2017 LexisNexis® Risk Solutions True Cost of Fraud℠ for e-commerce

LexisNexis®
RISK SOLUTIONS

The 2017 LexisNexis® Risk Solutions True Cost of Fraud℠ Study

This study was conducted to provide e-commerce merchants with insights to help them grow their business safely, in light of the growing risk of fraud

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

The study included a comprehensive survey of 190 risk and fraud executives in retail organizations with 80% or more in revenue from online or mobile channels

FRAUD =

- Fraudulent transactions due to identity fraud
- Fraudulent requests for refunds/returns, bounced checks
- Lost or stolen merchandise, as well as redistribution costs associated with redelivering purchased items

The LexisNexis® Fraud Multiplier℠ cost =

Total amount of costs related to fees, interest, merchandise replacement and redistribution per dollar of fraud for which the merchant is held liable.

E-COMMERCE COMPANIES INCLUDE:

Mid/Large

Earn $10 million+ in annual sales.

Small

Earn <$10 million in annual sales.

MERCHANT DEFINITIONS ARE DEFINED AS:

M-commerce

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

E-commerce

May earn revenue through multiple channels, but a large majority is through the online channel.

LexisNexis® RISK SOLUTIONS

Research was deployed March & April 2017.

Summary of key findings

LexisNexis®
RISK SOLUTIONS

Key findings

1

Sizeable fraud is occurring within the e-commerce sector, particularly among mid / large e-commerce merchants selling digital goods.

2

While the acceptance of mobile payments is still emerging among e-commerce merchants, fraud will likely grow as this channel becomes more prevalent.

3

Some of these higher fraud volumes and costs relate to less optimal approaches in managing fraud.

Key findings

4

E-commerce merchants allowing mobile payments or selling digital goods are also not fully leveraging the value of risk mitigation solutions.

5

While much is spoken about mid/large fraud challenges, small e-commerce merchants are at even more risk.

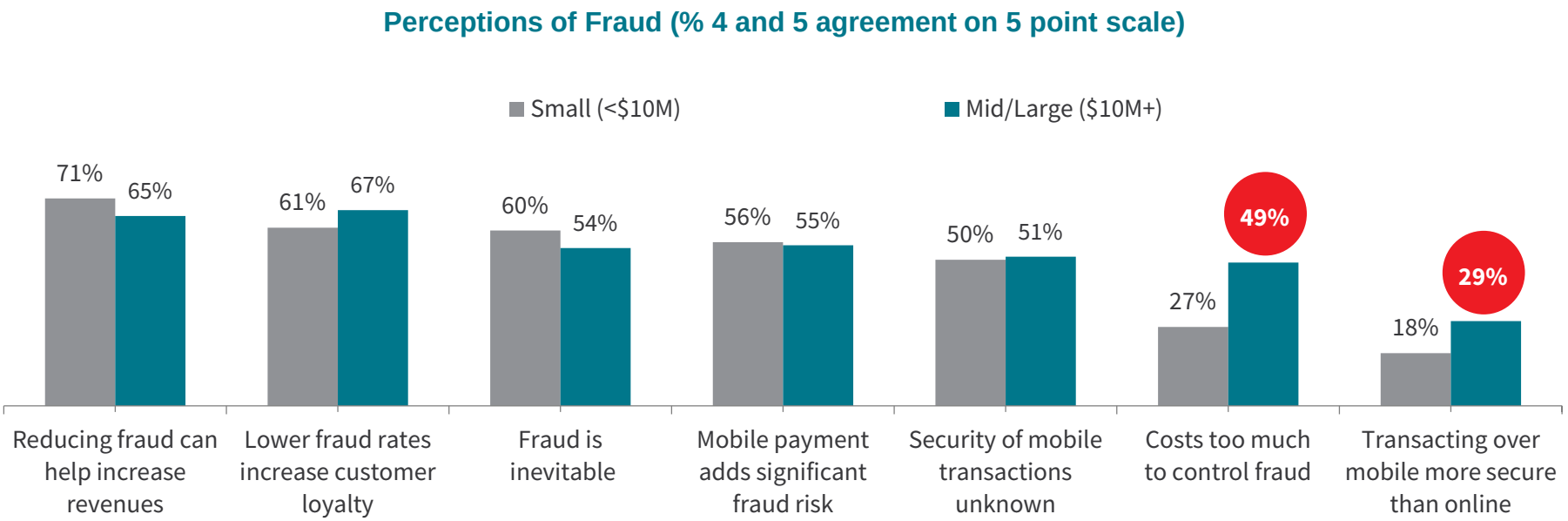
6

Findings show that remote merchants who layer solutions by identity and fraud transaction solutions experience fewer issues and cost of fraud.

Findings by merchant size

LexisNexis®
RISK SOLUTIONS

M-commerce is still limited due to concerns around mobile security and risk

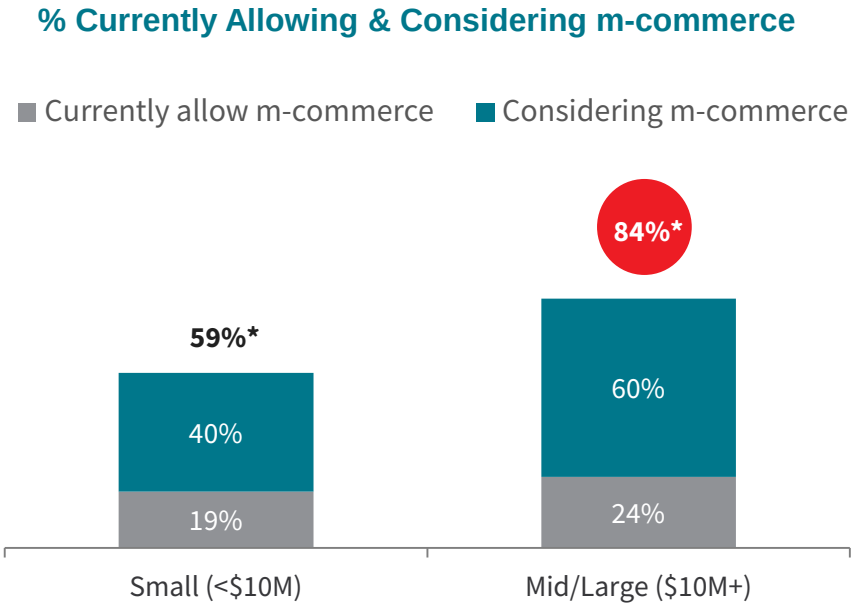


Q33: Using a 5-point scale, please rate the extent to which you agree or disagree with the statements below.

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

Despite risk concerns m-commerce is expected to grow

A number of e-commerce merchants expect to allow mobile purchases within the next 1 – 2 years despite concerns about it's security. Mid/large merchants is a particular area for potential m-commerce growth.



Q2: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following channels used by your company.
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?

*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.

LexisNexis® RISK SOLUTIONS

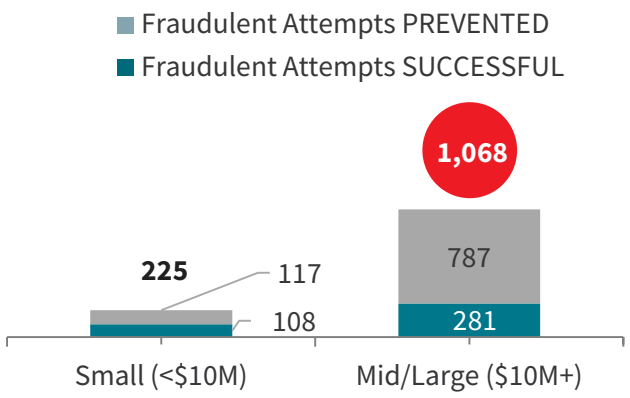
Significantly different from other segment within category at the 95% Confidence Interval

The volume and value of successful fraud transactions among Mid/Large e/m-commerce merchants are nearly 3x that of Small e/m-commerce merchants

Although smaller in volume, significantly more small e-commerce fraudulent attempts are successful (48%).

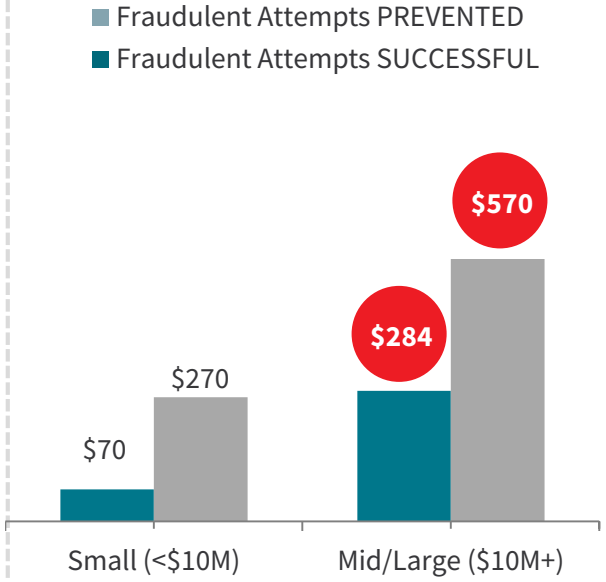
This is not surprising when reviewing other findings that show less use of fraud prevention solutions and fraud tracking among this segment (as shown on subsequent slides).

Average # Reported Fraud Transactions per Month*



% Prevented/Successful of Fraud Transactions

Average $ Amount Per Fraud Transactions per Month*



Q22: In a typical month, approximately how many fraudulent transactions are prevented by your company? Q23: What is the average value of such a transaction? Q24: In a typical month, approximately how many fraudulent transactions are successfully completed? Q25: What is the average value of such a transaction?

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

LexisNexis® RISK SOLUTIONS

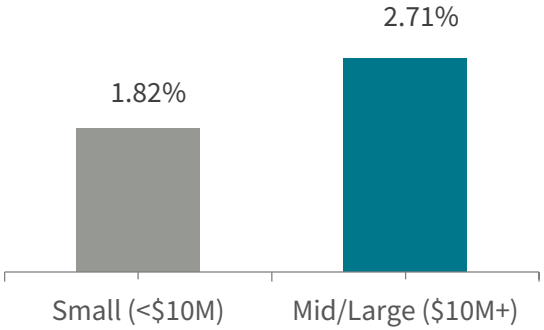
Growth in m-commerce and digital goods sales could have a negative impact on Mid/Large e-commerce merchants, for which every $1 of fraud already costs them $3.37 on average

Mid/Large e-commerce merchants are much more likely than Small to sell digital goods (63% vs. 33%).

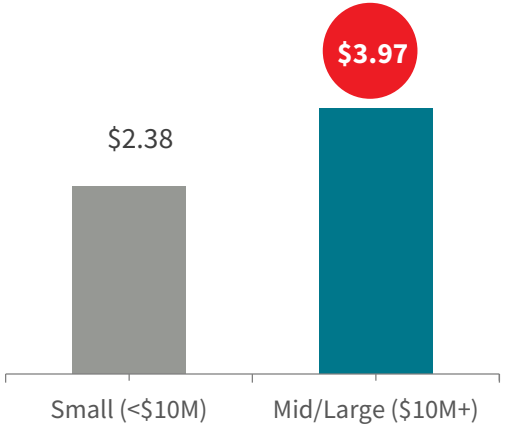
Sellers of digital goods experience higher fraud costs and volumes, particularly involving e-gift cards. This comes with a higher proportion of indirect losses, such as fees and interest, than physical goods, which drives up the LexisNexis Fraud Multiplier℠ per $1 of direct fraud losses. Such fees are levied by credit/debit card providers and third-party channels.

Small e-commerce merchants are more likely to sell physical goods. Thus, when they experience fraud, a higher proportion of this is due to chargebacks rather than fees. This results in lower indirect losses.

Fraud Costs as a % of Revenues



LexisNexis Fraud Multiplier℠



Types of Goods Sold

	Small (<$10M)	Mid/Large ($10M+)
Digital & physical	33%	**63%**
Physical-only	**67%**	37%

Q10: What is the approximate value of your company's total fraud losses over the past 12 months, as a % of total revenues?
Q16: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud costs over the past 12 months.
D1: Please indicate the type of products sold by your company.

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

LexisNexis® RISK SOLUTIONS

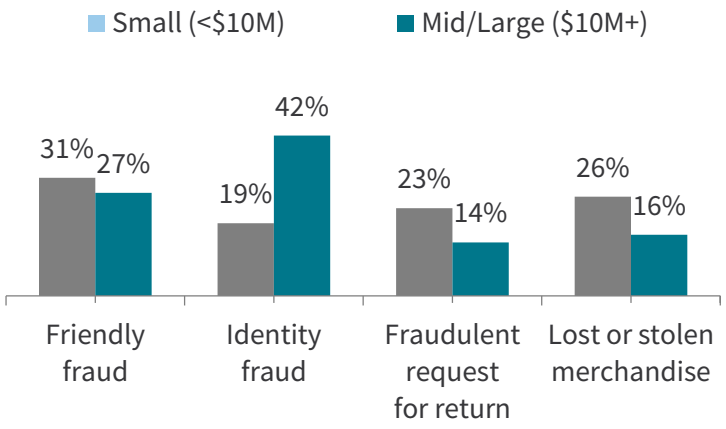
Digital goods sales likely also drive higher identity theft and international fraud for Mid/Large e/m-commerce merchants

Identity theft represents nearly half of fraud losses among mid/large merchants, which are more likely to have an international presence as well digital goods sales.

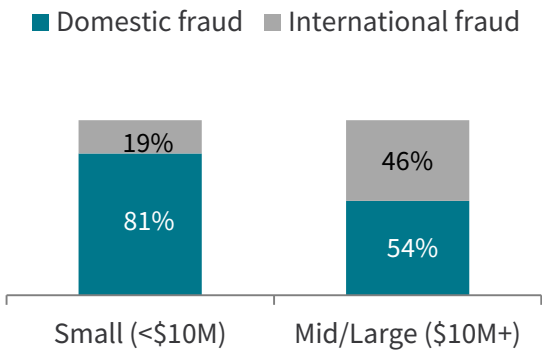
While these mid/large merchants are more likely to track fraud costs by channel and payment method, they are still struggling with such costs.

For small e/m-commerce merchants, even though they are losing nearly 2% of revenue to fraud costs, a sizeable group doesn't track these by channel or method. This leaves them exposed.

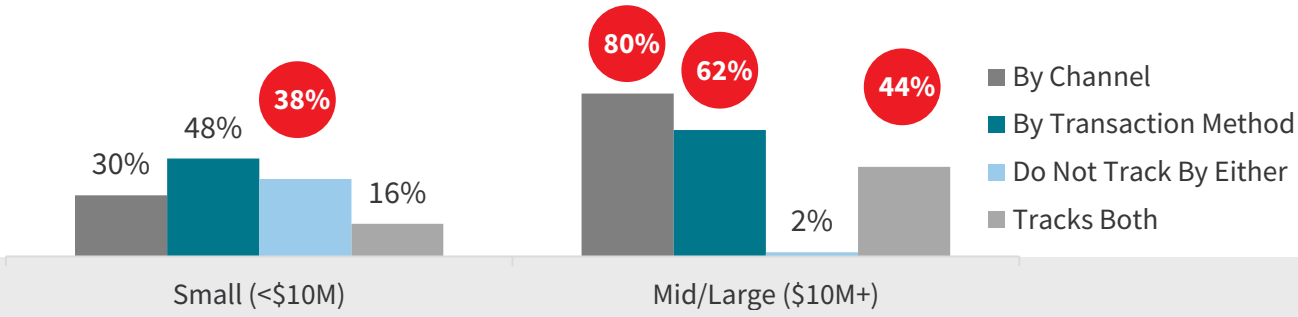
% Distribution of Fraud Losses by Method



% Distribution of Fraud Losses by Geo



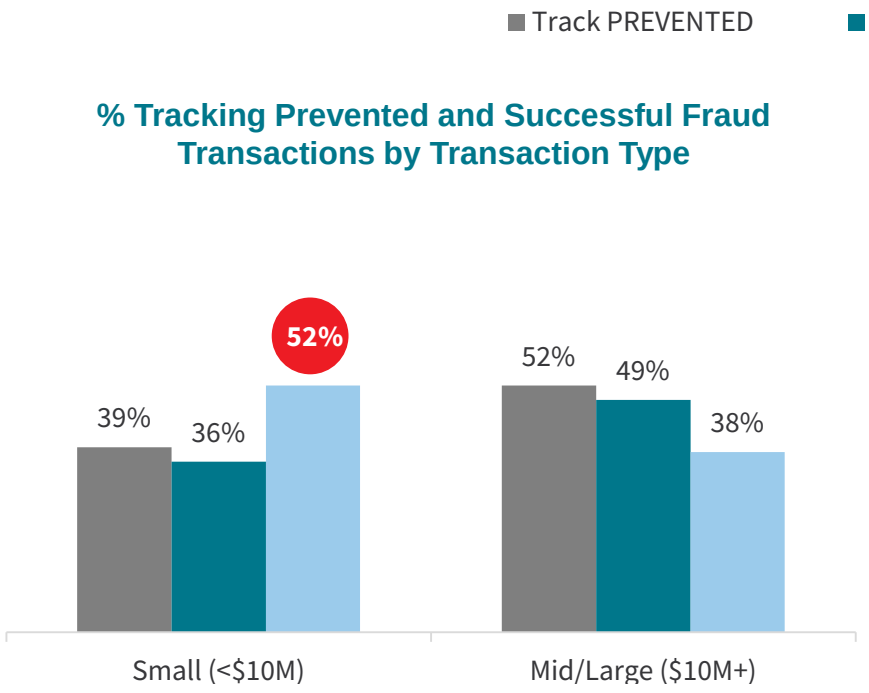
% Tracking Fraud Costs by Channel & Transaction Method

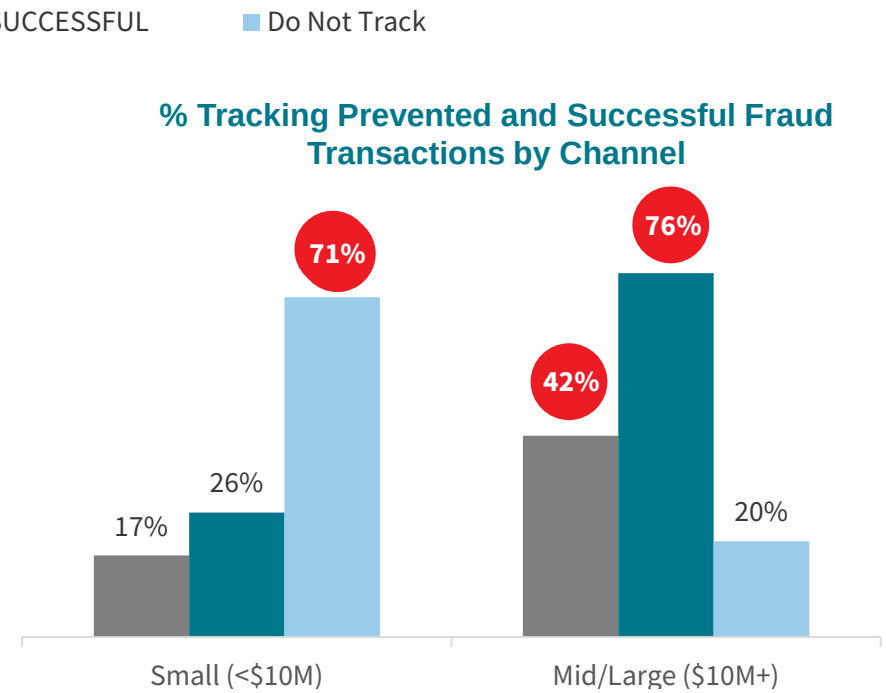


Q12: Please indicate the percentage distribution of the following fraud methods as attributed to your total annual fraud loss over the past 12 months.
Q13: Please indicate the percent of fraud costs generated through domestic orders compared to international orders in the last 12 months.
Q14: Does your company track the cost of fraudulent transactions by channels or methods?

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

When it comes to prevented vs. successful fraudulent transactions, merchants aren't optimally tracking for this which leaves gaps for fraudsters to leverage





LexisNexis® RISK SOLUTIONS

Q26a: Does your company track prevented vs. successful transactions by type or channel?

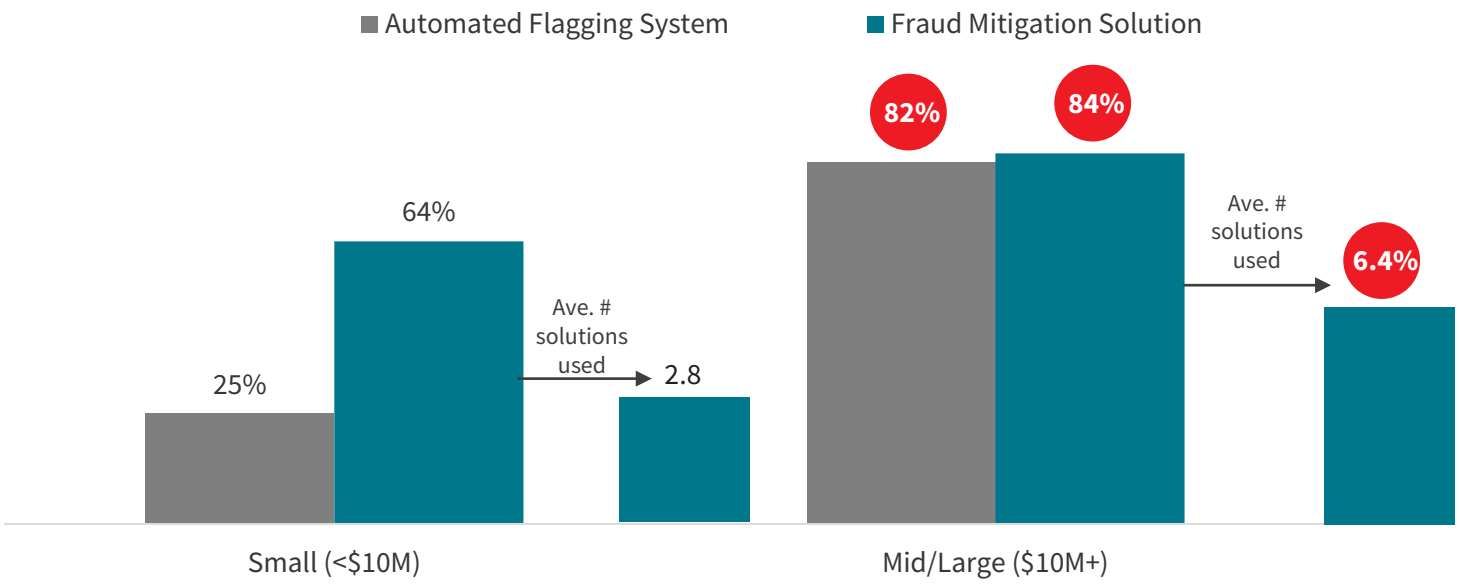
Significantly different from other segment within category at the 95% Confidence Interval

Mid/large e/m-commerce merchants are fighting fraud through use of auto flagging systems and fraud mitigation solutions

These merchants are handling larger volumes of transactions, which makes manual review harder to scale.

While Small e/m-commerce merchants are much less likely to use an automated flagging system, nearly two-thirds use a fraud mitigation solution.

% Merchants Who Use an Automated Flagging System or Fraud Mitigation Solution



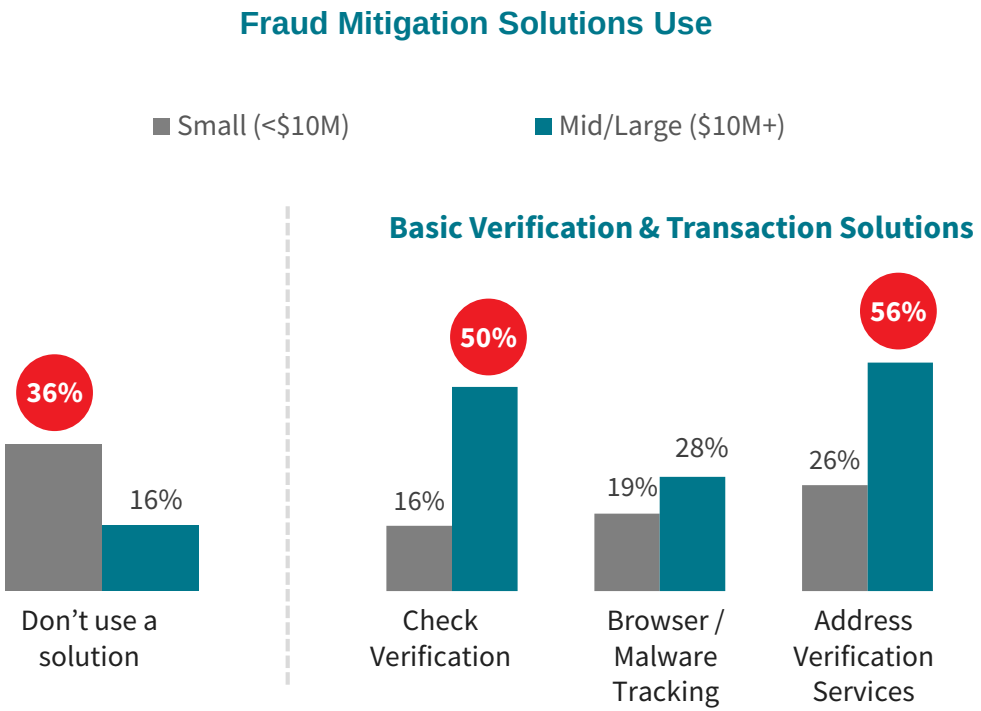
36% are not using a fraud mitigation solution

16% are not using a fraud mitigation solution

Q27: Which of the following best describes your awareness and use of the fraud solutions listed below? Usage.
Q35: Does your company use an automated system to flag potentially fraudulent transactions?

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

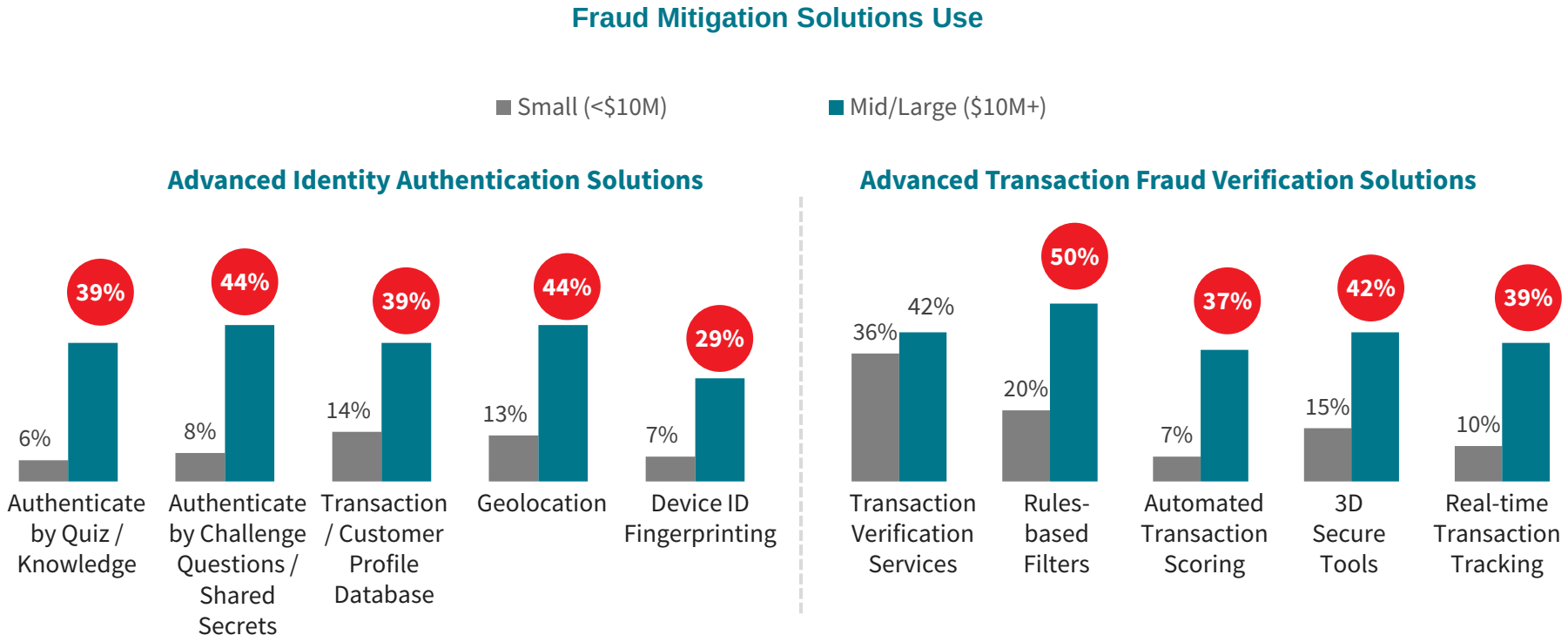
Small e/m-commerce merchants are more likely implement more basic verification solutions than Mid/Large merchants



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

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

Mid/large e/m-commerce merchants may not be using the right combination of solutions and are still getting hit by fraud



Mid/large merchants are dealing with multiple channels and fraud scenarios (online vs. mobile; domestic vs. international; physical versus digital goods). Each of these involve different technologies or sales environments such that unique solutions should be used to address the uniquely different threats.

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

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

Findings by Type of Goods Sold

Digital with Physical
vs. Physical-only

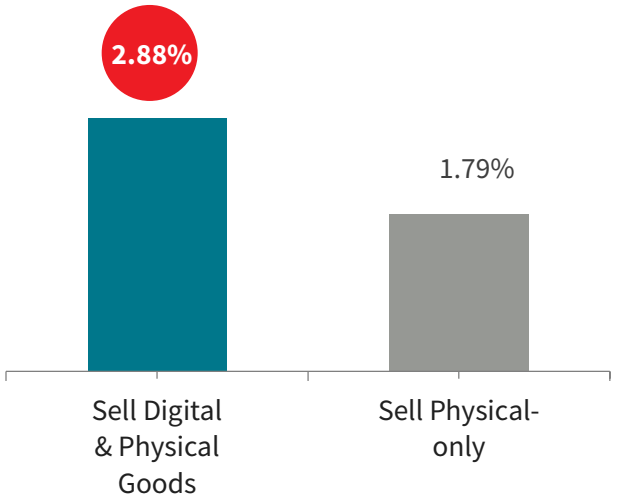
LexisNexis®
RISK SOLUTIONS

The cost of fraud is higher for those selling digital and physical goods

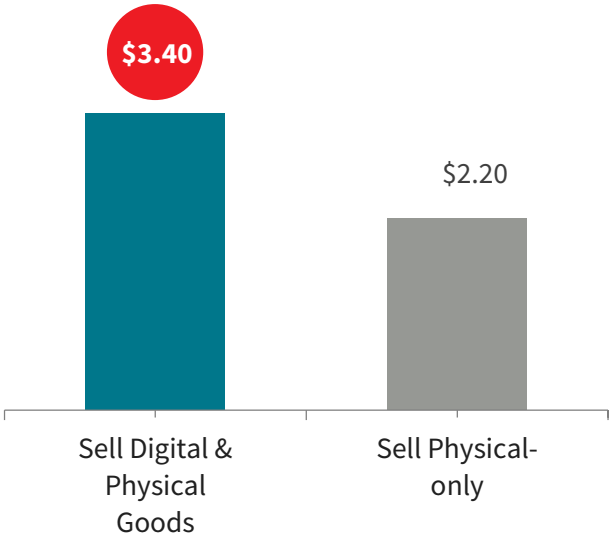
Fraud associated with digital goods, particularly e-gift cards, comes with a higher proportion of indirect losses, such as fees and interest, than physical goods. This drives up the LexisNexis Fraud Multiplier℠ per $1 of direct fraud losses (i.e. chargebacks).

When merchants selling physical goods experience fraud, a higher proportion of this is due to chargebacks (i.e. the cost of purchasing the good plus any refunds issued). This results in a lower LexisNexis Fraud Multiplier℠.

Fraud Costs as a % of Revenues



LexisNexis Fraud Multiplier℠



Q10: What is the approximate value of your company's total fraud losses over the past 12 months, as a % of total revenues?
Q16: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud costs over the past 12 months.

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

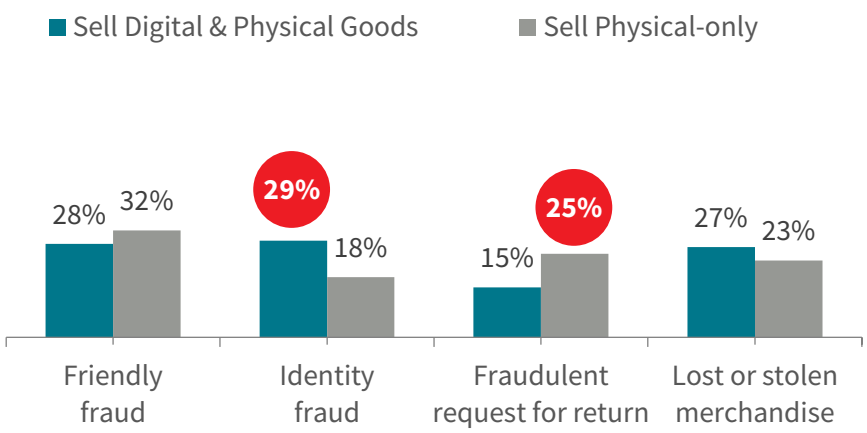
LexisNexis® RISK SOLUTIONS

Identity fraud likely drives higher costs among digital goods sellers, as it is much more of a problem for them

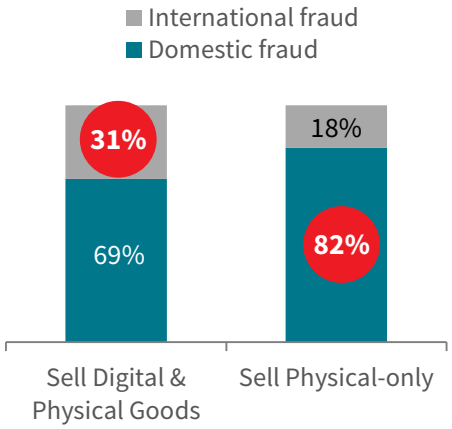
While most fraud losses for those selling digital goods are domestic, there is a sizeable portion (31% on average) that come from international sales. This international element, along with higher costs, seems to have an impact of tracking behaviors - a large majority of digital and physical goods e/m-commerce merchants are tracking fraud costs by channel or method. However, not by both.

Nearly half of physical-only goods merchants are not tracking fraud costs in either manner.

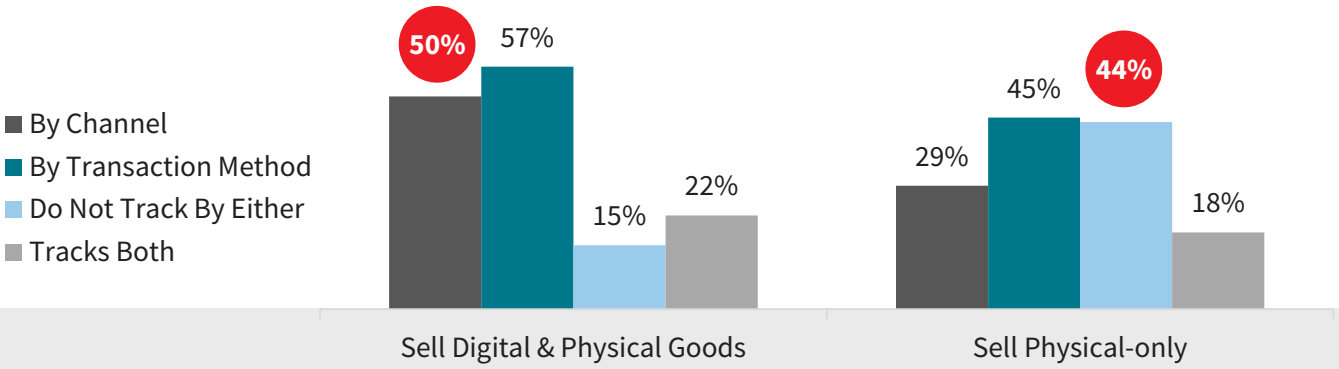
% Distribution of Fraud Losses by Method



% Distribution of Fraud Losses by Geo



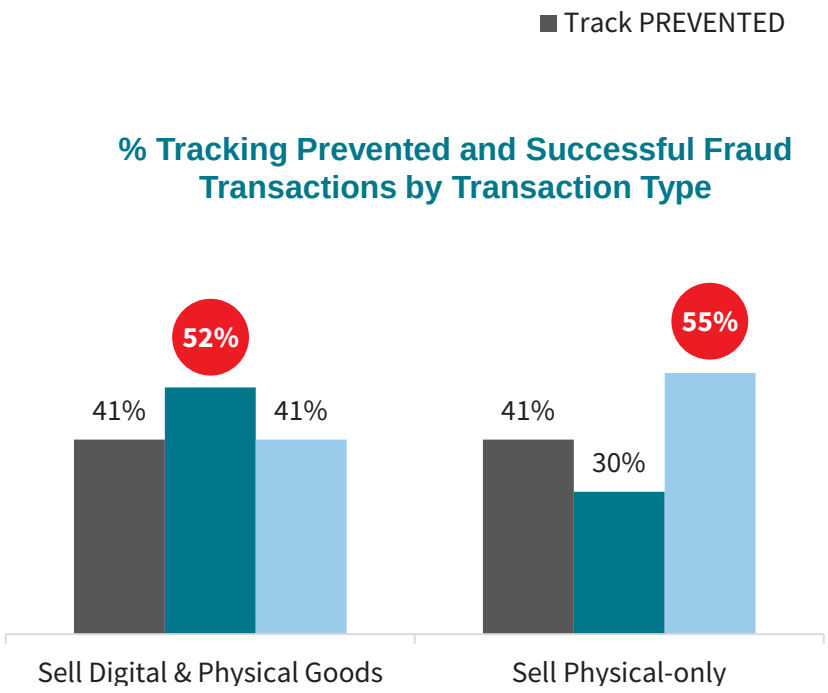
% Tracking Fraud Costs by Channel & Transaction Method

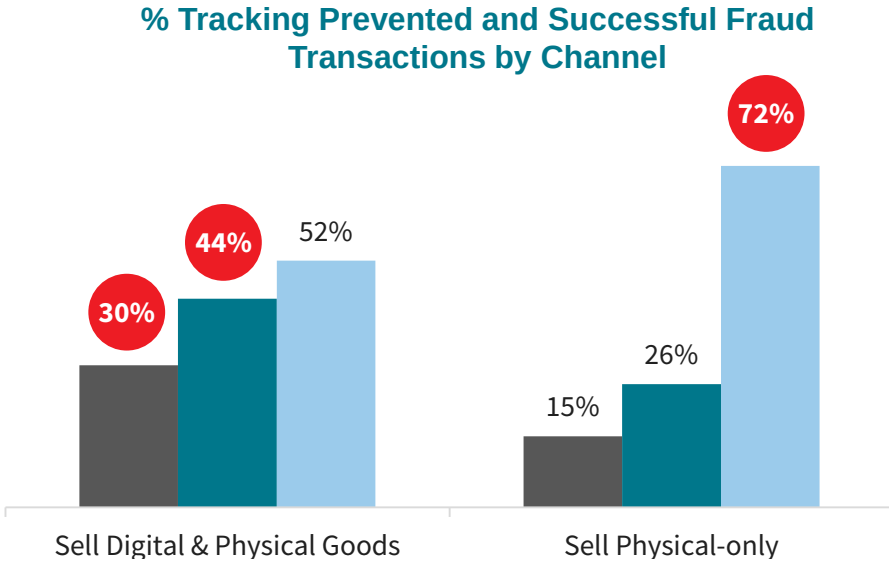


Q12: Please indicate the percentage distribution of the following fraud methods as attributed to your total annual fraud loss over the past 12 months.
Q13: Please indicate the percent of fraud costs generated through domestic orders compared to international orders in the last 12 months.
Q14: Does your company track the cost of fraudulent transactions by channels or methods?

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

Though e/m-commerce merchants selling digital and physical goods are more likely to track prevented vs. successful fraud transactions than others, half of these merchants aren't tracking at all





LexisNexis® RISK SOLUTIONS

Q26a: Does your company track prevented vs. successful transactions by type or channel?

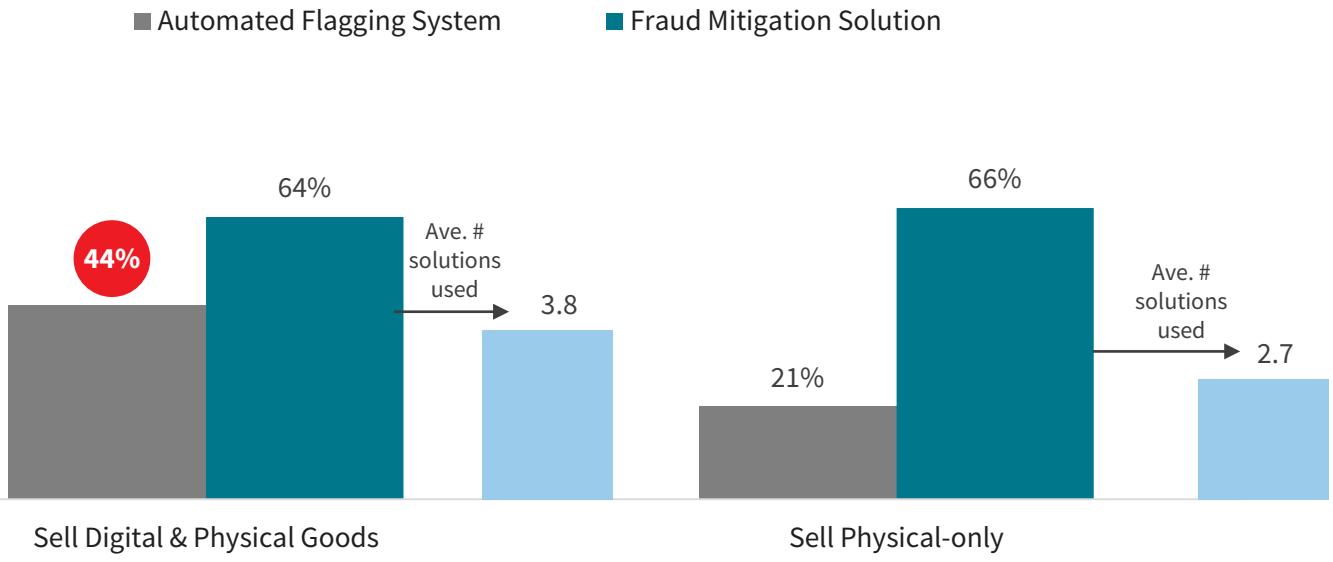
Significantly different from other segment within category at the 95% Confidence Interval

E/m-commerce merchants selling digital goods dedicate a large portion of their risk mitigation budgets to solutions (67%), but use a limited number of them

While they are more likely than physical goods-only merchants to also use an automate flagging system, this accounts for just under half of these retailers.

Physical goods-only merchants are just as likely to use fraud mitigation solutions, but in a more limited manner.

% Merchants Who Use an Automated Flagging System or Fraud Mitigation Solution



Ave. 67% of fraud mitigation budget dedicated to solutions

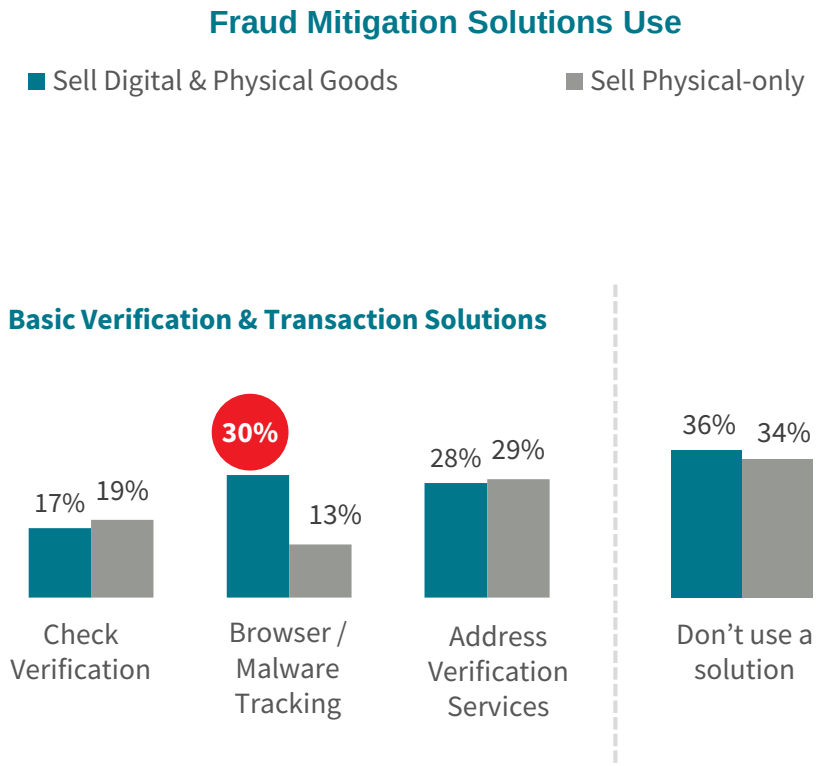
Ave. 54% of fraud mitigation budget dedicated to solutions

LexisNexis® RISK SOLUTIONS

Q27: Which of the following best describes your awareness and use of the fraud solutions listed below? Usage.
Q35: Does your company use an automated system to flag potentially fraudulent transactions?

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

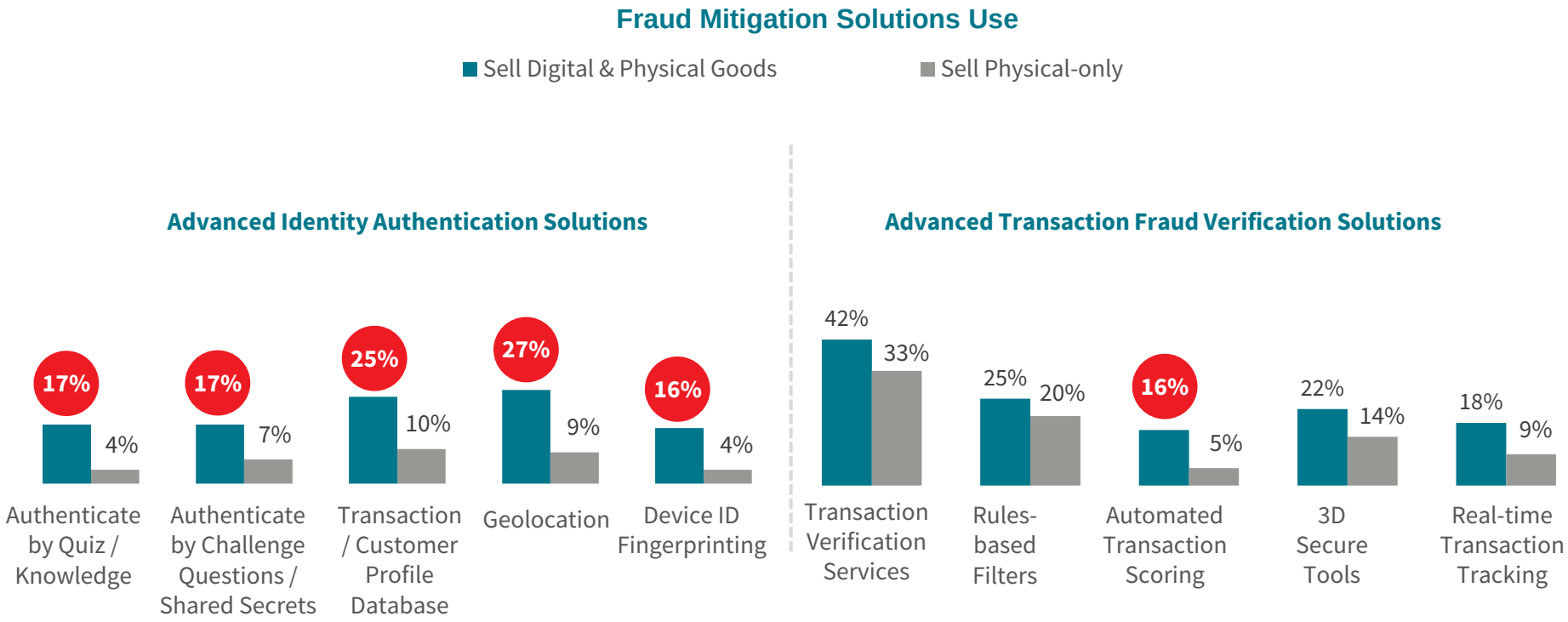
Different solutions used by digital and physical merchants for basic coverage



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

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

Many hybrid merchants (selling both physical and digital) are using physical-related goods solutions for digital goods screening



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

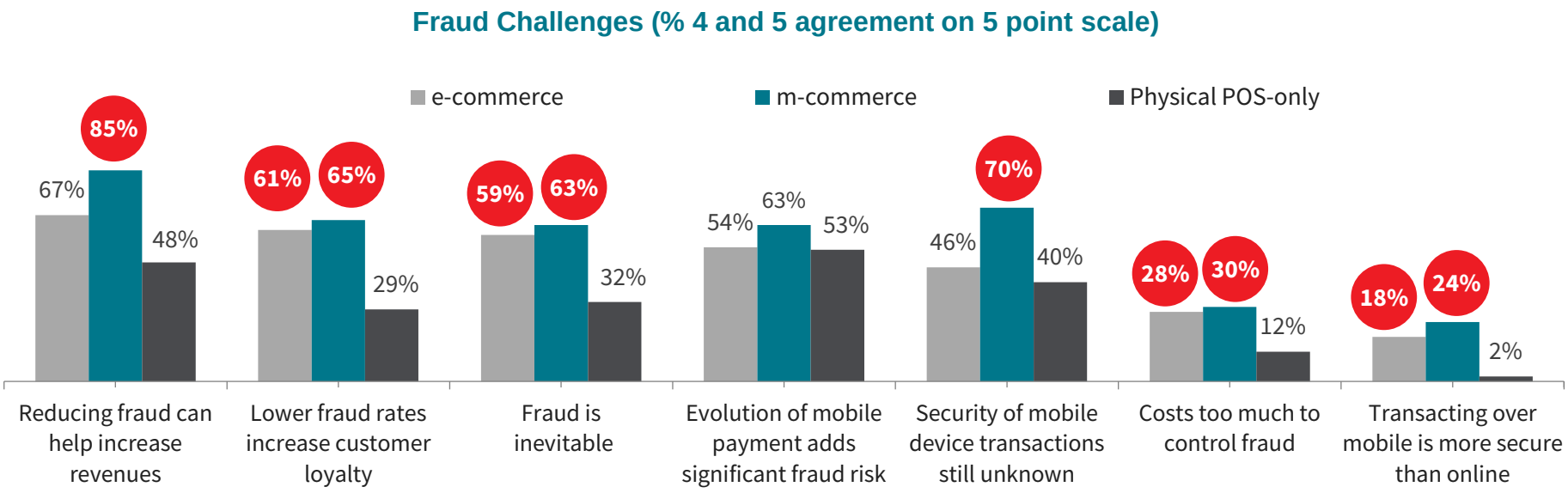
Significantly different from other segment within category at the 95% Confidence Interval

Findings by Channel

E-commerce
M-commerce
Physical POS

LexisNexis® RISK SOLUTIONS

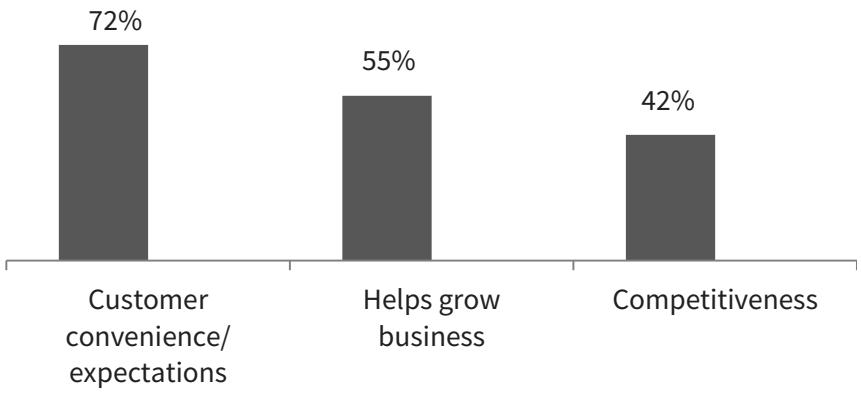
Merchants allowing m-commerce are doing so despite serious concerns regarding the security of mobile transactions



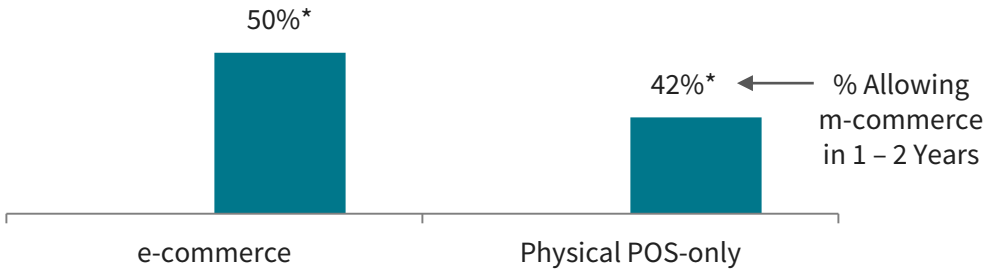
Despite understanding the benefits of fraud management, a sizable portion also feel that the cost of controlling fraud is too high.

Despite concerns, half of e-commerce merchants are considering m-commerce in the next 1-2 years. Interestingly, Physical POS-only merchants have similar expectations

Key Reasons For Allowing m-commerce



% Considering m-commerce



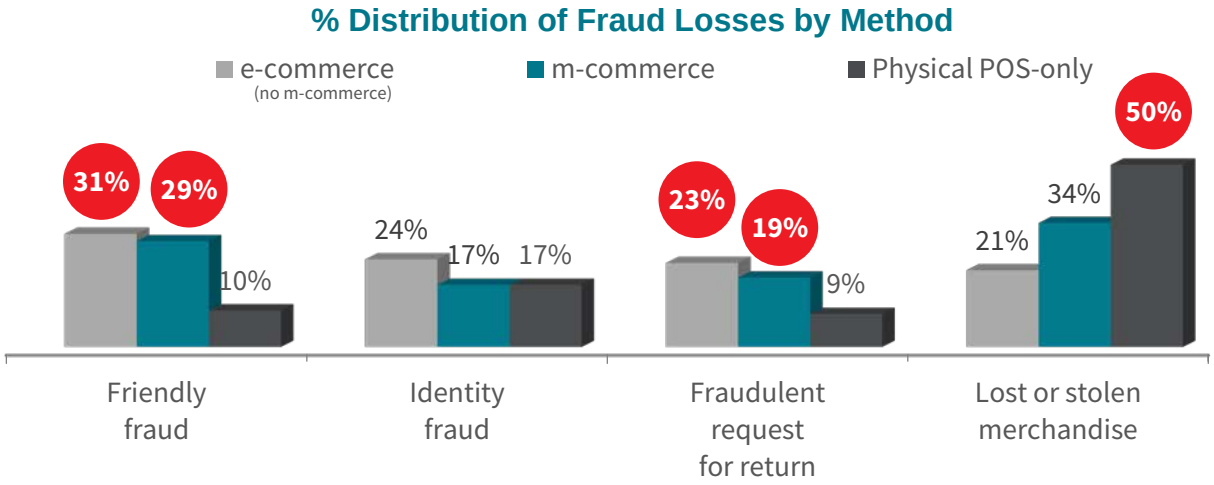
Q4: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment channels currently accepted by your company.
Q5: Why does your company accept payments by mobile device?
Q6: Is your company considering accepting mobile payments over the next 12 months?
*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.

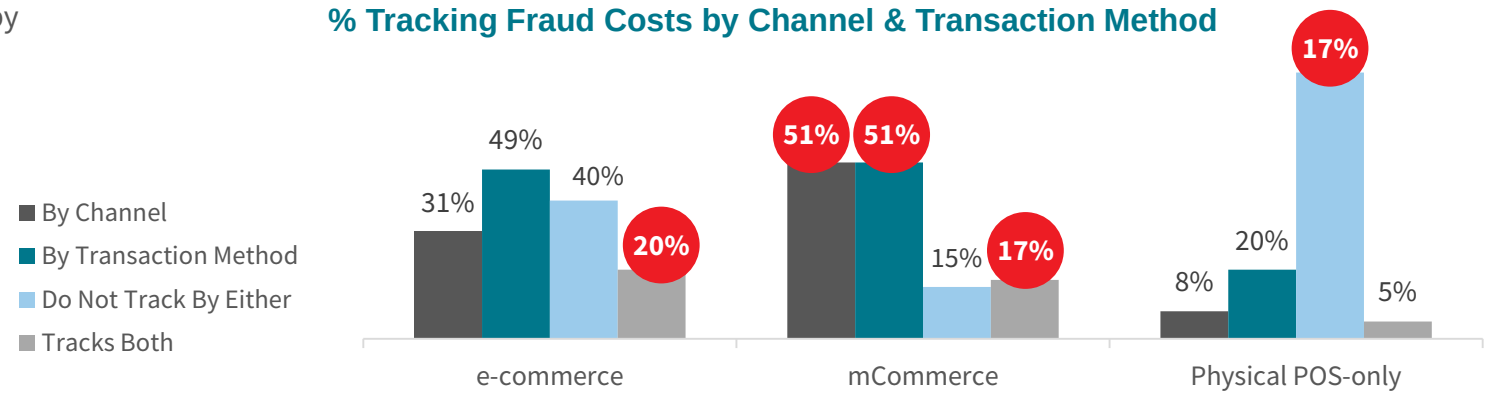
Significantly different from other segment within category at the 95% Confidence Interval

When it comes to fraud costs no one type contributes more than another

Remote merchants are less likely to track fraud costs by both channel and payment method.

Not surprisingly, merchandise losses are a significant issue for Physical POS-only merchants. Given this, they are even less likely to track fraud costs by channel and/or method.



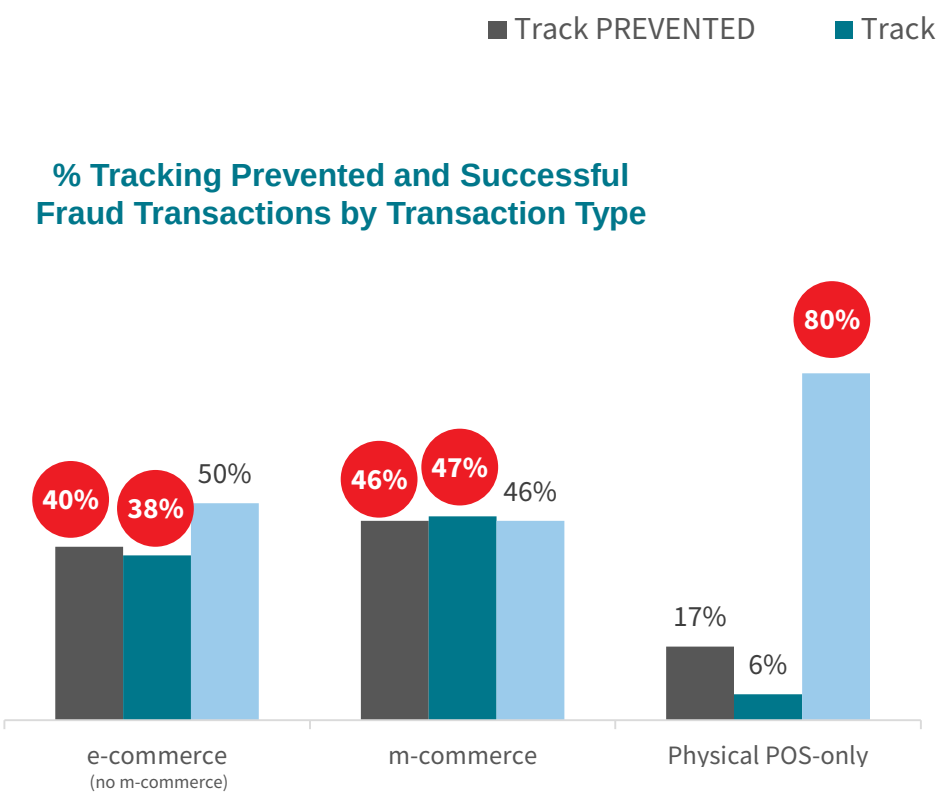


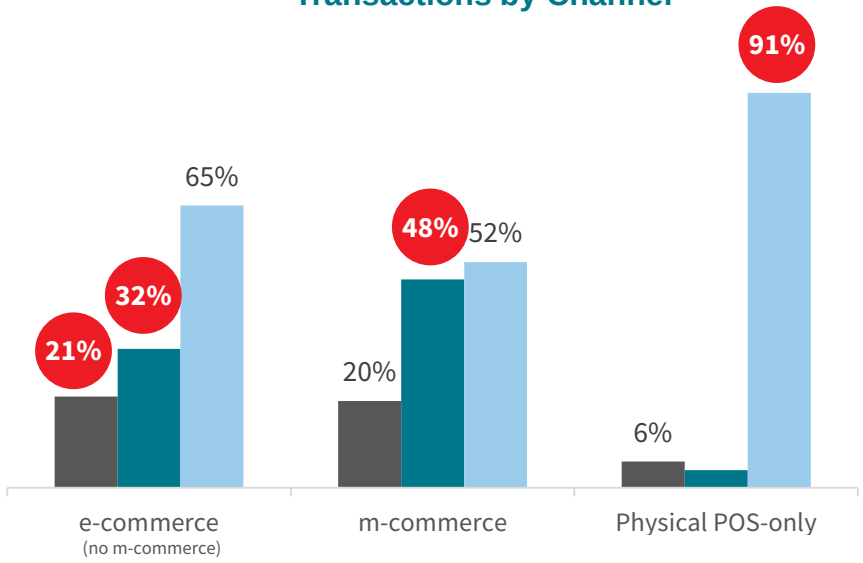
(no m-commerce)

Q12: Please indicate the percentage distribution of the following fraud methods as attributed to your total annual fraud loss over the past 12 months.
Q13: Please indicate the percent of fraud costs generated through domestic orders compared to international orders in the last 12 months.
Q14: Does your company track the cost of fraudulent transactions by channels or methods?

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

Limited tracking of prevented vs. successful fraudulent transactions leaves gaps for fraudsters





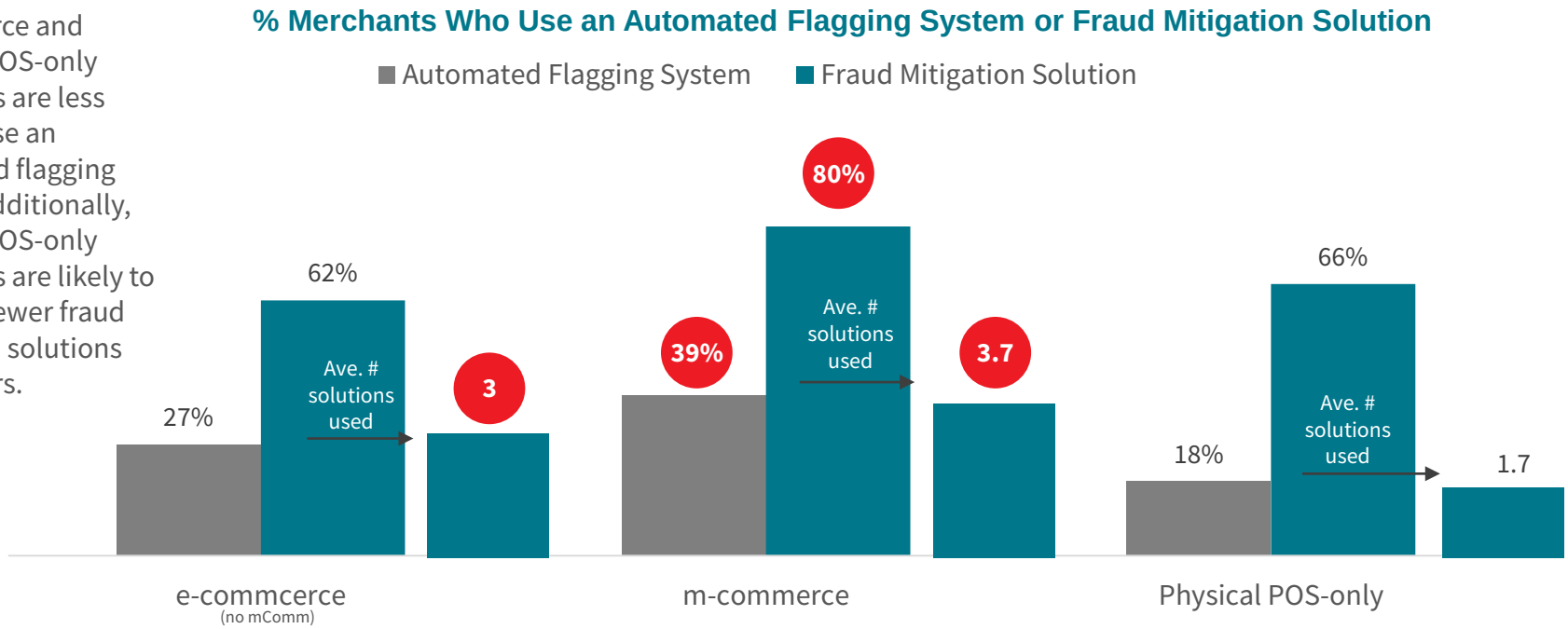
LexisNexis® RISK SOLUTIONS

Q26a: Does your company track prevented vs. successful transactions by type or channel?

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

M-commerce merchants dedicate a significant portion of their risk mitigation budgets to solutions (74%), but use a limited number of them

E-commerce and Physical POS-only merchants are less likely to use an automated flagging system. Additionally, Physical POS-only merchants are likely to be using fewer fraud mitigation solutions than others.



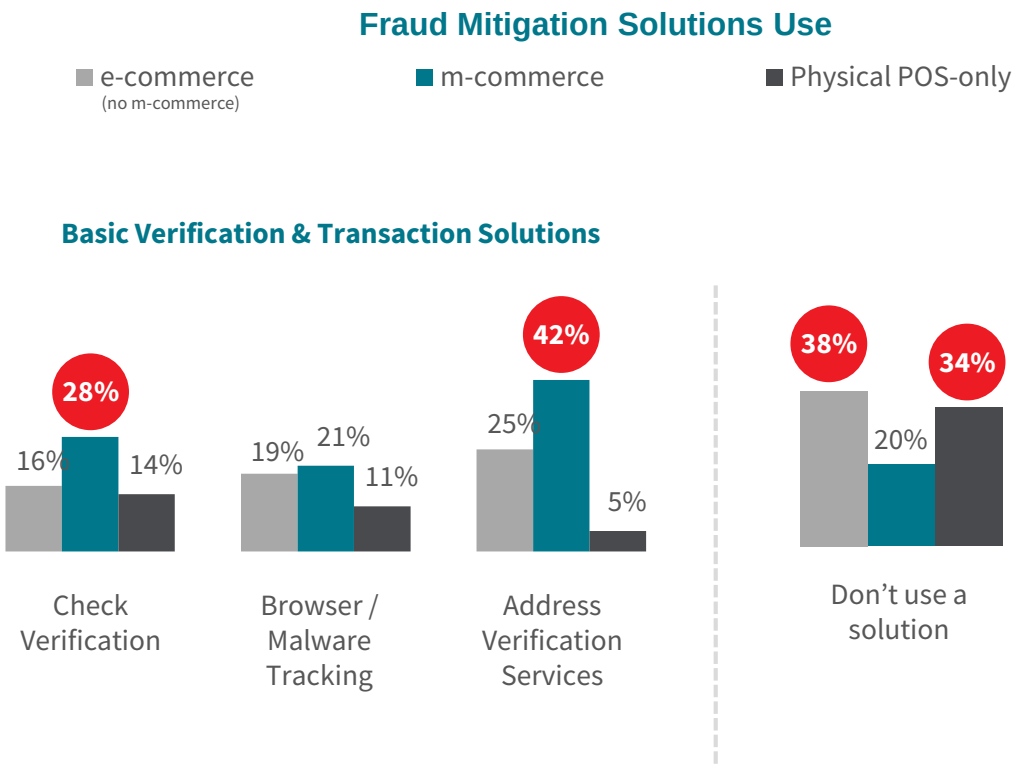
Ave. 57% of fraud mitigation budget dedicated to solutions

Ave. 74% of fraud mitigation budget dedicated to solutions

Q27: Which of the following best describes your awareness and use of the fraud solutions listed below? Usage.
Q35: Does your company use an automated system to flag potentially fraudulent transactions?

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

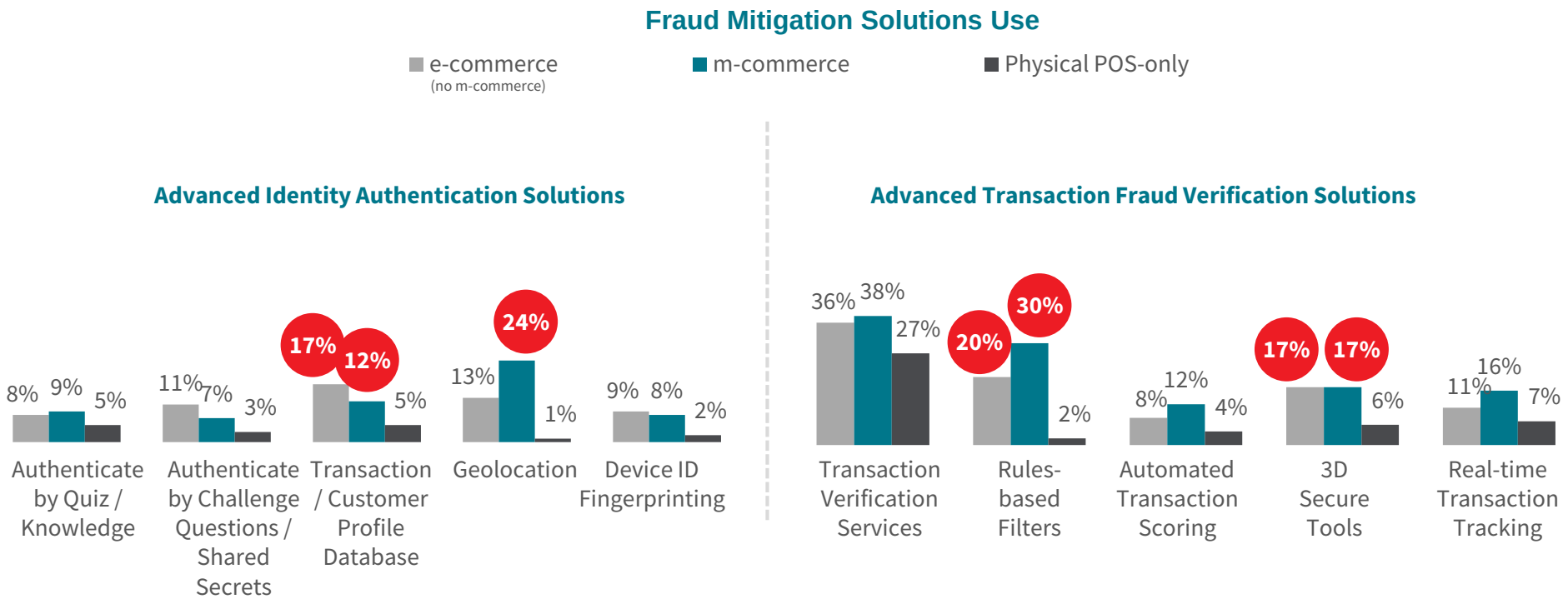
Solutions use is very fragmented



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

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

Implementation of advanced solutions represented less than half of merchants, regardless of channel

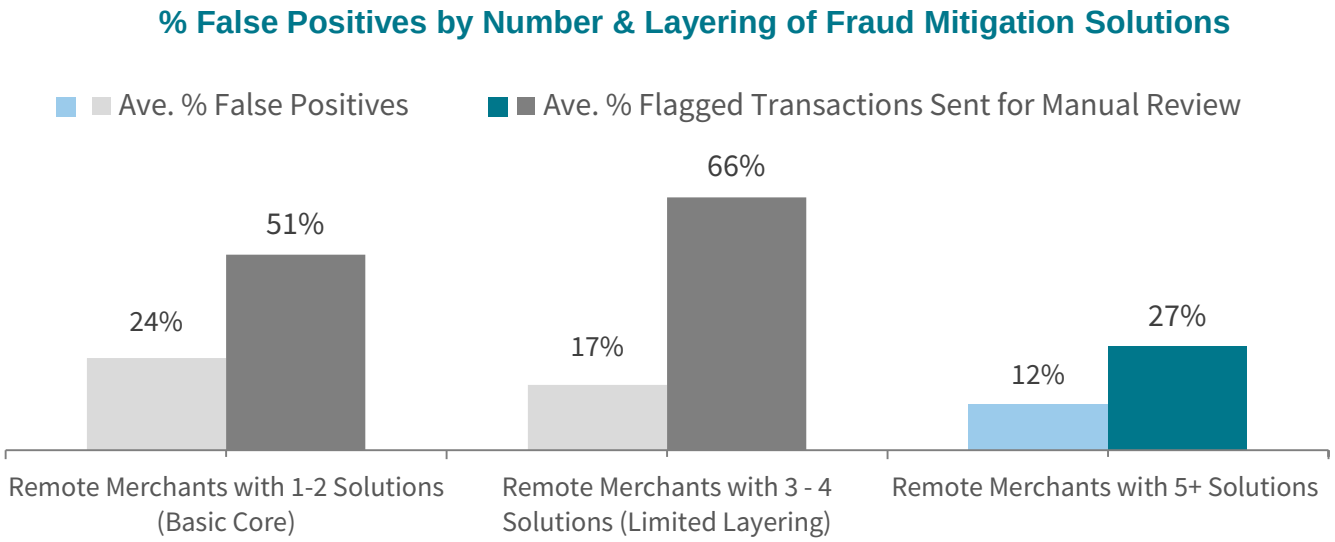


Using the right combination is crucial

LexisNexis®
RISK SOLUTIONS

E-commerce merchants which layer identity & fraud transaction-based protection solutions experience fewer false positives and need for manual reviews

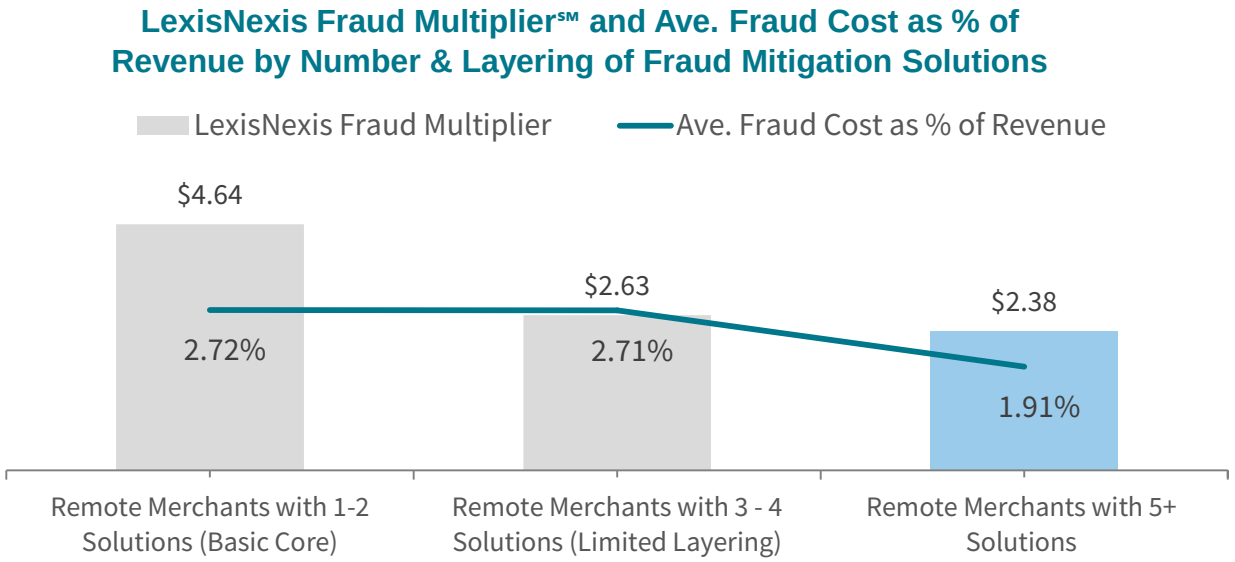
Survey findings show that e-commerce merchants who invest in a multi-layered solution approach including advanced identity and fraud transaction verification & authentication experience fewer false positives and required manual reviews.



	Layers of Protection	Basic	Some Layering	Multi-Layered
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, Customer Profile Database		✓	✓
Layering of Fraud Transaction Risk Assessment Solutions	Automated Transaction Scoring, Real-Time Transaction Tracking, Transaction Verification, Rules-Based Filters, Authentication of Transaction by 3D Tools			✓

And, there is less cost of fraud for e-commerce merchants who layer identity & fraud transaction-based protection

eCommerce merchants who layer core + identity + fraud transaction solutions have lower fraud costs ($2.38 for every $1 of fraud) than others (up to $4.64 per $1 of fraud). Relatedly, those who layer these solutions have lower fraud costs as a percent of annual revenues.



	Layers of Protection	Basic	Some Layering	Multi-Layered
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, Customer Profile Database		✓	✓
Layering of Fraud Transaction Risk Assessment Solutions	Automated Transaction Scoring, Real-Time Transaction Tracking, Transaction Verification, Rules-Based Filters, Authentication of Transaction by 3D Tools			✓

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

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

Recommendations

LexisNexis®
RISK SOLUTIONS

Recommendation #1

E-commerce merchants should implement different risk mitigation solutions to address unique risks from different channels and sales 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 require specific solutions** that support domestic versus international remote channels.

And, the very nature of mobility means that mobile-based **payment transactions and devices carry different levels of risk and challenges** with regard to identity and device verification than with online / Internet browser transactions.

Recommendation #2

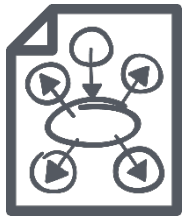
It's not just about the number of risk mitigation solutions, but rather the most effective multi-layered approach that attacks different types of fraud.

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.



Recommendation #3

E-commerce merchants need to track both payment and channel fraud – in terms of costs and successful attempts.

- Fraud occurs in multiple ways, particularly for merchants using both the online and mobile channels and / or selling digital and physical goods. The nature of mobile apps payments involves different technology and security features than Internet browsers. **The addition of a 3rd party payment providers (“middle man”) adds another point of risk.**
- **Tracking is essential** for knowing how and where to apply preventative solutions. Gaps will remain unless done so holistically.

Recommendation #4

Mid/large e-commerce merchants selling digital goods need to remain particularly 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. And, this will become more heightened as more of these merchants adopt the mobile channel in the near-term.
- **E-gift card fraud has become an issue**, without regulated protection with smaller transactions.
- **A layered solution approach should particularly consider those which support faster / real-time identity and transaction verification decision making**.

Recommendation #5

Fraud isn't just occurring among mid/large. Smaller e-commerce firms should invest in a layering of identity and transaction verification solutions, as well as increase vigilance through fraud tracking.

- Smaller e-commerce merchants will continue to experience a high percentage of fraud among monthly transactions until criminals become thwarted.
- **Over time, the cost of solutions should prove a justifiable ROI** compared to the dollars that are continually lost on an ongoing basis – which, of course, adds up to unnecessary significant losses over time.