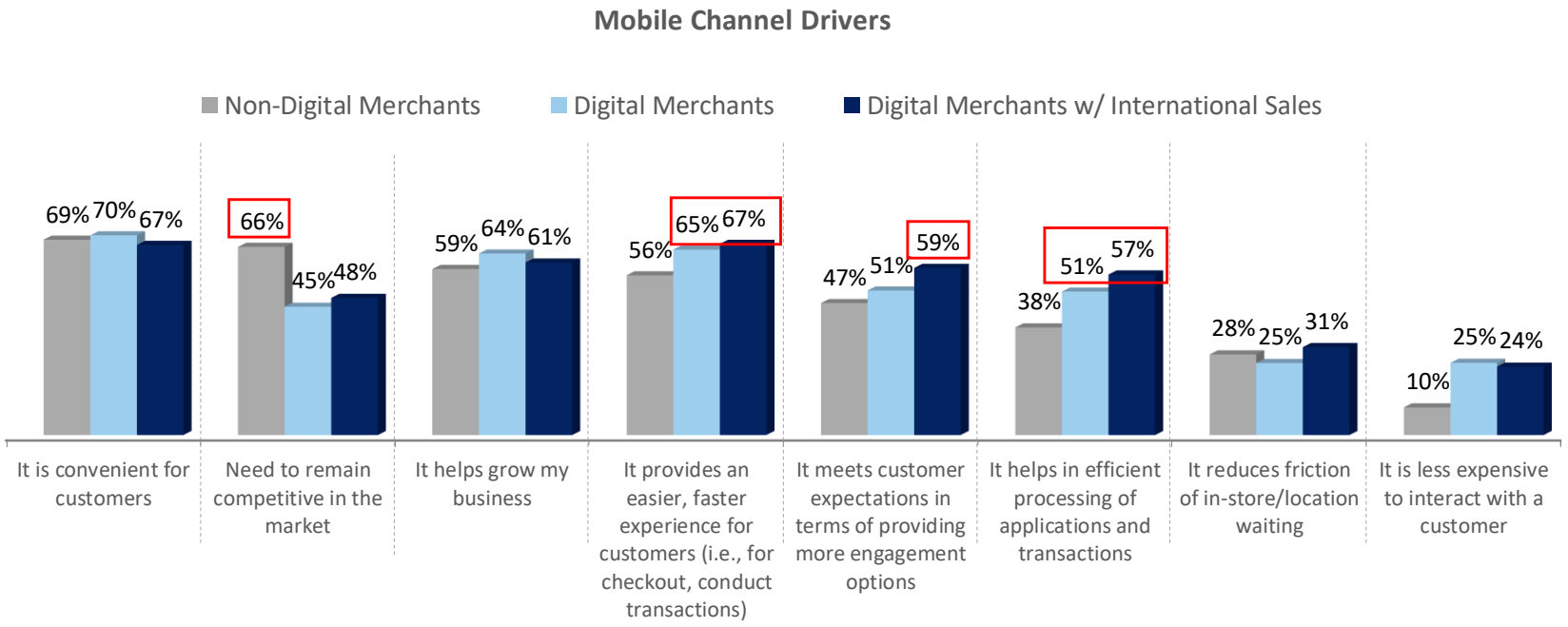
LexisNexis® RISK SOLUTIONS

Q10: What is the approximate dollar value of your company's total fraud losses over the past 12 months? Fraud losses as a percent of total annual revenue.

But, m-Commerce is worth it for customer acquisition/retention and revenue growth. Given this, it's essential for merchants to proactively plan for and manage mobile channel fraud.

Those selling digital goods are concerned with ***meeting customer expectations*** for a faster checkout and supporting ***more efficient processing*** of applications and transactions.

Those selling only physical goods via m-Commerce are more likely to be doing so based on the need to keep up with others / remaining competitive.



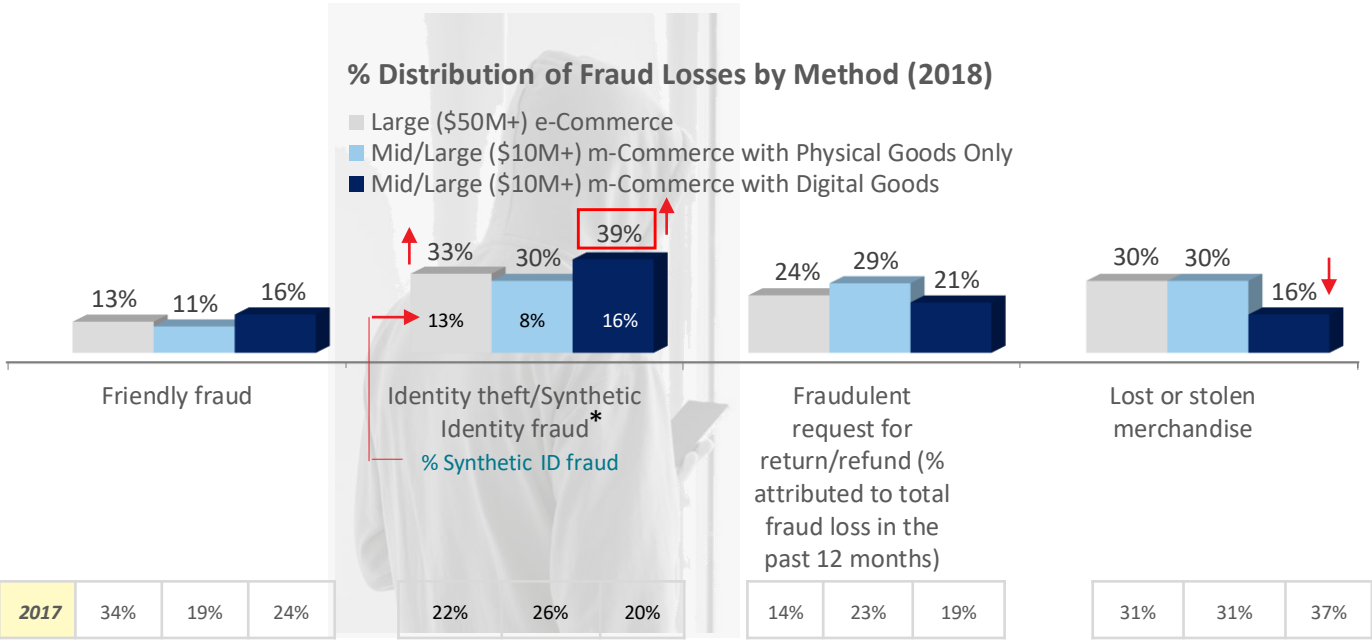
LexisNexis® RISK SOLUTIONS

Q5: What were the reasons your company decided to start accepting mobile account origination or transactions?

Significantly different from other segments within category at the 95% Confidence Interval

Unfortunately, these drivers have also increased risk for identity-related fraud.

Identity-related losses have grown significantly among larger remote channel merchants, particularly those selling digital goods. And, nearly half of identity fraud reported by these larger m-Commerce merchants with digital goods is attributed to the use of synthetic identities.



* Identity theft is unauthorized transaction using other people's personal identity information; Synthetic identity fraud is developing fraudulent identities based on some portion of real PII; first asked for Retail in 2018

↑ Significantly different than 2017 within Segment ▭ Significantly different from other segments at the 95% Confidence Interval

Q12: 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.

LexisNexis® RISK SOLUTIONS

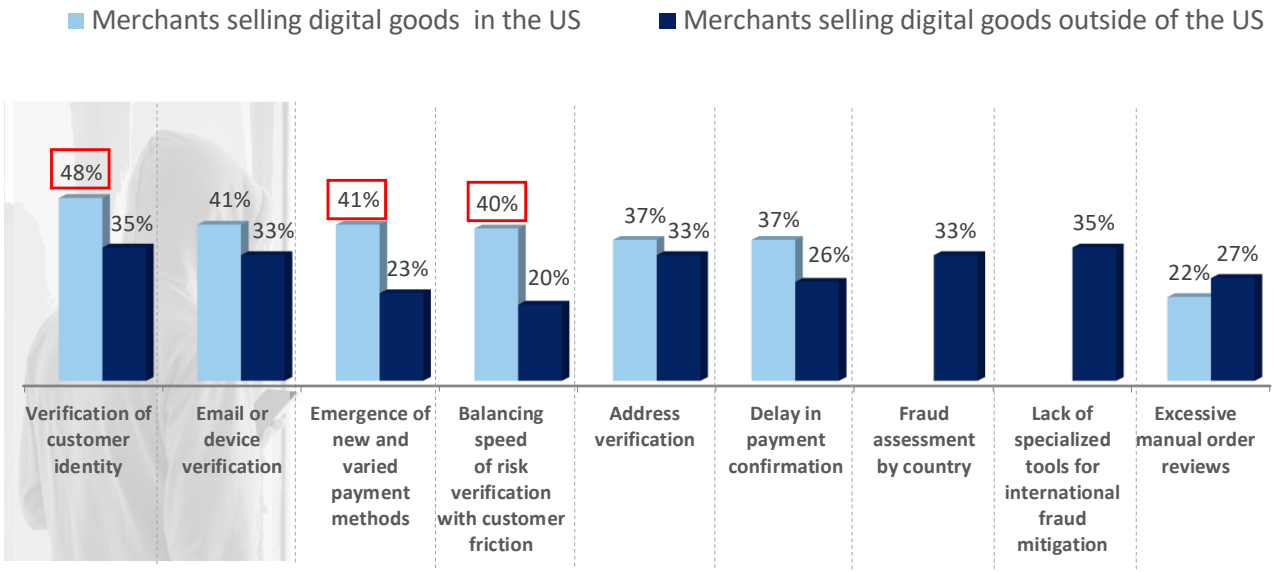
Not surprisingly, then, larger m-Commerce merchants are challenged by minimizing customer friction while verifying identities in the U.S., particularly with the use of newer payment methods.

This includes verifying digital identities (41% rank email or device verification) among their top 3 challenges when selling digital goods in the US.

Top 3 challenges for selling digital goods outside of the US are more fragmented, indicating more variety of issues faced with these digital transactions.

With digital fraud being "fast fraud", time is of the essence when verifying a transaction. This can relate to delay in payment confirmation as a top challenge.

Mid/Large ($10M+) m-Commerce Merchants Selling Digital Goods Within / Outside of the US (Ranking Among Top 3 Challenges)



Significantly different from segment within challenge at the 95% Confidence Interval

Q19aa: Please rank the top 3 challenges related to fraud faced by your company when selling digital goods to customers in the US
Q19bb: Please rank the top 3 challenges related to fraud faced by your company when selling digital goods to customers outside of the US

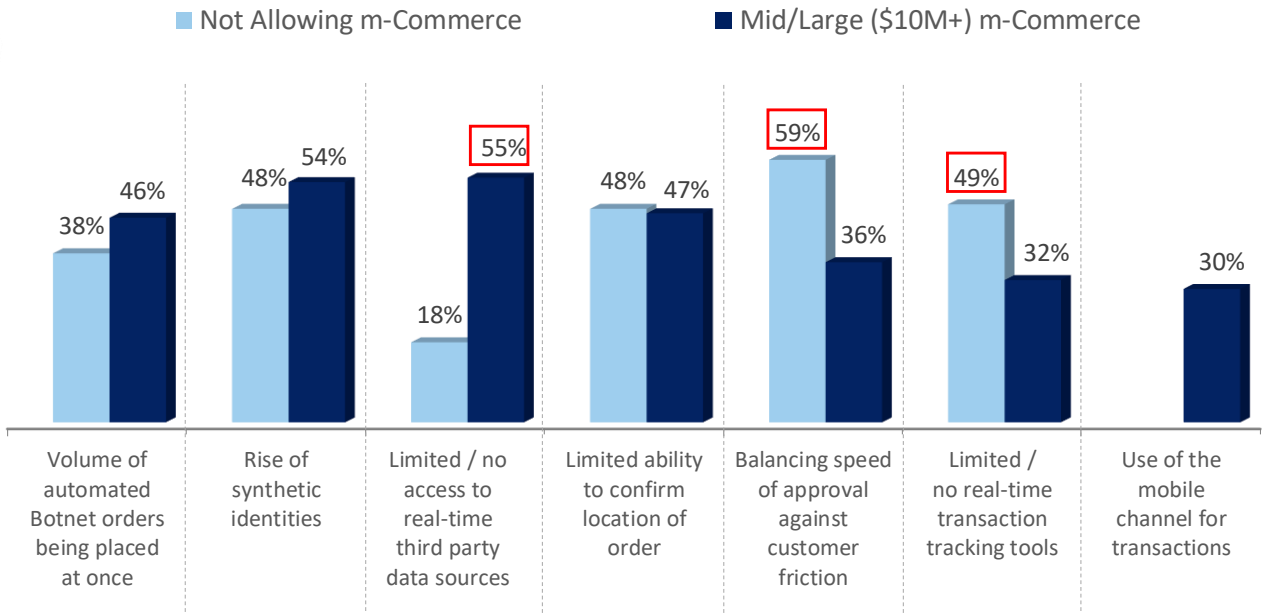
LexisNexis® RISK SOLUTIONS

The rise of synthetic identities and volume of Botnet orders have made identity verification even more difficult for those selling digital goods. It's even more significant of an issue among those specifically challenged with e-mail and / or device verification.

Interestingly, larger digital merchants allowing m-Commerce feel that there are no real-time third party data sources to help them with identity verification challenges.

Those ranking digital identity verification* as a top challenge are significantly more likely to mention risk of synthetic identities as a problem (76%)

Merchants Selling Digital Goods Within the US
Top 3 Factors Driving VERIFICATION OF CUSTOMER IDENTITY as a Challenge



Significantly different from segment within challenge at the 95% Confidence Interval

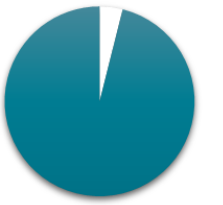
Q19a/b_2: Please rank the top 3 factors that make customer identity verification a challenge when selling digital goods inside/ outside the US.

* Those ranking e-mail / device / address verification as a challenge

LexisNexis® RISK SOLUTIONS

Profile of m-Commerce Merchants Who Rank Digital Identity Verification as a Key Challenge

- ✓ They also tend to sell physical goods.
- ✓ The digital goods they sell are easy to steal quickly or reuse until caught.
- ✓ They accept payments via mobile apps, which are often more secure but not immune to identity fraud.
- ✓ They do tend to track fraud, including from where it originates.



98% sell both physical and digital goods

Ave. % Transactions via
- Mobile browser **(38%)**
- Own branded mobile app **(20%)**
- 3rd Party mobile app **(19%)**

Every $1 of fraud actually costs them **$3.50**

Types of Digital Goods Sold

eGift Cards **57%**

Downloadable SW

53%

Digital Subscriptions **49%**

Mobile Apps

43%

Online Gaming **40%**

Video Streaming

40%

Ave. % of international fraud

26% from Eastern Europe / Russia

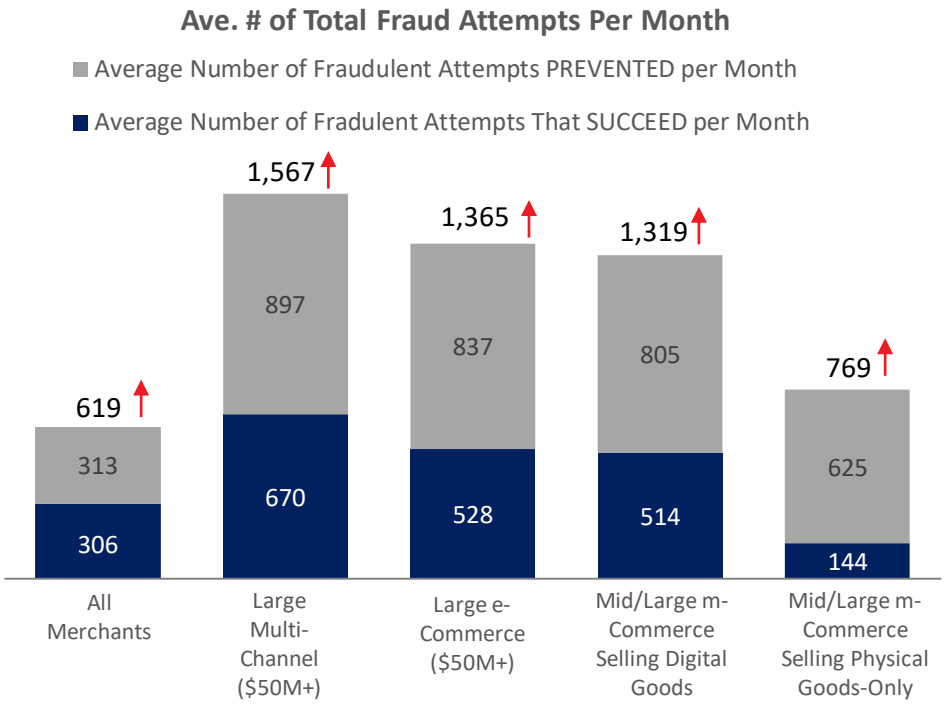
LexisNexis® RISK SOLUTIONS

Fraud volume continues to grow, particularly among larger multi-channel merchants. Attempts have been more successful when targeting digital goods than physical goods-only merchants.

Fraud volume in these larger remote channels has grown 32% - 36%, which is higher than the 2016-17 year-on-year change.

Adding digital goods adds the ability for "fast fraud" given the immediacy of distribution / downloading. Along with an increase in e-gift card volume, this could explain the significant rise in overall fraudulent attempts among merchants with digital goods.

M-commerce adoption is still limited among mid/large merchants that only sell physical goods. While the number of fraud attempts has increased over 2017, these represented prevented ones. And, the overall volume of attacks is significantly lower compared to m-Commerce merchants of the same size that have digital goods in their portfolio. This underscores the degree to which fraudsters focus more on digital goods – particularly since they have more success.



2017 TOTAL	495	996	1,000	895	402
Avg. # Prevented	257	423	410	505	250
Avg. # Successful	238	573	590	390	146
% Successful	48%	58%	59%	44%	36%

2016 TOTAL	442	707	880
Avg. # Prevented	236	275	299
Avg. # Successful	206	432	581
% Successful	47%	61%	66%

↑ Significantly different than 2017 within Segment

LexisNexis® RISK SOLUTIONS

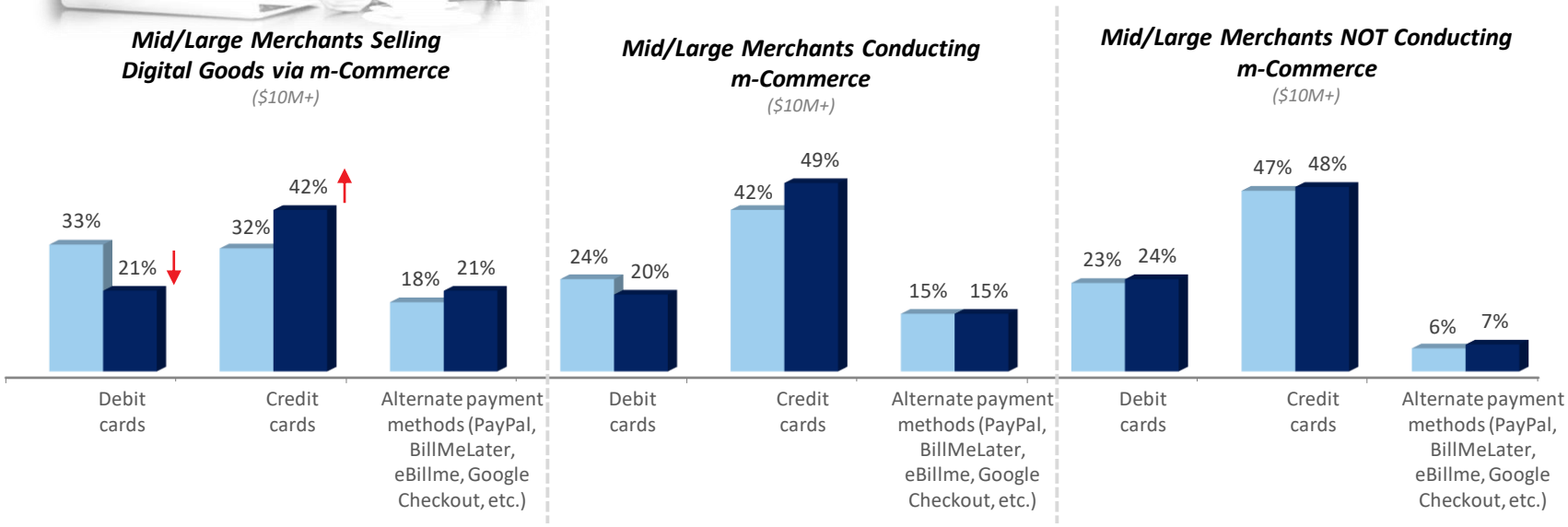
Q22: In a typical month, approximately how many fraudulent transactions are prevented by your company?
Q24: In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

Many merchants are fighting fraud, but still struggling with it – particularly in the mobile channel.

LexisNexis®
RISK SOLUTIONS

Credit card fraud remains high, with alternate payment method fraud being higher among m-Commerce merchants than others.

Those not conducting m-Commerce report only a small percentage of successful fraud through alternate payment methods.



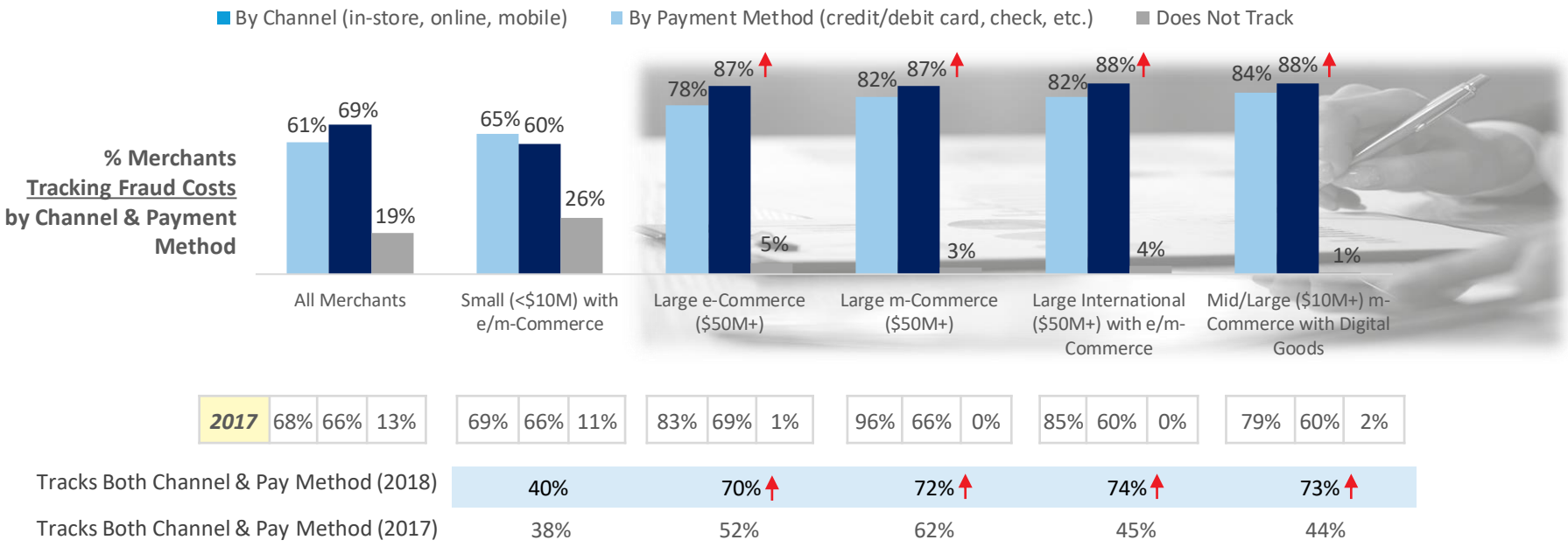
LexisNexis® RISK SOLUTIONS

Significantly different from other segments at the 95% Confidence Interval

Significantly different than 2017 within Segment

Q18: In thinking about the total fraud losses suffered by your company during the past 12 months, please indicate the distribution, to the best of your knowledge, of various fraud costs for each of the payment methods used by your company. .

But there has been a significant increase in the percent of larger e/m-Commerce merchants reporting that they track fraud cost by both channel and payment method; this is based on a significant rise in payment method tracking.



2017	68%	66%	13%	69%	66%	11%	83%	69%	1%	96%	66%	0%	85%	60%	0%	79%	60%	2%
Tracks Both Channel & Pay Method (2018)				40%			70% ↑			72% ↑			74% ↑			73% ↑		
Tracks Both Channel & Pay Method (2017)				38%			52%			62%			45%			44%		

LexisNexis® RISK SOLUTIONS

↑ Significantly different than 2017 within Segment

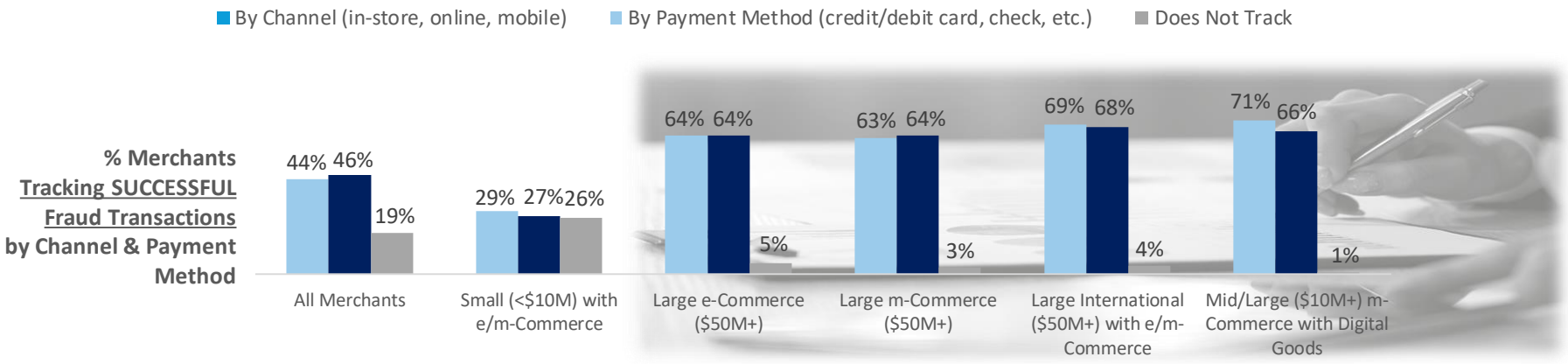
▭ Significantly different at the 95% Confidence Interval

Q14: Does your company track the cost of fraudulent transactions by payment channels or methods? Track successful fraud by payment channels or methods?

That said, merchants are more likely to be tracking where fraud has been *successful* rather than also tracking where they've been able to prevent it.

While tracking both successful and prevented fraud has increased over last year among mid/large m-Commerce merchants selling digital goods, this is by only half of this segment – similar to other remote channel segments.

This lessens the overall effectiveness of managing fraud since fraudsters are adept at testing for areas that are less of a focus by merchants and changing their attack points accordingly.



	All Merchants			Small (<$10M) with e/m-Commerce			Large e-Commerce ($50M+)			Large m-Commerce ($50M+)			Large International ($50M+) with e/m-Commerce			Mid/Large ($10M+) m-Commerce with Digital Goods		
2017	42%	33%	13%	40%	33%	11%	65%	47%	1%	77%	52%	0%	77%	55%	0%	72%	58%	1%
Tracks Both Successful & Prevented (2018)				22%			52%			51%			56%			53% ↑		
Tracks Both Successful & Prevented (2017)				30%			39%			47%			47%			40%		

LexisNexis® RISK SOLUTIONS

↑ Significantly different than 2017 within Segment

▭ Significantly different at the 95% Confidence Interval

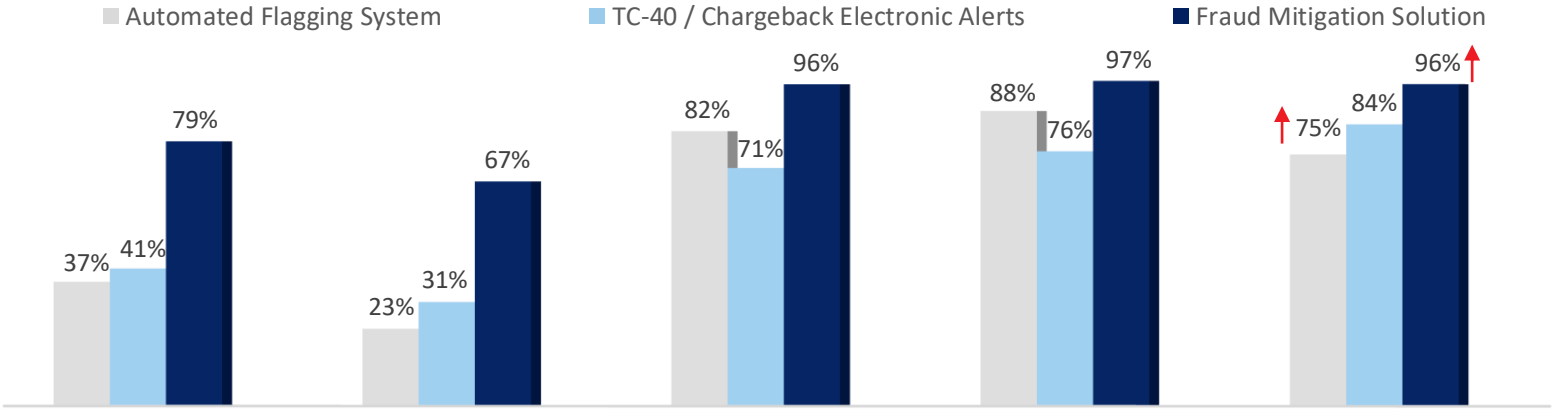
Q26: Does your company track the cost of fraudulent transactions by payment channels or methods? Track successful fraud by payment channels or methods?

Combined fraud solution and automated alert system use remains high among large remote merchants and has increased significantly among mid/large m-Commerce ones that sell digital goods.

This underscores the impact that fraud is having on this and other remote channel merchants.

The use of TC-40 / Chargeback Electronics Alerts is much more prevalent among larger remote merchants than small ones; that said, merchants may not always receive these reports from credit card / payment processes and, if they do, the large file sizes can become a barrier to actual use.

% Merchants Who Use an Automated Flagging System, TC-40 / Chargeback Electronic Service Alerts or Fraud Mitigation Solution



2017	35%		73%	44%		76%	84%	96%	84%	95%	45%		76%
2016	30%		66%	39%		73%	64%	79%	64%	84%	39%		69%

LexisNexis® RISK SOLUTIONS

↑ Significantly different than 2017 within Segment

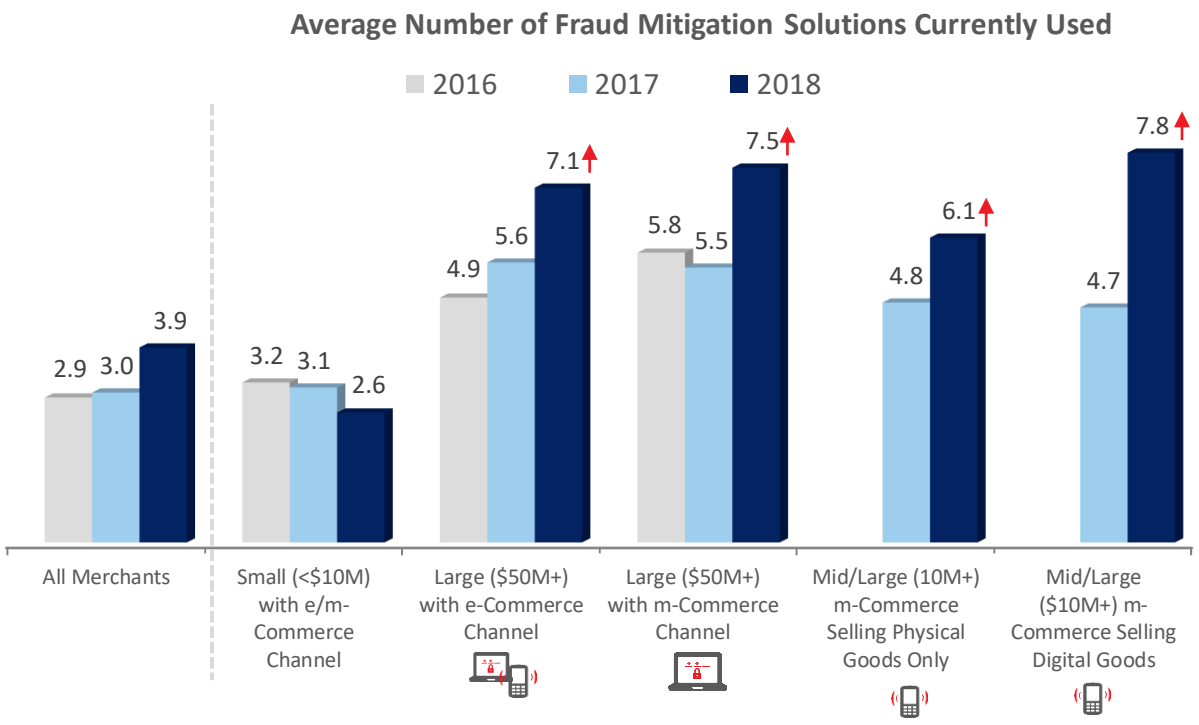
▭ Significantly different from other segments within system or solution category at the 95% Confidence Interval

Q35: Does your company use an automated system to flag potentially fraudulent transactions?
Q35b: Does your company use an electronic service that alerts you when a TC-40 / chargeback claim has been filed based on one of your transactions?
Q27: Which of the following best describes your awareness and use of the fraud solutions listed below?

This is consistent with an increase in the average number of fraud mitigation solutions used across larger remote channel merchants, particularly mid/large m-Commerce with digital goods.

Overall, though, these increases show that larger remote channel merchants, which have been getting hit harder by fraud in recent years, have started taking steps to add more fraud detection and prevention tools.

The larger rise among those selling digital goods speaks to the need for specific (and often different) solutions to address "fast fraud" that is associated with these types of products / services.



LexisNexis® RISK SOLUTIONS

Q27: Which of the following best describes your awareness and use of the fraud solutions listed below? Number of solutions being used.

↑ Significantly different than 2017 within Segment

▭ Significantly different from all or most other solutions at the 95% Confidence Interval

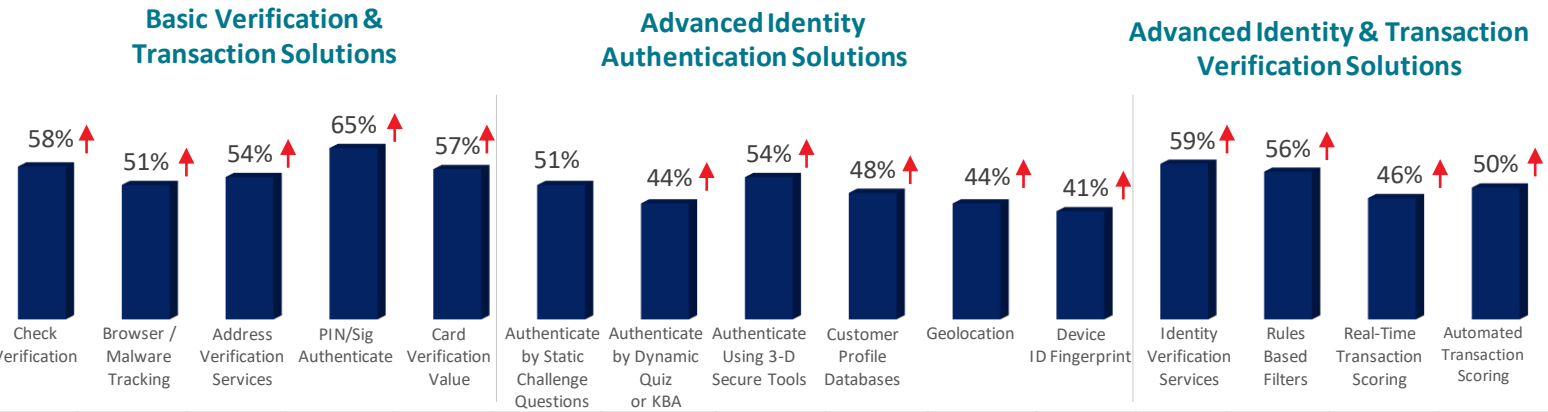
The increase in solutions use among mid/large m-Commerce selling digital goods has occurred for both ID authentication and verification.

This shows an understanding of the need for both types of solutions - including to support digital identity proofing. But not everyone has caught up to that; the use of many of these is still at or under 50% of the market.

There are differences between the solutions used by merchants selling digital versus physical goods-only, with digital goods merchants using more identity authentication solutions that can support "fast fraud" detection.

An increase in some solutions / services, such as check verification and PIN/signature authentication, reminds us that these merchants are using multiple channels – including physical point of sale locations.

MID/LARGE ($10M+) Merchants Selling Digital Goods via m-Commerce



	Check Verification	Browser / Malware Tracking	Address Verification Services	PIN/Sig Authenticate	Card Verification Value	Authenticate by Static Challenge Questions	Authenticate by Dynamic Quiz or KBA	Authenticate Using 3-D Secure Tools	Customer Profile Databases	Geolocation	Device ID Fingerprint	Identity Verification Services	Rules Based Filters	Real-Time Transaction Scoring	Automated Transaction Scoring
2017	33%	28%	44%	34%	38%	39%	34%	11%	27%	28%	12%	35%	38%	32%	40%
M/L m-Commerce Selling Physical Goods Only						Less use than those selling digital goods									
2018	60%	26%	43%	73%	74%	20%	19%	52%	34%	29%	16%	57%	40%	47%	19%

LexisNexis® RISK SOLUTIONS

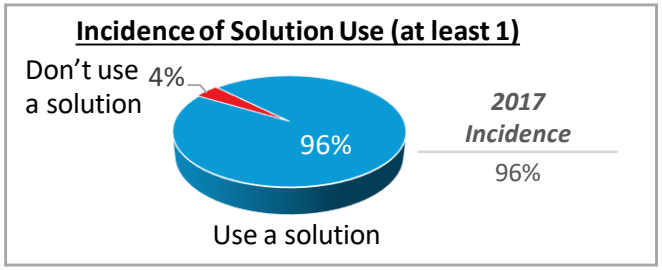
↑ Significantly different than 2017 within Segment

Q27: Which of the following best describes your awareness and use of the fraud solutions listed?

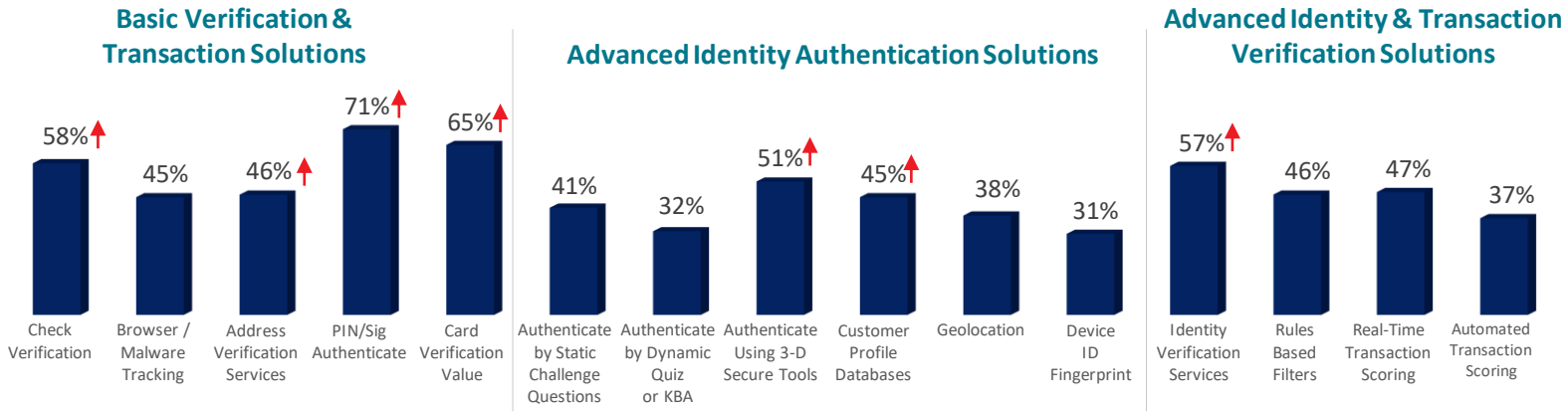
Solutions growth among large merchants with an e-Commerce channel has occurred with some identity authentication and verification solutions.

However, the most significant growth has occurred for select physical POS solutions / services (PIN/signature authentication and CVV).

While an increase in address verification services can support some digital identity proofing, the limited use of device ID / fingerprinting weakens that effort.



LARGE ($50M+) Merchants with an e-Commerce Channel



2017	42%	42%	33%	44%	44%	43%	29%	31%	29%	30%	27%	43%	45%	39%	35%
2016	39%	42%	36%	39%	43%			27%	23%	42%	25%	42%	31%	36%	26%

LexisNexis® RISK SOLUTIONS

▲ Significantly different than 2017 within Segment

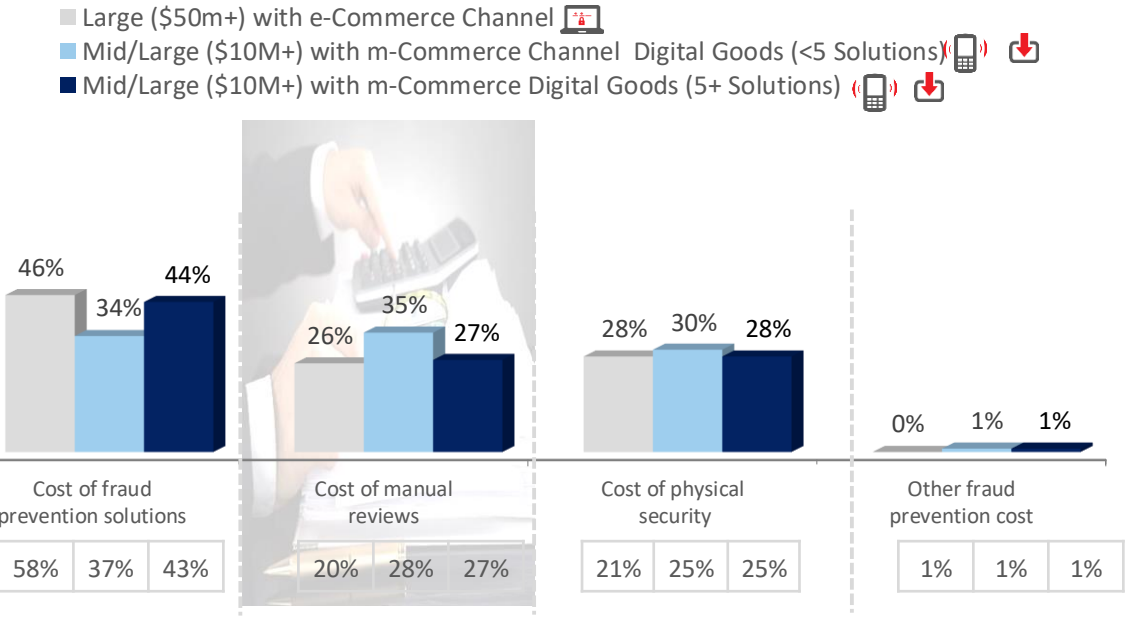
▭ Significantly different from all or most other solutions at the 95% Confidence Interval

Q27: Which of the following best describes your awareness and use of the fraud solutions listed?

Solutions remain the major component of fraud mitigation spend for larger merchants with e/m-Commerce channels. But for those which don't invest as much in fraud prevention solutions, costs tend to shift to manual reviews.

There is at least a directional difference in the percentage of fraud mitigation spend for manual reviews when comparing m-Commerce digital goods merchants having less than and more than 5 fraud prevention solutions. Those with fewer solutions tend to have as much of their fraud mitigation spend dedicated to human resources (manual reviews) as they do to solutions. Those with more solutions spend less on manual reviews.

Distribution of Fraud Mitigation Costs by Percent of Spend



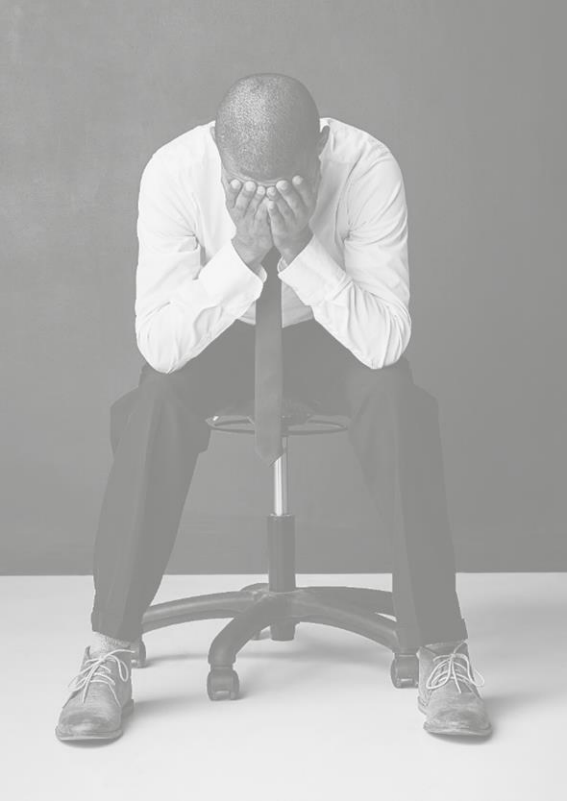
	Cost of fraud prevention solutions			Cost of manual reviews			Cost of physical security			Other fraud prevention cost		
2017	58%	37%	43%	20%	28%	27%	21%	25%	25%	1%	1%	1%

LexisNexis® RISK SOLUTIONS

↑ Significantly different than 2016 within Segment

▭ Significantly different from all or most others within category at the 95% Confidence Interval

Q41b: What is the percentage distribution of mitigation costs across the following areas in the past 12 months?

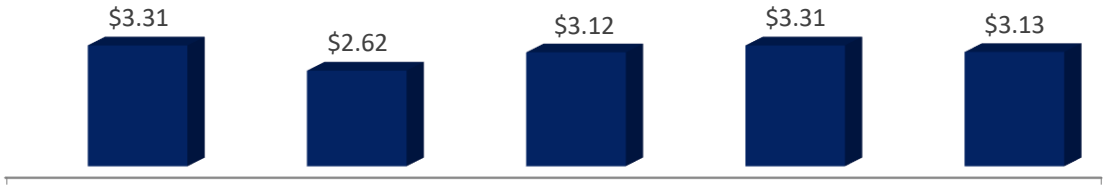


But, the number of solutions may not necessarily ensure lower fraud volumes, cost and frustrations.

While the cost of fraud is higher among remote channel merchants with fewer fraud prevention solutions, it is still high for those which have invested in a number of them. What tends to differ is the type of good or service sold; those selling digital goods have higher fraud costs and a higher percentage of false positives – even among those with more solutions.

They are also more concerned about continued e-Gift card fraud and Botnet activity regardless of the number of solutions they use.

LexisNexis Fraud Multiplier℠



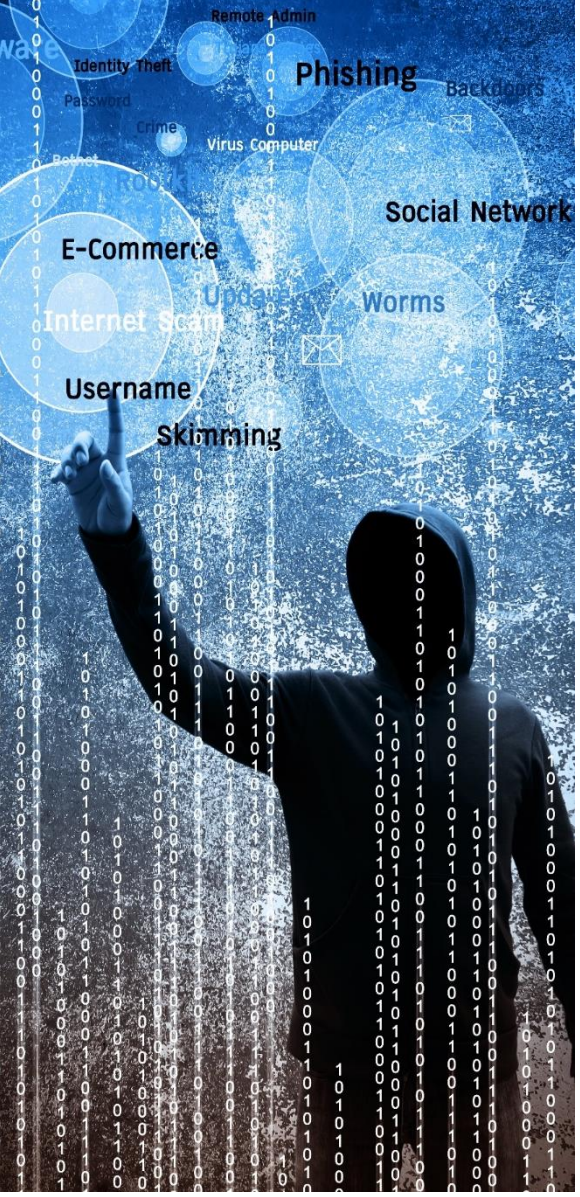
	Large ($50M+) e-Commerce (<5 Solutions)	Large ($50M+) e-Commerce Selling Physical Goods Only (5+ Solutions)	Large ($50M+) e-Commerce Selling Digital Goods (5+ Solutions)	Mid/Large ($10M+) m-Commerce Selling Digital Goods (<5 Solutions)	Mid/Large ($10M+) m-Commerce Selling Digital Goods (5+ Solutions)
			% Agree		
e-Gift card fraud will continue to rise	74%	NA	80%	64%	76%
Combatting automated Botnet activity is overwhelming & difficult to keep up with	60%	40%	63%	59%	62%
% of False Positives	26%	18%	28%	27%	24%

LexisNexis® RISK SOLUTIONS

Therefore, the current solution combinations may not be optimal.

A layered solution approach that addresses specific sales environments is more effective.

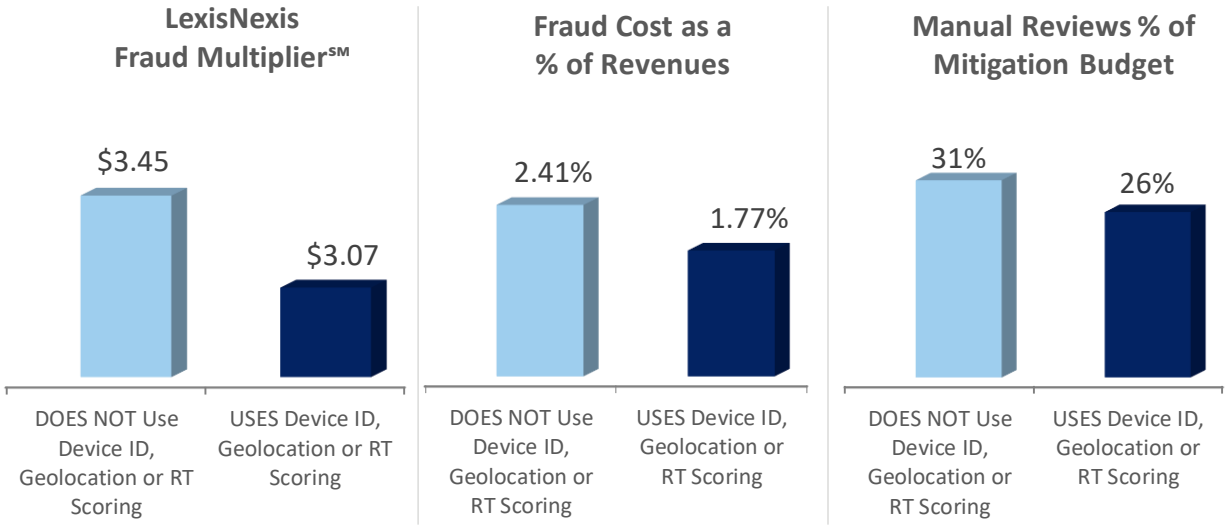
LexisNexis®
RISK SOLUTIONS



It is not necessarily the number of solutions, but the right combination and layering of them to meet different threats.

As an example, Device ID/Fingerprinting, Geolocation and Real-Time Scoring are particularly useful when dealing with mobile payments and sales of digital goods – they support digital identity verification.

m-Commerce Merchants Selling Digital Goods



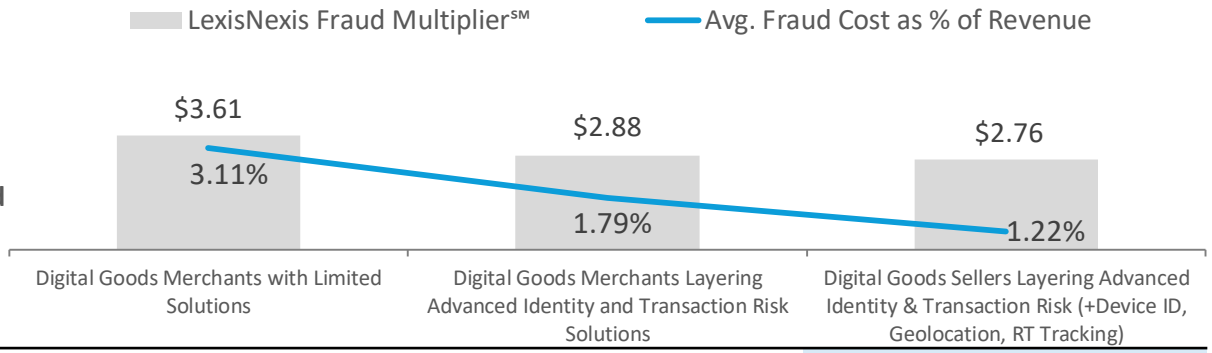
Findings indicate that m-Commerce merchants which sell digital goods and use these solutions tend to experience a lower cost of fraud than those who don't use them.

LexisNexis® RISK SOLUTIONS

That said, it's also important to layer both identity authentication and fraud transaction risk assessment solutions.

Digital goods merchants who layer core + identity + fraud transaction solutions have lower fraud costs ($2.88 for every $1 of fraud) than those which use only a limited set of core solutions (up to $3.61 per $1 of fraud). Those which also layer in specific solutions to address the unique risks of digital goods and mobile channel transactions have even lower fraud costs.

LexisNexis Fraud Multiplier℠ and Avg. Fraud Cost by Number & Layering of Fraud Mitigation Solutions



Layers of Protection		Basic	Multi-Layered	Multi-Layered with Specific Mobile Digital Goods Tools
Common Core Solutions Used Most Often	Card verification, PIN/Signature, Check Verification, Browser Malware, Address Verification	✓	✓	✓
Layering of Advanced Identity Solutions	Device ID Fingerprinting, Geolocation, Authentication by Quizzes, Authentication by Challenge Questions, Customer Profile Database, Authentication of Transaction by 3D Tools		✓	✓
Layering of Fraud Transaction Risk Assessment Solutions	Automated Transaction Scoring, Real-Time Transaction Tracking, Verification/Validation Services, Rules-Based Filters		✓	✓

LexisNexis® RISK SOLUTIONS

Recommendations

LexisNexis®
RISK SOLUTIONS

Recommendation #1

Retail merchants need to implement unique risk mitigation solutions for different business models. There is no one-size-fits-all solution.

Solutions used to mitigate risk with physical goods transactions won't fully mitigate risk with digital goods transactions because the nature of the goods changes the risk (i.e., more real-time, faster transactions with digital goods).

Different challenges and risks also require specific solutions that support domestic versus international and remote versus non-remote channels.

LexisNexis® RISK SOLUTIONS

Recommendation #2

Further, remote channel and digital goods merchants should consider a multi-layered solution approach that attacks different types of fraud.

It is critical for merchants to address both identity and transaction-related fraud. These are two different perspectives.

Identity verification / authentication is important for “letting your customers in” with the least amount of friction and risk.

Transaction-related fraud is about keeping the “bad guys out”.

A layered approach can reduce costs associated with manual reviews, successful fraud attempts and fewer false positives.

LexisNexis® RISK SOLUTIONS

Recommendation #3

Merchants selling digital goods via m-Commerce need to remain vigilant and open to a wider variety of risk mitigation solutions.

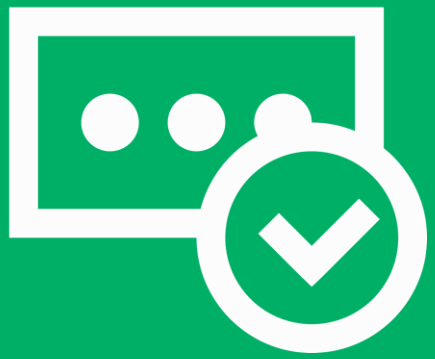
Fraud and its associated costs are already more of an issue for these merchants than many others. This will likely become more of an issue as the battle against Botnets and synthetic fraud continues.

E-gift card fraud has become an issue, without regulated protection with smaller transaction fraud.

A layered solution approach should particularly consider those which support faster / real-time identity and transaction verification decision making.

LexisNexis® RISK SOLUTIONS

Recommendation #4



Remote channel and digital-selling merchants need to track both payment and channel fraud – in terms of costs and successful attempts.

Fraud occurs in multiple ways, particularly for multi-channel merchants (given overlap between use of online and mobile channels). The remote channel, of course, is important to monitor in comparison to physical POS locations since the anonymity of online and mobile make these channels more high risk. Additionally, there are different security issues and approaches between online and mobile channels.

But, the rise of synthetic identities makes it easier for fraud via different payment methods in remote channels. This not only involves use of traditional credit / debit card fraud, but also 3rd party payment providers and distribution partners for digital goods.

LexisNexis® RISK SOLUTIONS

LexisNexis® Risk Solutions can help

LexisNexis®
RISK SOLUTIONS

LexisNexis® Risk Solutions provides powerful identity verification, identity authentication and transaction scoring tools to combat fraud.

LexisNexis® Risk Solutions:

- Vast Data Resources
- \+
- Big Data Technology
- \+
- Linking & Analytics
- \+
- Industry-Specific Expertise & Delivery

=

Customer-Focused Solutions

Identity Verification
- Validate name, address and phone information
- Reconcile name variations, duplicates, multiple addresses, and myriad other inconsistencies and linkages
- Perform global identity checks with seamless integration and reporting capabilities

Transaction Risk Scoring
- Identify risks associated with bill-to and ship-to identities with a single numeric risk score
- Quickly detect fraud patterns and isolate high-risk transactions
- Resolve false-positive and Address Verification Systems failures

Manual Research Support
- Access billions of data records on consumers and businesses
- Discover linkages between people, businesses and assets
- Leverage specialized tools for due diligence, account management and compliance

Identity Authentication
- Authenticate identities on the spot using knowledge-based quizzes
- Dynamically adjust security level to suit risk scenario
- Receive real-time pass/fail results

LexisNexis® RISK SOLUTIONS

For more information: visit http://www.lexisnexis.com/risk/retail or call 800.869.0751