LexisNexis® Risk Solutions 2019 True Cost of Fraud℠ Study

U.S. Retail Edition

LexisNexis® RISK SOLUTIONS

The LexisNexis® Risk Solutions 2019 US Retail True Cost of Fraud℠ Study helps merchants grow their business safely and manage the cost of fraud, while strengthening customer trust and loyalty.

The research provides a snapshot of:

Current fraud trends in the US retail and e-Commerce market

Key pain points related to adding new payment mechanisms, transacting though online and mobile channels, & expanding internationally

Fraud Definitions

- Fraud is defined as the following:
  - Fraudulent and/or unauthorized transactions;
  - Fraudulent requests for refund/return; bounced checks; and
  - Lost or stolen merchandise, as well as redistribution costs associated with redelivering purchased items
- This research covers consumer-facing retail fraud methods
  - It does not include insider fraud or employee fraud
- The LexisNexis Fraud Multiplier℠
  - Estimates the total amount of loss a merchant incurs based on the actual dollar value of a fraudulent transaction

LexisNexis® RISK SOLUTIONS

The study included a comprehensive survey of 700 U.S. risk and fraud decision makers . . .

Across a variety of retail and e-Commerce categories

Including the following retail and e-Commerce segments…

	Small Retailers	Mid/Large Retailers	Retailers w/ m-Commerce	Retailers w/ Digital Goods
# completions:	481	219	317	288

	Small e-Commerce Merchants	Mid/Large e-Commerce Merchants	e-Commerce Merchants w/ m-Commerce	e-Commerce Merchants w/ Digital Goods
# completions:	160	40	70	72

Segment Definitions:

Small Earn <$10 million in annual revenues

Mid/Large Earn $10 million+ in annual revenues

Retailers with e-Commerce
May accept payments through multiple channels, but earn at least 10% of their revenue from the online channel

E-Commerce Merchants
Earn a large majority of revenues through the online/mobile channels

With m-Commerce
Accept payments through either a mobile browser or app, or "bill to mobile phone"

LexisNexis® RISK SOLUTIONS

Research was conducted in January - March 2019.

Key Findings

LexisNexis®
RISK SOLUTIONS

Key Findings

1

U.S. retail fraud has grown significantly during the past year, with more and different types of retailers being impacted. This translates into sharply increasing fraud volumes and costs.

- ✓ Overall **fraud attempts have doubled** year-over year and tripled since 2017.
- ✓ **Fraudsters have begun targeting more types** of retailers and e-Commerce merchants, including small businesses.
- ✓ This has **resulted in an increasing cost of fraud**. Every $1 of fraud now costs retailers $3.13 compared to $2.94 a year ago.

2

A number of trends are increasing fraud risk for retailers and e-Commerce merchants.

- ✓ The number of businesses allowing m-Commerce has expanded beyond the traditional mid/large bricks/mortar retailer which sells digital goods and services. Small retailers with digital goods and services along with mid/larger retailers and e-Commerce merchants that sell physical goods have entered this space.
- ✓ Digital goods and services are being offered by more retailers and merchants.
- ✓ More international transactions are taking place.
- ✓ More automated botnet activity is occurring.
- ✓ The insidious nature of synthetic identities continues to be prevalent.

LexisNexis® RISK SOLUTIONS

Key Findings (cont.)

3

These trends are making identity verification and the ability to balance fraud detection with minimal customer friction harder. This is particularly true for mobile channel transactions.

- ✓ Across retail and e-Commerce businesses, verifying customer identity, the inability to determine transaction source, the inability to distinguish between human and malicious bots and minimizing customer friction are top ranked mobile channel challenges.
- ✓ Study findings show a link between synthetic identities, automated botnet attacks and identity verification challenges.

4

This is translating into a perfect storm of increased fraud for merchants with cross-border, digital and mobile channel transactions.

- ✓ Fraud attacks have increased among these types of retailers and e-Commerce merchants.
- ✓ Fraud from the mobile channel has increase, with mobile apps usage being a key contributor.
- ✓ Account-related fraud is a significant portion of identity-related fraud.
- ✓ Payment card fraud has risen.
- ✓ And, the cost of fraud for these types of businesses continues to trend upwards.

Key Findings (cont.)

5

But, as fraud continues to become more sophisticated, the use of more sophisticated solutions remains limited.

- ✓ Fraud is not a one-size fits all. The risks posed by digital goods is higher than when selling physical goods; the ability to detect fraud in the remote channels, particularly mobile, is harder than doing so in-store. The ability to distinguish between a legitimate customer and a fraudster is very difficult when the criminal is using a synthetic identity with real personally identifiable information.

- ✓ Different solutions need to be applied for different channels and types of transactions. These should assess fraud for both the identity and the transaction, using physical and digital identifying information.

- ✓ However, retailers and merchants appear to still be using a limited set of solutions to cover all channel and transaction risks. Those newer to m-Commerce are particularly at-risk; they tend to have embraced this channel without investing in solutions to meet specific threats from m-Commerce.

- ✓ Study findings show that those retailers and merchants which use a layered solution approach involving identity authentication and transaction verification, including digital identity / behavior biometric tools, experience a lower cost of fraud.

1

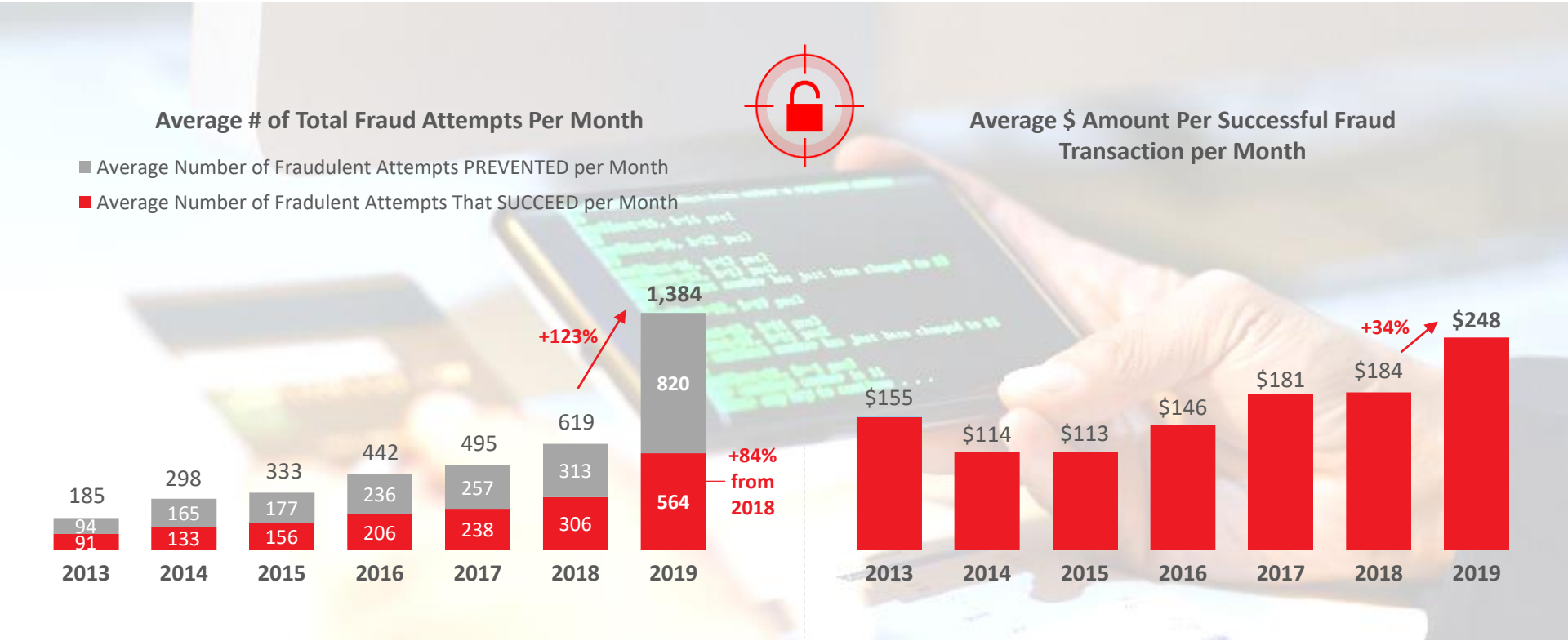
U.S. retail fraud has grown significantly in terms of attacks and cost.

- ✓ Fraud attempts have doubled.
- ✓ Fraudsters are targeting a broader set of retailers and e-Commerce merchants.
- ✓ The cost of fraud continues to rise.

LexisNexis®
RISK SOLUTIONS

Overall fraud *attempts* have doubled year-over-year, and tripled since 2017.

And the number of *successful* fraud transactions alone have **grown by 84%** since just last year. Not only has the number grown, but the dollar amount of these transactions has increased to nearly $250 on average.



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?
Q25: What is the average value of successful fraud transactions?

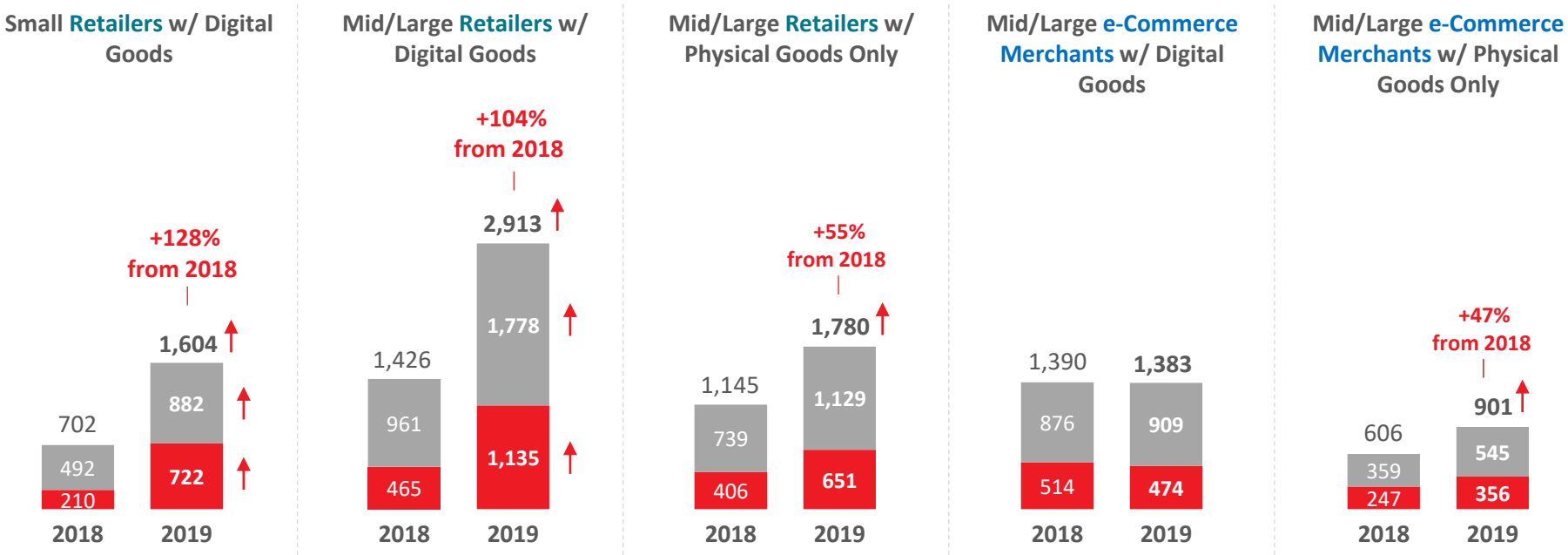
And fraudsters have begun targeting more types of retailers and e-Commerce merchants.

The average volume of monthly fraud attacks is **highest for mid/large retailers selling digital goods**, but continues to remain high for mid/large e-Commerce merchants with digital goods as well.

However, fraud volume has grown significantly among other segments that have seen less fraud activity in previous years, **particularly smaller retailers selling digital goods** and **mid/large retailers and e-Commerce merchants that sell only physical goods**.

Average # of Total Fraud Attempts Per Month

- Average Number of Fraudulent Attempts PREVENTED per Month
- Average Number of Fradulent Attempts That SUCCEEDED per Month



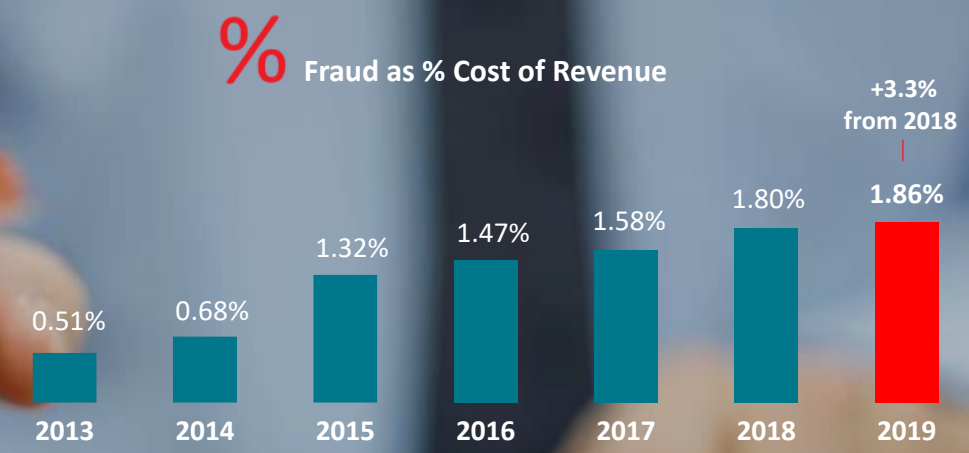
LexisNexis® RISK SOLUTIONS

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 by fraudsters?

↑ Significantly different from 2018 within Segment

This has resulted in an increased cost of fraud.

Fraud losses as a percentage of annual revenue continues its upward trend since 2015.



The cost for each dollar of fraud losses is **up 6.5% from last year**, crossing over the $3 mark to come in at **$3.13**. This cost involves increased expenses related to chargebacks, fees, merchandise redistribution, labor/investigation, legal prosecution and IT/software security.

As shown later, the increased cost of fraud is based on a combination of factors.

LexisNexis® RISK SOLUTIONS

*Estimates the total amount of loss a merchant occurs based on the actual dollar value of a fraudulent transaction, which includes not only the chargeback/face value of the transaction, but also costs associated with fees, merchandise redistribution, and labor/investigation.

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

2

A number of trends are increasing fraud risk for retailers and e-Commerce merchants.

- ✓ Mobile channel use is expanding.
- ✓ More digital goods/services are being offered.
- ✓ More international transactions are taking place.
- ✓ More automated botnet activity is occurring.
- ✓ The insidious nature of synthetic identities continues to be prevalent.

LexisNexis®
RISK SOLUTIONS

Use of the mobile channel has expanded significantly, with newer adoption from small retailers that sell digital goods and mid/large retailers and e-Commerce merchants that sell physical goods only.

This aligns with consumer demand and behavior for more remote purchasing options and is reflected by significant growth of mobile shopping during the 2018 holiday season.[1]

Adding these additional segments to earlier adopters of the mobile channel (mid/large retailers and e-Commerce merchants that sell digital goods) broadens the landscape for fraudsters.

[1] https://www.pymnts.com/mobile/2018/paypal-smartphones-holiday-shopping-cyber-monday/

*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?

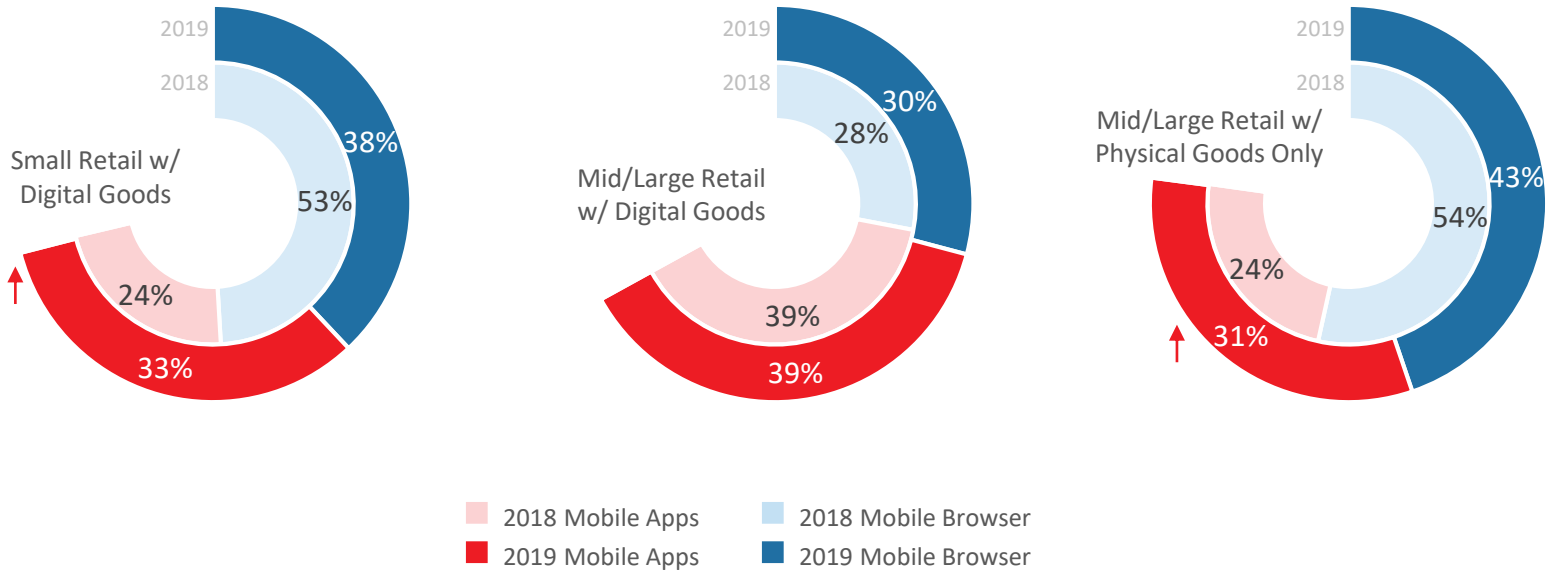
↑ Significantly different from 2018 within Segment

LexisNexis® RISK SOLUTIONS

While mobile browsers continue to be a major source for m-Commerce transactions, the use of mobile apps has significantly increased to be a comparable option.

This increase comes from segments that have seen new entrants to the mobile channel, suggesting that those who have recently added this option recognize the speed with which mobile app use is growing – and the way in which mobile apps provide a faster direct-to-the-customer experience.

% Distribution of Mobile Channel Transactions Completed by Platform



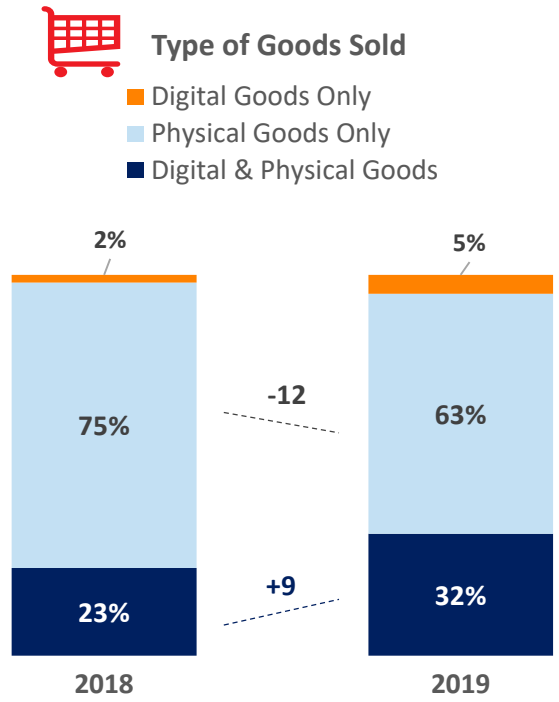
LexisNexis® RISK SOLUTIONS

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.

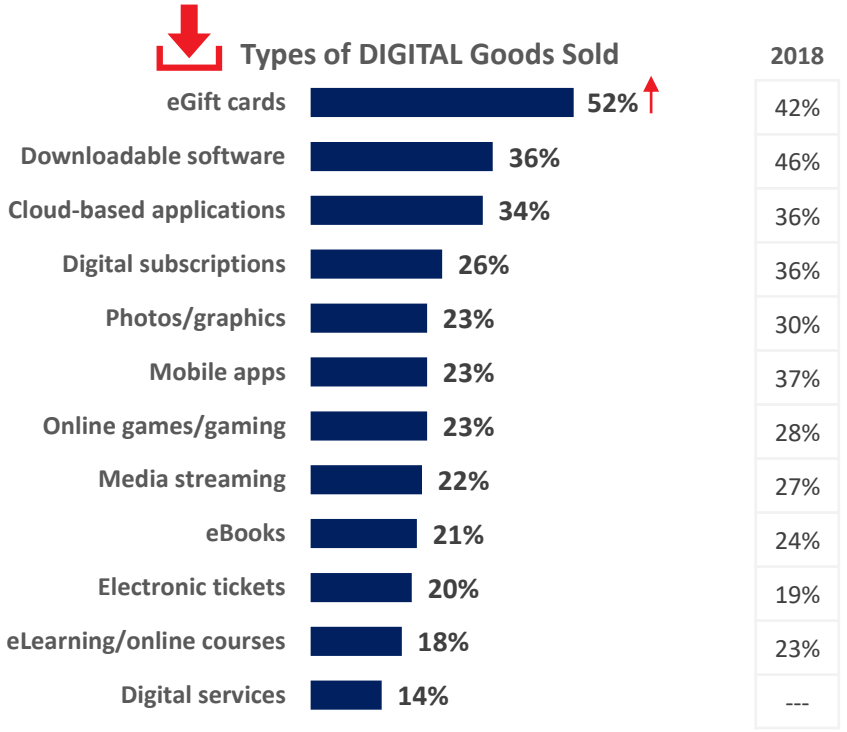
↑ Significantly different from 2018 within Segment

There has been growth in the number of retail and e-commerce businesses that offer digital goods/services.

Fewer merchants report selling **only** physical goods, with a number having added digital goods to their offerings. The incidence of digital-only merchants has remained at similar levels, while the incidence of mixed digital and physical goods merchants has increased.



This could be driven, in part, by an increase in the number of retailers indicating the sale of e-gift cards.



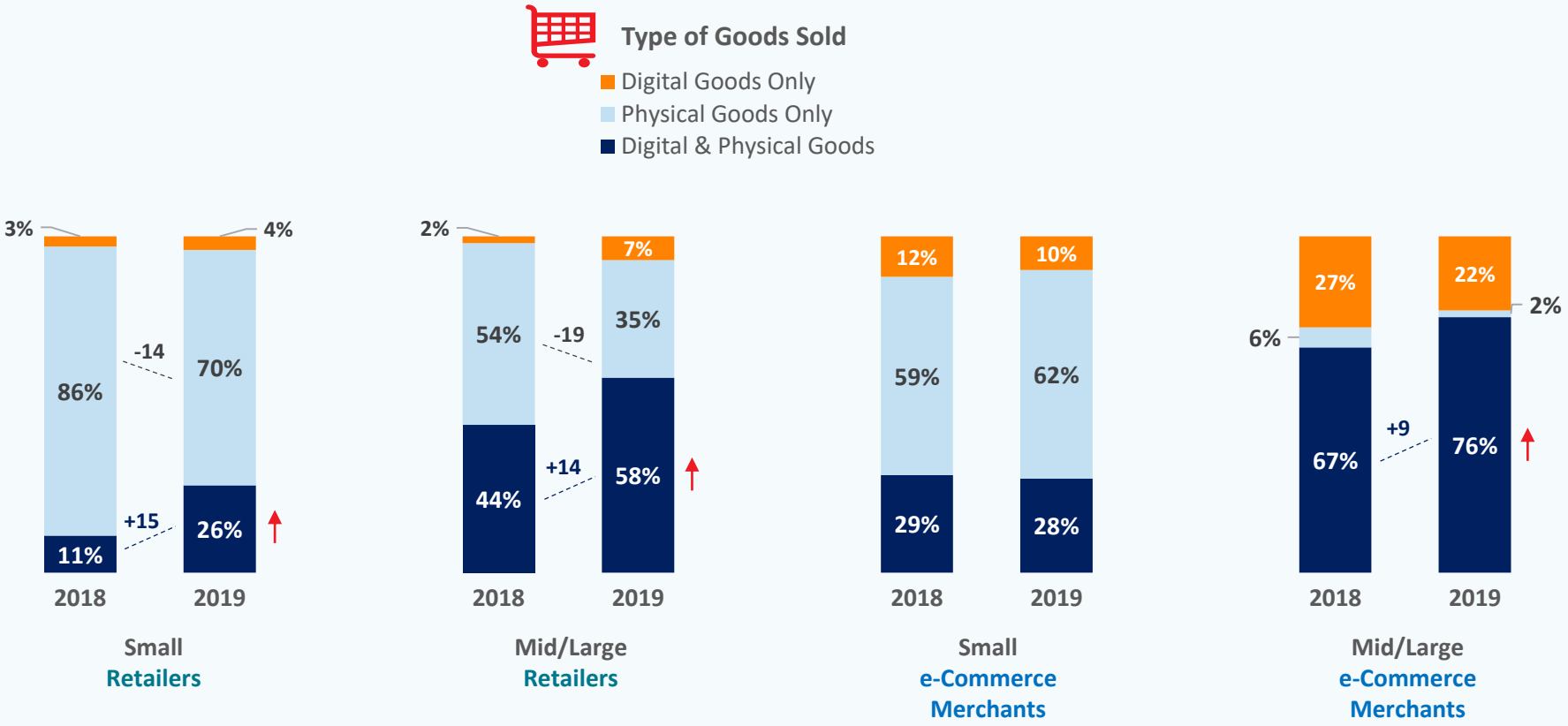
But merchants with eGift cards need to remain vigilant and employ strong fraud detection tools. Fraudsters are using more sophisticated synthetic identities and stolen credit card accounts to obtain these to then resell. Since gift cards, in general, tend to involve lower dollar amounts, fraudsters are often able to remain under the radar.

LexisNexis® RISK SOLUTIONS

D1: Please indicate the type of products sold by your company (physical, digital)?
D1b: What types of digital goods are sold by your company?

↑ Significantly different from 2018 within Segment

While mid/large retailers and e-Commerce merchants are more likely to offer digital goods, the number of small retailers offering these has more than doubled year-over-year.



LexisNexis® RISK SOLUTIONS

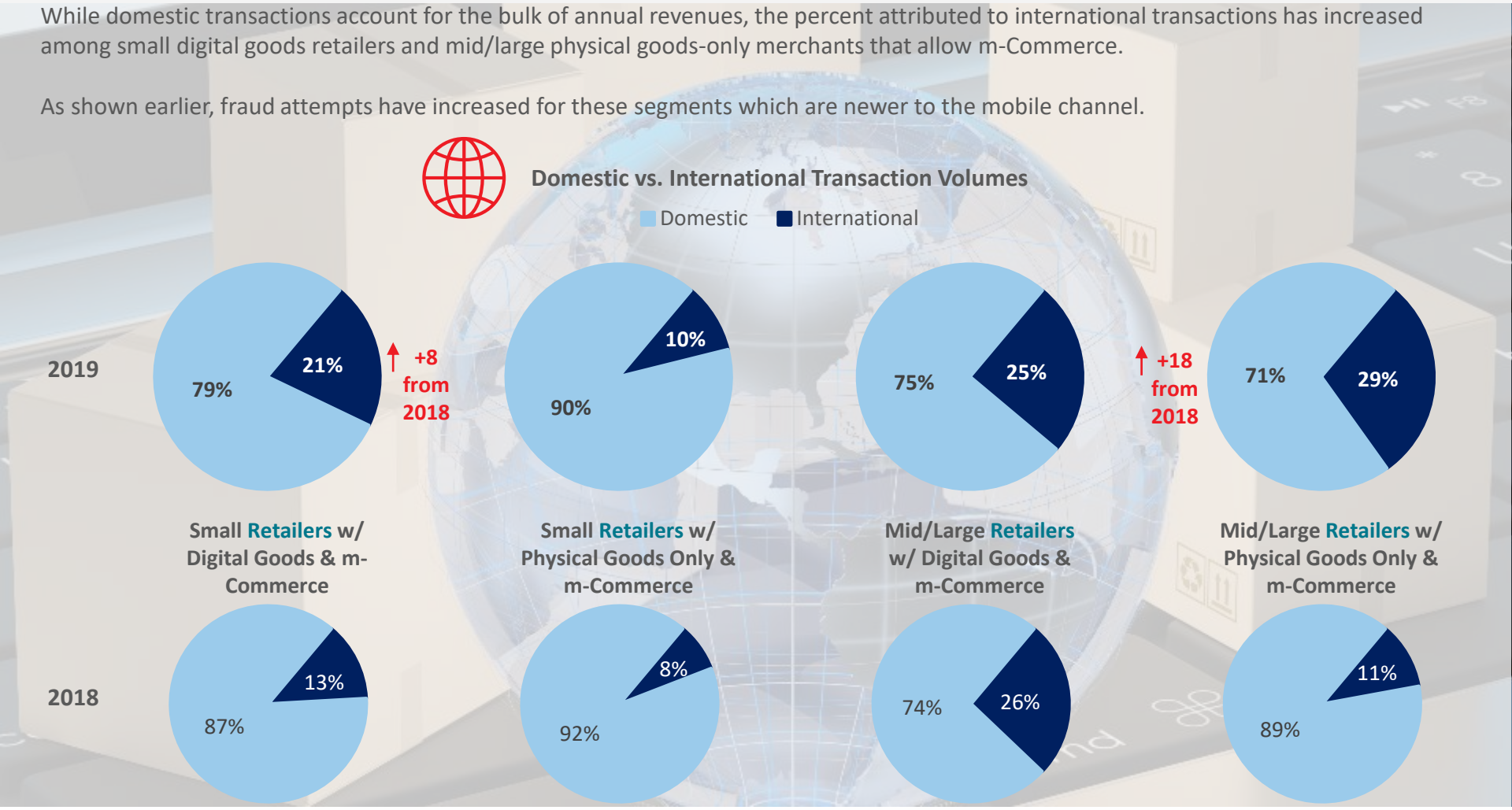
D1: Please indicate the type of products sold by your company (physical, digital)?

↑ Significantly different from 2018 within Segment

And, there has been an increase in the volume of international transactions.

While domestic transactions account for the bulk of annual revenues, the percent attributed to international transactions has increased among small digital goods retailers and mid/large physical goods-only merchants that allow m-Commerce.

As shown earlier, fraud attempts have increased for these segments which are newer to the mobile channel.



LexisNexis® RISK SOLUTIONS

Q9: Please indicate the percent of annual revenue generated through domestic compared to international transactions in the last 12 months.

↑ Significantly different from 2018 within Segment

So, why is mobile, digital and international more risky?

Mobile

- **Rise of mobile botnet attacks**; malware infects devices without consumer knowledge; steals identity, hacks accounts, makes fraudulent purchases[2]
- **Consumer risk behaviors** – using open WiFi networks increases risk of smishing (SMS-based phishing) and man-in-the-middle interception of passcodes used for multi-factor authentication[3]; "keep me logged in" habits become an unlocked entry point to accounts
- **Increasing pool for fraudster opportunity** as more people conduct mobile transactions

Cross Border

- **Uncertainties, blind spots and new payment methods**; it becomes difficult to determine transaction origination; lack of verifiable data on consumers in other markets (particularly with GDPR)

Digital

- **Fast transaction**; digital goods/services, such as downloads and subscriptions, tend to occur quickly; lack of a physical delivery address eliminates buffer period for fraud verification before shipment; with fear of abandonment, merchants struggle with balancing fraud prevention and minimizing customer friction.

- **Favorite target for fraudster card testing**; use of bots to test stolen credit card information with lower value goods/services (typical of digital goods/services) tend to arouse less suspicion.
- **Easy targets**; synthetic identities and stolen data make it difficult to distinguish between malicious attacks and legitimate customers in the anonymous channel.

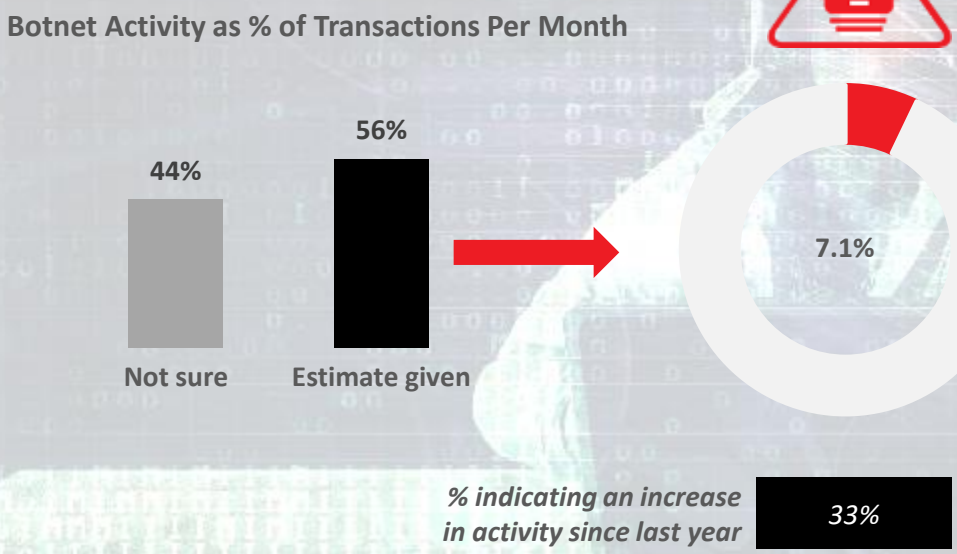
LexisNexis® RISK SOLUTIONS

[2] ThreatMetrix® H2 2018 Cybercrime Report
[3] 4 Mobile Fraud Trends to Look for in 2019; https://threatmetrix.com/digital-identity-blog/fraud-prevention/4-mobile-fraud-trends-look-out-for-2019

↑ Significantly different from 2018 within Segment

Automated botnet activity is reportedly increasing, though many merchants are unable to quantify the level at this point.

Among those who have estimates, this activity appears to target mid/large retailers somewhat more than small, especially those offering m-Commerce and selling digital goods.



When it comes to Botnets, there is a distinction between those that are human/manually launched and those that are automated. According to ThreatMetrix®, a LexisNexis® Risk Solutions Company, the 2018 Thanksgiving holiday shopping week involved a high volume of automated bot attacks.[4]

These involve the specific types of risk mentioned on the previous slide:

- ✓ **A number were mobile bots**, with a significant increase from early 2018;
- ✓ **These mobile bots steal credentials** and identity data for account takeovers and fraudulent purchases;
- ✓ Stolen credentials were likely **used for card testing**; and
- ✓ Bots originated not just from the United States, but other regions including Asia.[5]

LexisNexis® RISK SOLUTIONS

[4] ThreatMetrix® H2 2018 Cybercrime Report
[5] Ibid

B1a: In a typical month, what percent of your transactions are determined to be malicious automated bot attacks?
B1b: How does this compare to the same time last year? Would you say the percent of monthly automated malicious bot attacks has:

Synthetic identities are a serious threat. Their very nature makes it extremely difficult to detect before damage is incurred.

Synthetic identities are comprised of real and/or fake personal information. They are created by using information from either:

Multiple real persons into a single fake identity, with a valid shipping address, Social Security Number (SSN), date of birth, name, etc. – none of which matches any one person. This type may be used for shorter-term fraud gains, such as bigger ticket items.

One real person by using some of his / her information combined with fake data. In this case, the fraudster is likely to be nurturing this identity, using it to establish a good credit history before ultimately "going bad".

No known persons in which the personally identifiable information doesn't belong to any consumer. It is entirely fabricated based on a new SSN, using the same range as the Social Security Administration for randomly-issued numbers. This may also be nurtured for longer-term gain and is useful when posing as an underbanked consumer with a less established purchasing footprint (i.e., younger Millennials).

Risks & Challenges

Extremely Hard to Distinguish from Legitimate Customers

✓ Focus on nurturing the identity to mimic a good customer; establishes good credit, pays on-time, etc. before "breaking bad"

Difficult to detect with traditional identity verification / authentication solutions

✓ These are professional fraudsters; they often know the types of information required to gain approval and pass certain checkpoints. Use of real identity data helps them do this.

Real customers don't help; behaviors make it difficult to spot anomalies with current ID solutions.

✓ Consumers have more ways to purchase, from different locations anywhere and anytime. They might share passwords and use different devices at different times. It is harder to make physical and digital connections that distinguish fraudulent from legitimate patterns.

LexisNexis® RISK SOLUTIONS

3

These trends are making identity verification and the ability to balance fraud detection with minimal customer friction harder.

LexisNexis®
RISK SOLUTIONS

Identity verification has become an even greater challenge for m-Commerce since 2018, impacting efforts to determine fraud while minimizing customer friction.

Top Ranked Mobile Channel Challenges*

Verifying Customer Identity

Increase from 2018 (32% to **43%**)

Ranked among Top 3 by all retail and e-Commerce segments **when selling digital goods**

Small retailers (42%)
Mid/large retailers (38%)
Small e-Commerce (60%)
Mid/large e-Commerce (46%)

Inability to determine source / origination of transaction when selling digital goods internationally

Small retailers (23%)
Mid/large retailers (33%)

Small e-Commerce (37%)
Mid/large e-Commerce (31%)

Balancing fraud prevention with customer friction when selling digital goods

Small retailers (36%)
Mid/large retailers (34%)
Small e-Commerce (41%)
Mid/large e-Commerce (35%)

Inability to distinguish between human and malicious bots when selling digital goods

Small retailers (34%)
Mid/large retailers (40%)

Small e-Commerce (39%)
Mid/large e-Commerce (27%)

LexisNexis® RISK SOLUTIONS

* See Appendix for details with other challenges

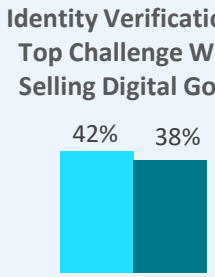
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers in the Mobile Channel.

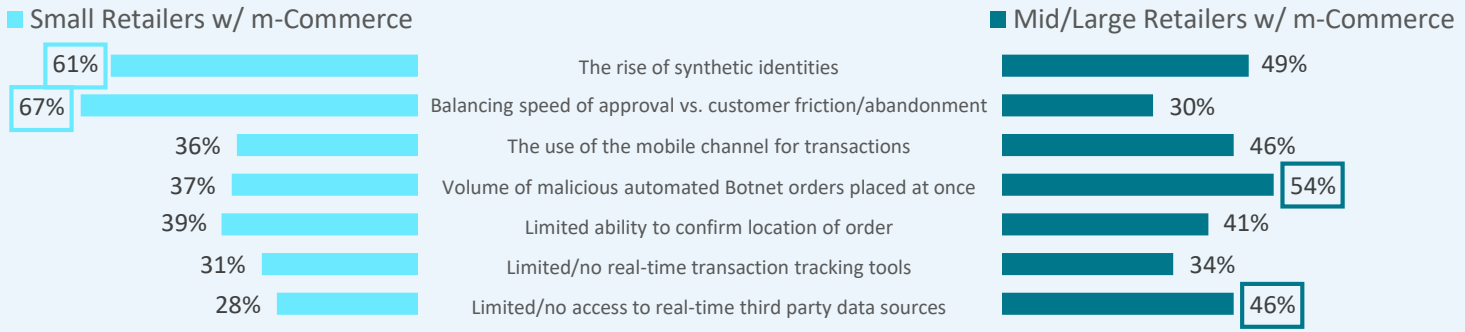
There is clear linkage between the rise of synthetic identities, automated botnet attacks and identity verification challenges.

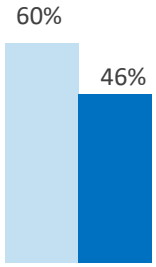
As mentioned earlier, automated botnet attacks are being noticed more often by mid/large retailers with digital and mobile transactions. Other segments are newer to the mobile channel and are significantly more likely to mention synthetic identities and minimizing customer friction as issues with identity verification. e-Commerce merchants, which have been slower to adopt m-Commerce, are particularly likely to blame it on using the mobile channel.

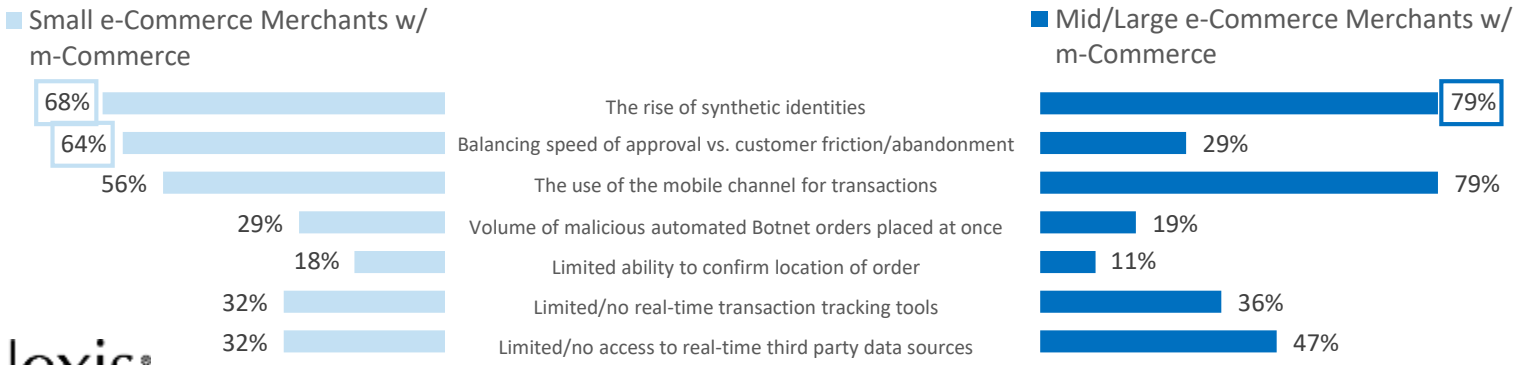
For these newer m-Commerce merchants, their limited use of fraud detection / mitigation solutions to support unique mobile channel risks is likely contributing to these issues.

Top 3 Factors That Make ID Verification A Challenge with Digital Goods Sales among m-Commerce Merchants







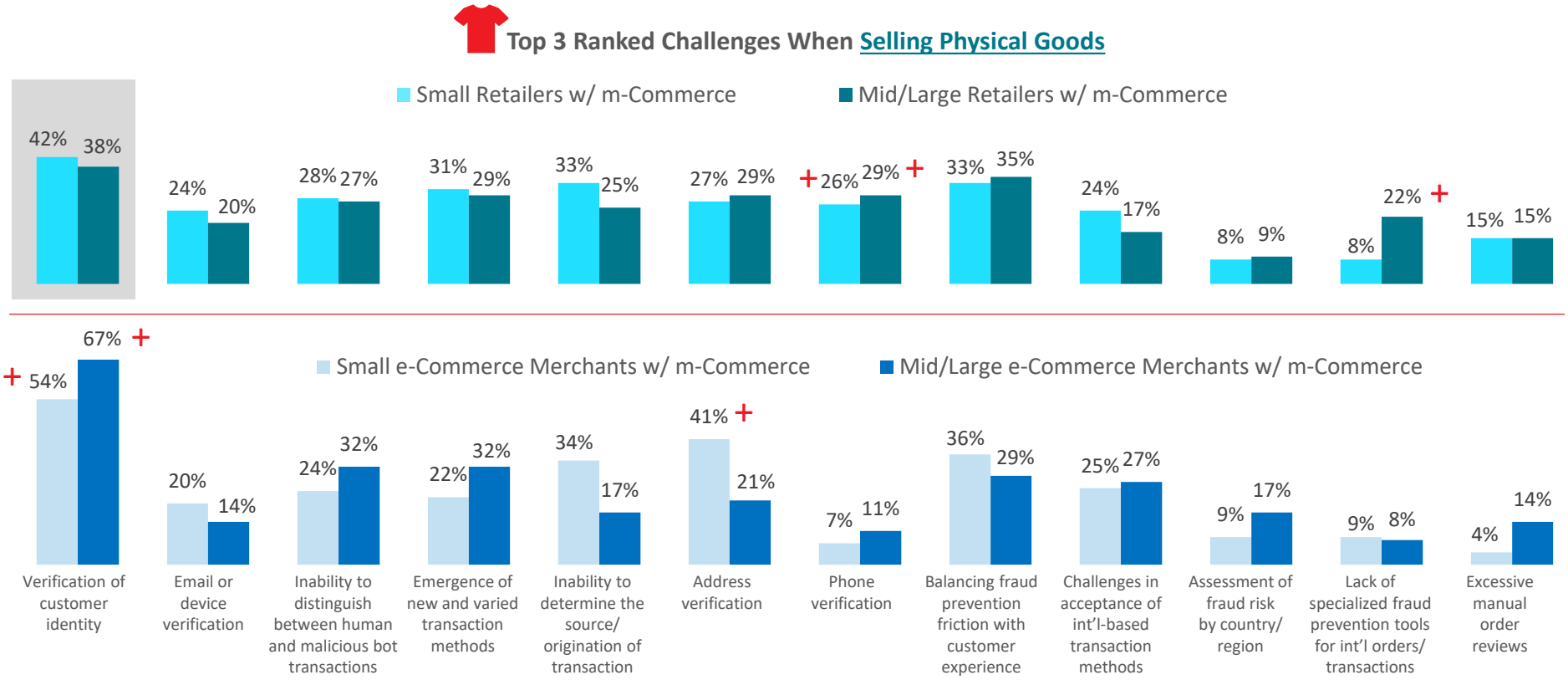


LexisNexis® RISK SOLUTIONS

Q19a/b_2: Please rank the top 3 challenges related to fraud faced by your company when selling digital goods.

With physical goods sales, e-Commerce merchants using the mobile channel rank identity verification as a top challenge significantly more so than do bricks/mortar retailers.

This is found particularly among mid/large e-Commerce merchants selling physical goods, which are newer to the m-Commerce space and haven't yet implemented solutions to address unique mobile channel risks.



LexisNexis® RISK SOLUTIONS

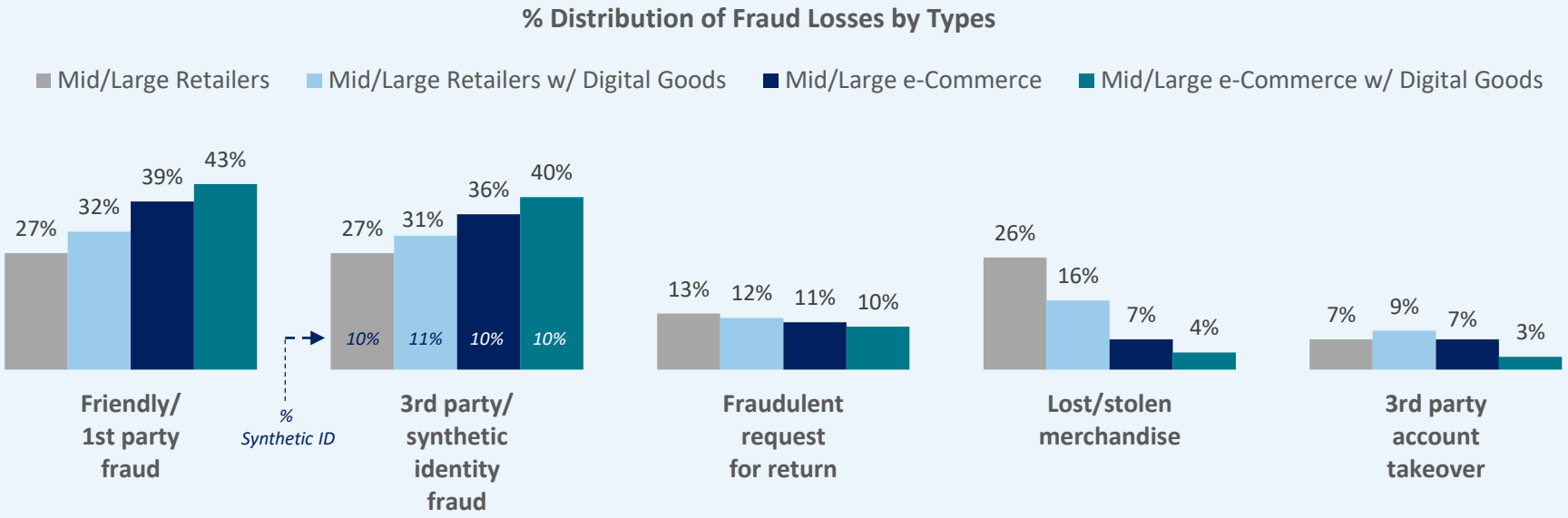
+ Significantly different between small retail and e-Commerce merchants or between mid/large retail and e-Commerce merchants

Q19aa/bb: Please rank the top 3 challenges related to fraud faced by your company when selling digital goods.

Friendly/first-party fraud and 3rd party/synthetic identity fraud account for the significant portion of fraud losses among retailers and e-Commerce merchants.

This is likely related to identity testing bot attacks, which according to ThreatMetrix® can represent a sizeable degree of e-Commerce merchants' transaction volume.[6]

Given the difficulty of detecting synthetic identities, these could represent a larger percent than is reported.



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.

- Friendly fraud (an individual associated with/having access to an account conducts transaction without the primary account owner's knowledge or permission)
- 1st party fraud (owner to authorized user of the account commits the fraud)
- 3rd party identity fraud (unauthorized transaction using other people's existing/real information)
- Synthetic identity fraud (creation of a new identity using a combination of real and fabricated information, sometimes entirely fictitious

[6] ThreatMetrix® H2 2018 Cybercrime Report

LexisNexis® RISK SOLUTIONS

4

All of this is translating into a perfect storm of increased fraud for merchants with cross-border, mobile or digital goods transactions.

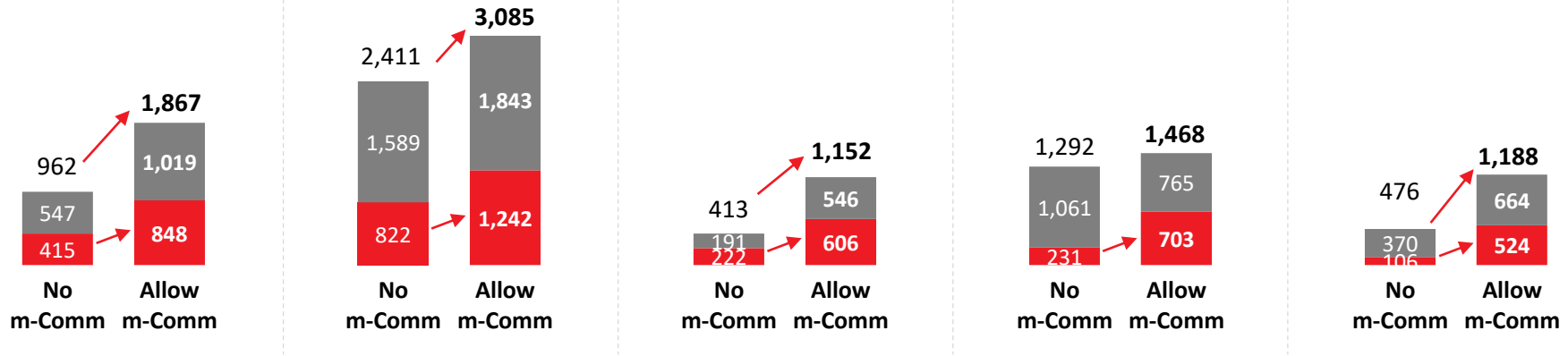
- ✓ Fraud attacks have increased among those using the mobile channel, selling digital goods and allowing international transactions.
- ✓ Fraud from the mobile channel has increased; losses related to mobile apps use is sizeable.
- ✓ Account-related fraud is a problem.
- ✓ Payment card fraud has risen.
- ✓ The cost of fraud trends upward.

LexisNexis®
RISK SOLUTIONS

Fraud volume is significantly higher among those allowing m-Commerce transactions compared to merchants who don't.

Combining digital goods sales increases fraud risk. Its not just the successful fraud attempts that are up, but also those which have been averted. This suggests that, while fraudsters are looking for successes, they are also testing for the weak points: more botnet attacks and card testing of breached credentials; more SMS-based phishing (smishing); seeking out two-step authentication by attacking devices and being the "man in the middle" to intercept one-time passwords.

Average # of Total Fraud Attempts Per Month (2019)



LexisNexis® RISK SOLUTIONS

Average Number of Fraudulent Attempts PREVENTED per Month

Average Number of Fradulent Attempts That SUCCEED per Month

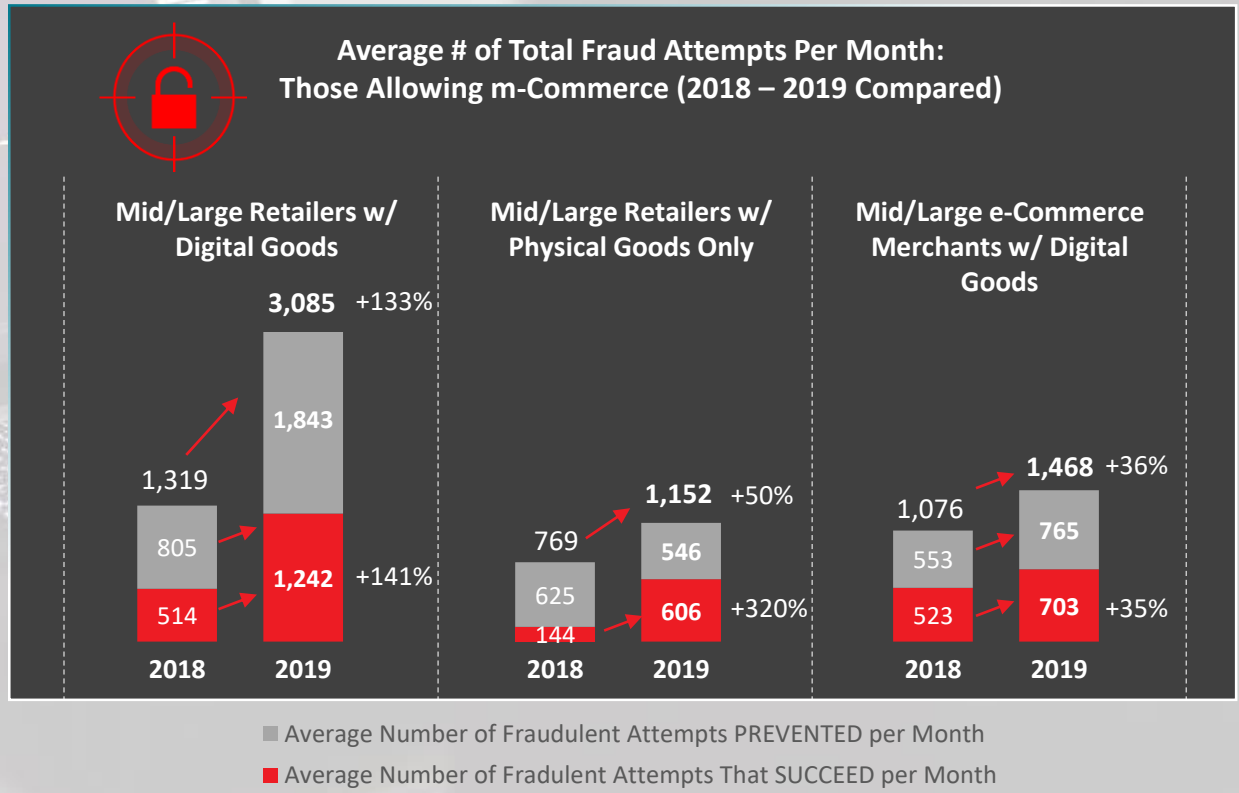
Q22: In a typical month, approximately how many fraudulent transactions are prevented by your company?
Q24: In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

In fact, the average monthly fraud volume for mid/large retailers that sell digital goods through the mobile channel has spiked significantly (133%).

As shown later, they also have one of the highest fraud costs, further underscoring the risky mix of mobile and digital transactions.

Mid/large retailers that sell only physical goods may not have been as prepared for the mobile channel; as this segment has increased use of these transactions since 2018, the volume of successful fraud attacks has outpaced everyone else (up 320%). This would suggest reliance on current legacy solutions used with other channels to detect/mitigate fraud in the more unique mobile channel.

Increased m-Commerce fraud volumes could also be reflective of the increased volume of mobile transactions being conducted by consumers, particularly during the 2018 holidays.



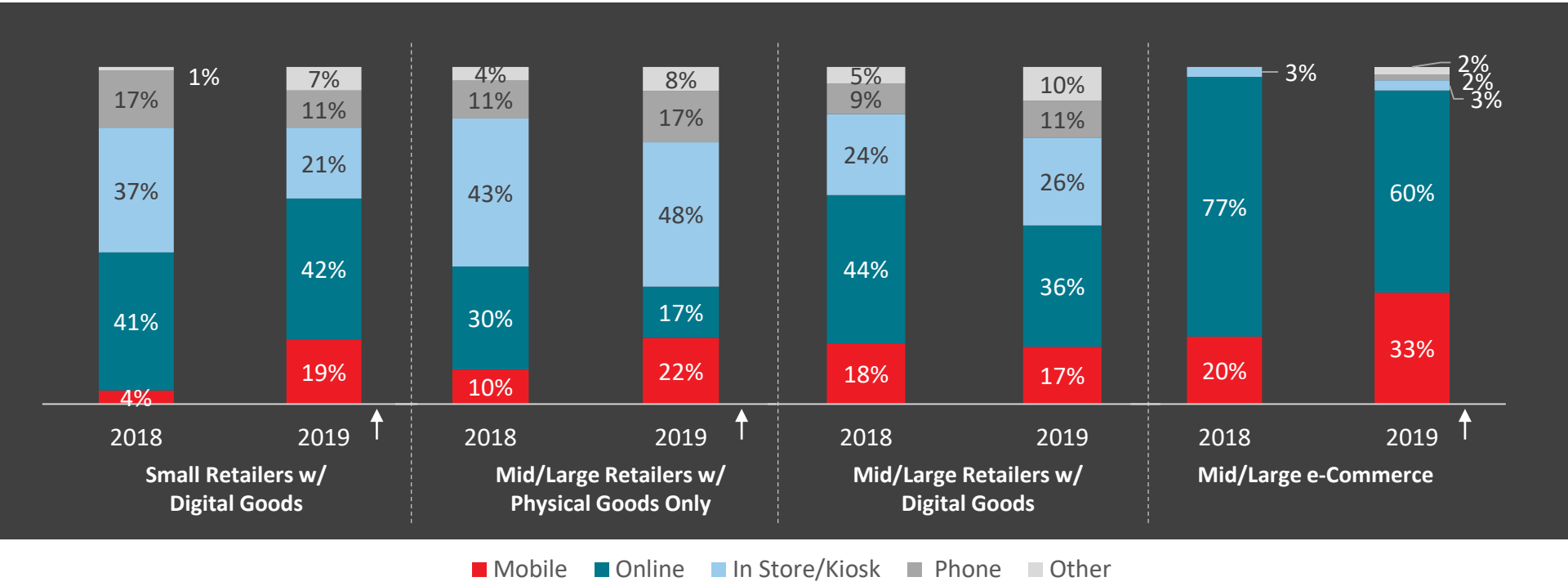
LexisNexis® RISK SOLUTIONS

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?

Not surprisingly, the distribution of fraud losses has risen for the mobile channel, contributing to nearly one-fifth of fraud costs for retailers and even more for mid/large e-Commerce merchants.

In cases of mobile bots being launched from smartphones, current fraud detection solutions that assess IP addresses may provide less effective. For mobile, IP addresses are not often device specific, but are rather "leased / provided" by the network that a person is using. An ISP assigns a public IP address that is the one seen when using the Internet; one's router creates a private IP address for the in-home local area network. Therefore, IP addresses are often dynamic, meaning that they change frequently.

Average # of Total Fraud Attempts Per Month: Those Allowing m-Commerce (2018 – 2019 Compared)



LexisNexis® RISK SOLUTIONS

Q15. Please indicate the percent of fraud costs generated through each of the following transaction channels used by your company.

↑ Significantly different from 2018 within Segment

A significant portion of these mobile channel fraud losses involve apps-based transactions.

Mobile apps represent the largest portion of mobile fraud losses among mid/large retailers; company-branded mobile wallet apps account for somewhat more of this app-based fraud.

Mobile apps can be lucrative for fraudsters. The registration process can be a target where fraudsters have either a stolen card or stolen/breach data that allows them to enroll. When enrolling a card, the authentication role typically falls to banks/financial institutions. Where fraudsters have access to sensitive / personal data on consumers, knowledge-based authentication / challenge questions can be made ineffective. It becomes critical for retailers to have their own authentication tools that rely on behavioral biometrics to reveal digital and physical patterns, connections, transactions, devices and so forth in order to distinguish the good from the bad actors.

% Distribution of Fraud Losses Across Various Mobile Channels (2019)

LexisNexis® RISK SOLUTIONS

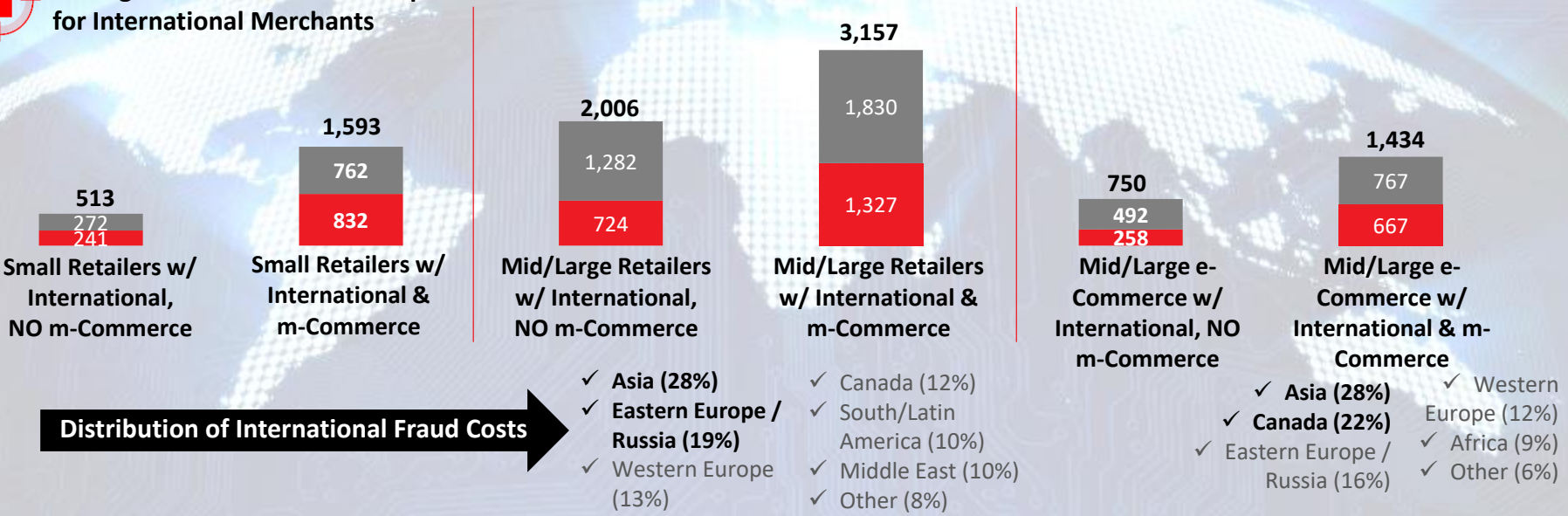
Q17: Please indicate the distribution of fraud losses across the various mobile channels you use.

Fraud attempts are significantly higher for retailers that conduct international transactions and allow m-Commerce, particularly for mid/large retailers.

Botnet attacks are occurring across markets; its not just a case of attacks from within the US. Eastern / Southeast / Central Asia, Eastern Europe / Russia and Canada are reported as origination points among retailers and e-Commerce merchants who track fraud

Identity proofing involves both **verification and authentication**. Access to verifying consumer data can be limited for certain regions, including with GDPR in the EU. It is critical that retailers and e-Commerce merchants use tools that provide insight into digital identities; these inform on identifying characteristics such as device/e-mail/URL/IP addresses and digital behaviors; these should be accompanied by behavioral biometrics tools that look for patterns and anomalies to support **authentication** since fraudsters can spoof devices.

Average # of Total Fraud Attempts Per Month for International Merchants



Distribution of International Fraud Costs

- ✓ **Asia (28%)**
- ✓ **Eastern Europe / Russia (19%)**
- ✓ Western Europe (13%)
- ✓ Canada (12%)
- ✓ South/Latin America (10%)
- ✓ Middle East (10%)
- ✓ Other (8%)
- ✓ **Asia (28%)**
- ✓ **Canada (22%)**
- ✓ Eastern Europe / Russia (16%)
- ✓ Western Europe (12%)
- ✓ Africa (9%)
- ✓ Other (6%)

■ Average Number of Fraudulent Attempts PREVENTED per Month
■ Average Number of Fradulent Attempts That SUCCEED per Month

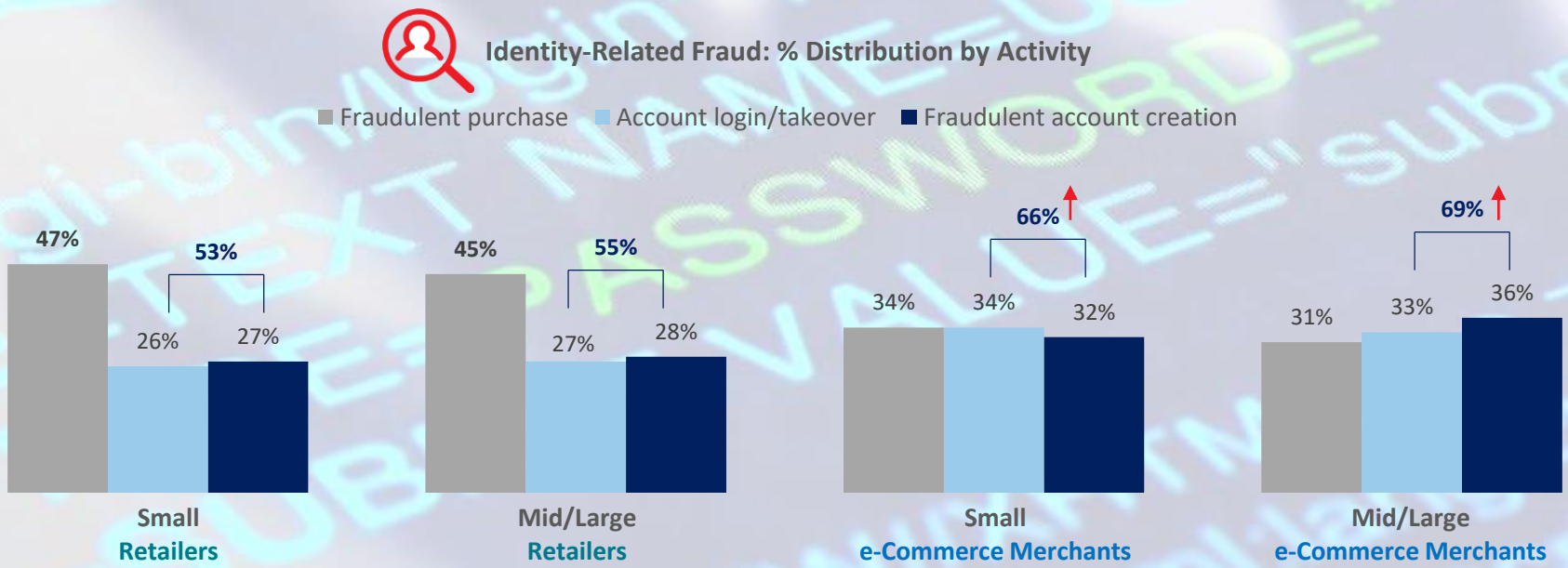
LexisNexis® RISK SOLUTIONS

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?

Account login/take-overs and fraudulent creations represent the majority of identity-related fraud activity, particularly for e-Commerce merchants.

One-third of identity-related fraud among e-Commerce merchants involves account takeovers, with a similar proportion involving fraudulent creation of new accounts. That said, there is still a sizeable level of this occurring in the remote channels used by bricks/mortar retailers (just over half of identity-related fraud activity).

Using breached data, fraudsters will continue to test passwords from one place to another in an attempt to find a match.



LexisNexis® RISK SOLUTIONS

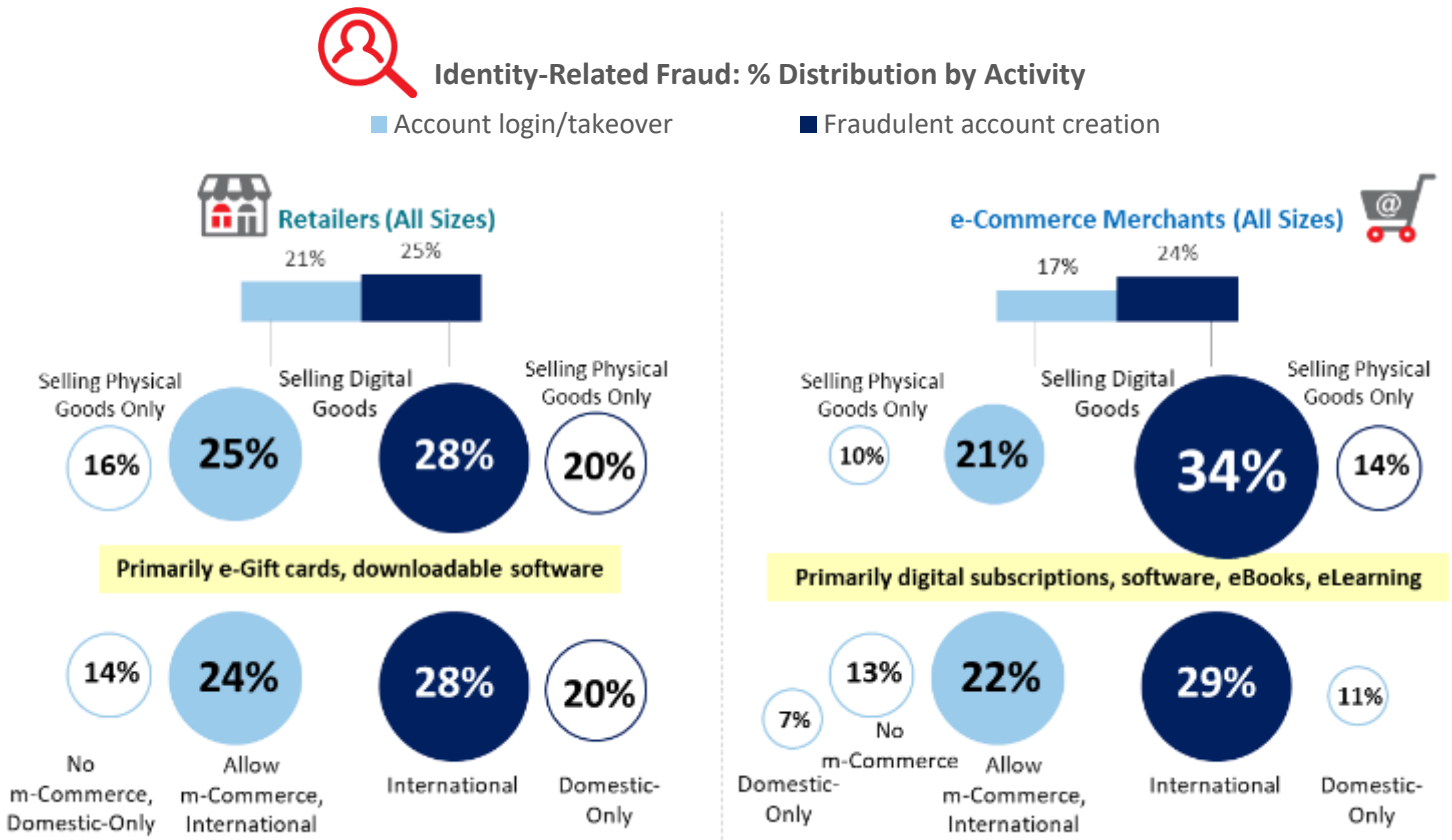
Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?
- Account login (to hack, access or take over an account)
- Account creation (fraudulently establish an account using other people's identity/personal information

Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?.

↑ Significantly different from other segments

Selling digital goods/services, allowing m-Commerce and conducting international transactions adds risk for takeovers and fraudulent creation of accounts.

As mentioned earlier, new account creation is of particular interest to fraudsters seeking to nurture good credit and behavioral patterns with synthetic identities, prior to "breaking out/breaking bad" on a significant fraudulent transaction.



LexisNexis® RISK SOLUTIONS

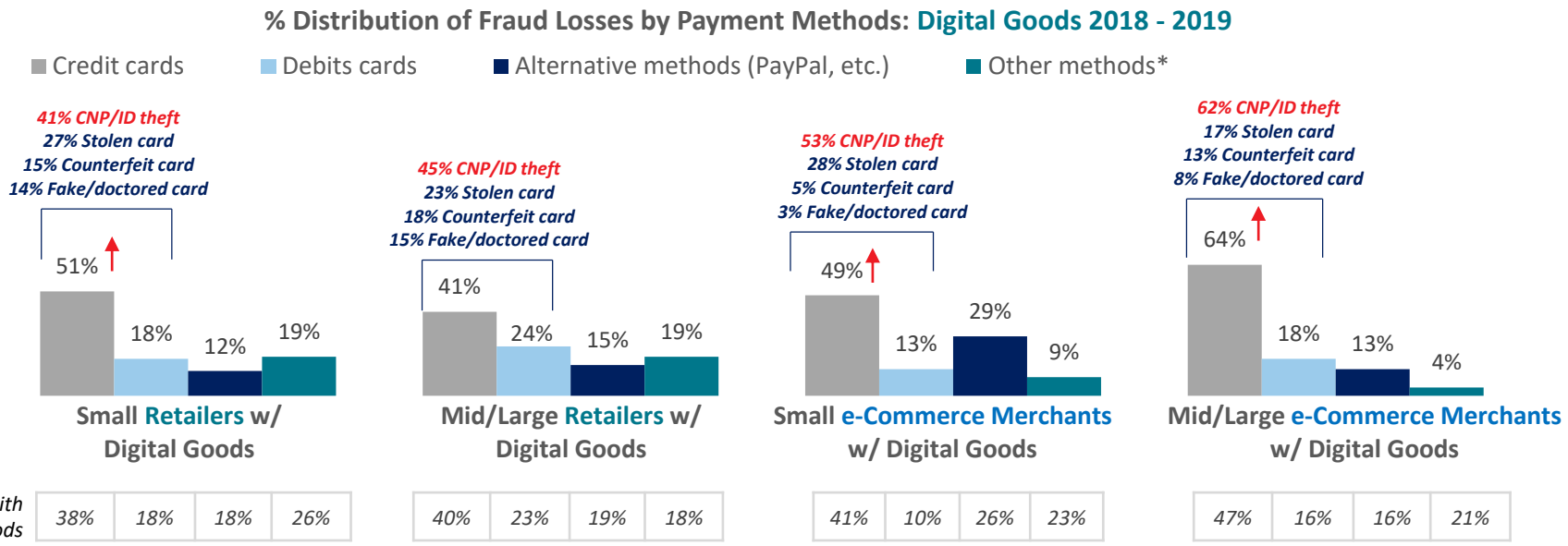
Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?
- Account login (to hack, access or take over an account)
- Account creation (fraudulently establish an account using other people's identity/personal information

Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?.

Payment / credit card fraud has risen sharply during the past year for most retailers / merchants that sell digital goods, based largely on breached data (CNP fraud, card ID theft).

It has spiked the most and is currently highest among mid/large e-Commerce merchants who offer digital goods, with 64% of losses by credit card compared to other payment methods; a significant portion of that relates to Card Not Present and Card Identity fraud.

With the introduction of EMV moving more fraud to remote channels, the use of counterfeit cards is low. For remote channel merchants, it is important to use velocity checks to assess whether there are repetitive patterns occurring with the same credit card information; tools that also assess behavioral risk and digital identities should be considered given the anonymous online channel and complexity of detecting synthetic identity fraud.



*Other transaction method include cash, paper checks, gift cards, mobile device-based wallets, social media payments, and virtual currency

Q18: Please indicate the percentage distribution of the payment methods used to commit fraud against your company.
Q18e: Of your credit or debit related fraud losses, please indicate the distribution across the following types of card fraud.

- Card Not Present fraud (fraudster knows the account number, expiration data and uses to transact remotely)
- Card ID theft (criminals use details from a person's card and use it to take over an account or open a new one)
- Stolen or lost card use
- Counterfeit card fraud (use of skimmed information; a fake magnetic strip holds the victim's card details
- Fake or doctored card fraud (magnetic strip is erased / replaced with data from other valid cards but won't work when swiped; fraudster convinces a merchant to enter details manually

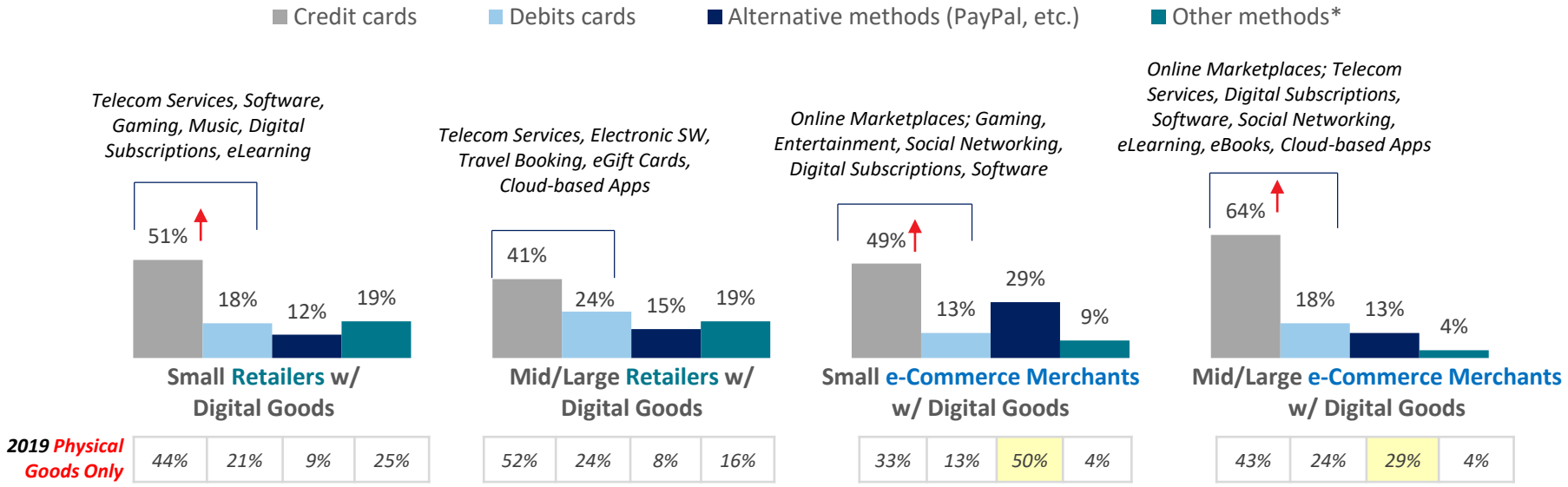
↑ Significantly different from 2018 within Segment

LexisNexis® RISK SOLUTIONS

Many digital goods retailers / e-Commerce merchants report a higher proportion of fraud losses to payment / credit cards than those selling physical goods only.

While payment fraud occurs for both physical and digital goods, fraudsters tend to prefer digital goods/services based on various reasons, including: the speed to obtain; the ability to leverage remote channel anonymity; the ability to launch mass automated bots where merchants are not using advanced authentication tools; and, the opportunity to quickly resell these types of goods on other sites.

% Distribution of Fraud Losses by Payment Methods: Digital vs. Physical Goods (2019)



*Other transaction method include cash, paper checks, gift cards, mobile device-based wallets, social media payments, and virtual currency

Q18: Please indicate the percentage distribution of the payment methods used to commit fraud against your company.
Q18e: Of your credit or debit related fraud losses, please indicate the distribution across the following types of card fraud.

- Card Not Present fraud (fraudster knows the account number, expiration data and uses to transact remotely)
- Card ID theft (criminals use details from a person's card and use it to take over an account or open a new one)
- Stolen or lost card use
- Counterfeit card fraud (use of skimmed information; a fake magnetic strip holds the victim's card details
- Fake or doctored card fraud (magnetic strip is erased / replaced with data from other valid cards but won't work when swiped; fraudster convinces a merchant to enter details manually

↑ Directionally or significantly different from Physical Goods-Only Segment

LexisNexis® RISK SOLUTIONS

Not surprisingly, fraud costs have risen and are highest for mid/large retailers and e-Commerce merchants that sell digital goods. But, the mobile channel sends costs higher.

Mid/large retailers selling digital goods and using the mobile channel have experienced a significant jump in fraud costs over 2018 (every $1 of fraud costs them $3.40 compared to $2.91 previously).

However, mid/large e-Commerce merchants selling digital goods and using the mobile channel have the highest cost of fraud (every $1 of fraud costs them $4.06).

LexisNexis® RISK SOLUTIONS

See Appendix for further details

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.

5

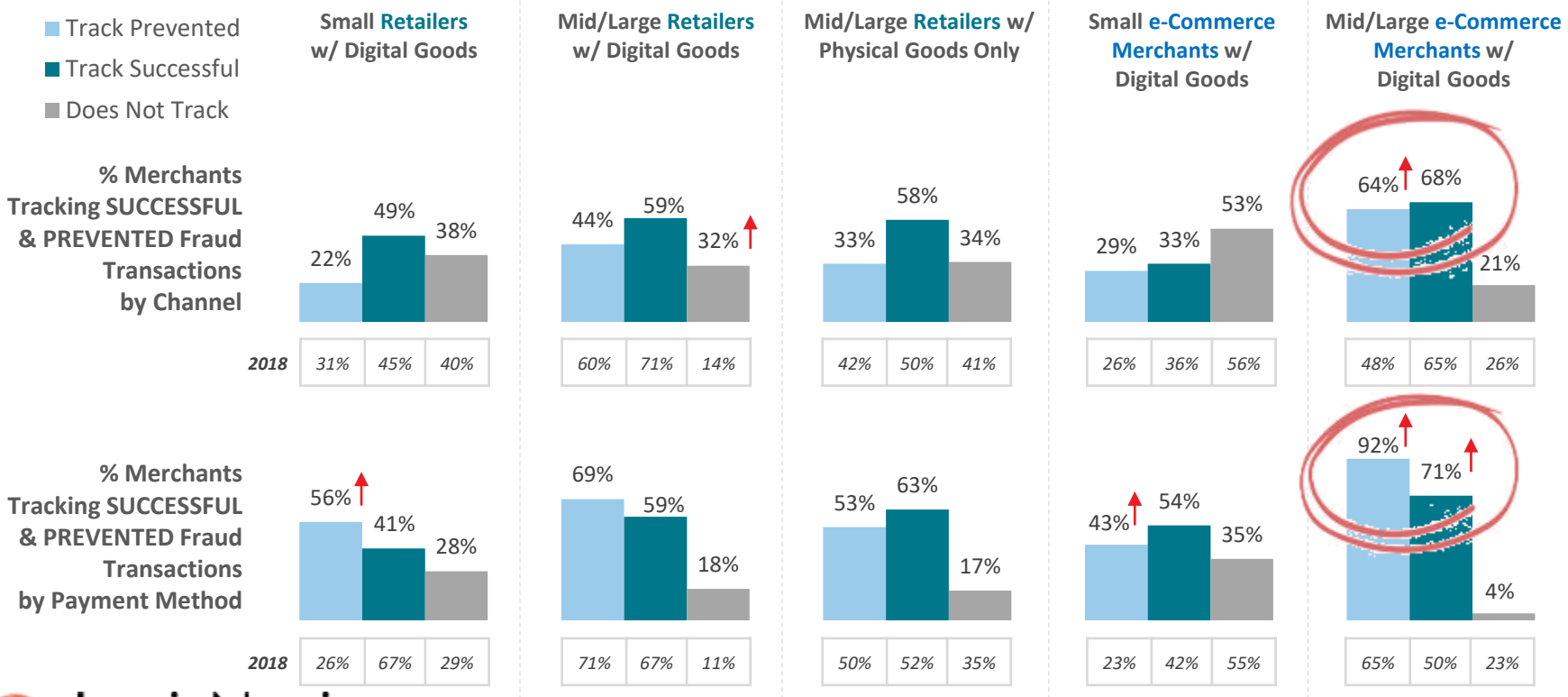
Retailers and e-Commerce merchants most at-risk for attack may not be optimizing solutions and approaches to fight newer and more complex types of fraud.

LexisNexis®
RISK SOLUTIONS

Tracking all of the ways that fraud impacts the business is essential – both successful and prevented by channel and payment methods.

Mid/large e-Commerce merchants that sell digital goods have been most at-risk and hit hardest by retail fraud in recent years; this appears to have driven significantly more of them to add more rigorous tracking to their approaches.

However, other segments continue to be slower to implement this activity, particularly with regard to the different channels where fraud can penetrate their business. This weakens efforts to fully detect and mitigate fraud as criminals constantly probe for the weakest links.



LexisNexis® RISK SOLUTIONS

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

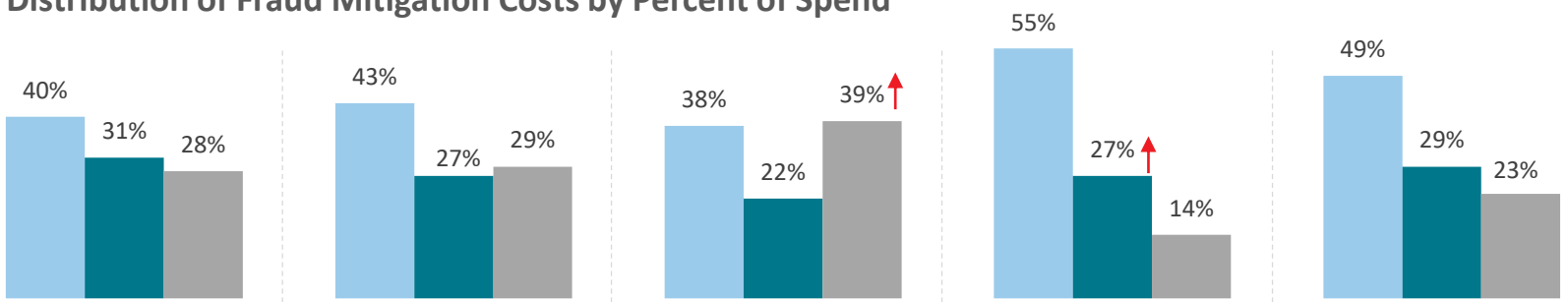
↑ Significantly different from 2018 within Segment

Retail and e-Commerce merchants continue to allocate a sizeable portion of their risk mitigation budgets to manual efforts.

That is typically an every-increasing cost, since labor generally doesn't get cheaper over time.

While e-Commerce merchants allocate somewhat more of their budgets to fraud solutions, over-one quarter is still represented by manual reviews.

Distribution of Fraud Mitigation Costs by Percent of Spend



	Small Retailers w/ Digital Goods	Mid/Large Retailers w/ Digital Goods	Mid/Large Retailers w/ Physical Goods Only	Small e-Commerce Merchants w/ Digital Goods	Mid/Large e-Commerce Merchants w/ Digital Goods
2018	*45% 23% 26%*	*42% 29% 29%*	*44% 27% 28%*	*64% 17% 15%*	*52% 25% 23%*

Cost of fraud solutions Cost of manual reviews Cost of physical security

LexisNexis® RISK SOLUTIONS

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

↑ Significantly different from 2018 within Segment

Fraud has become more complex; various risks can occur at the same time with no single solution. Fraud tools need to authenticate both digital and physical criteria as well as both identity and transaction risk.

Fraud Issues

- **Digital Goods & Services**: fast transactions, easy synthetic identity and botnet targets; ***need velocity checking*** to determine ***transaction risk*** along with ***data and analytics to authenticate*** the individual
- **Account-related fraud**: breached data ***requires more levels of security, as well as authenticating the person from a bot or synthetic ID***
- **Synthetic identities**: ***need to authenticate the whole individual*** behind the transaction in order to distinguish from fake identity based on partial real data
- **Botnet attacks**: mass human or automated attacks often to test cards, passwords/credentials or infect devices
- **Mobile channel**: source origination and infected devices add risk; mobile bots and malicious malware makes authentication difficult; ***need to assess the device and the individual***

Solution Options

Assessing the transaction risk

Velocity checks / transaction scoring: monitors historical shopping patterns of an individual against their current purchases to detect if the number of orders by the cardholder match up or if there appears to be an irregularity ***(Solution examples: real-time transaction scoring; automated transaction scoring)***

Authenticating the physical person

Basic Verification verifying name, address, DOB or providing a CVV code associated with a card ***(Solution examples: check verification services; payment instrument authentication; name/address/DOB verification)***

Active ID Authentication use of personal data known to the customer for authentication; or where user provides two different authentication factors to verify themselves ***(Solution examples: authentication by challenge or quiz; authentication using OTP / 2 factor)***

Authenticating the digital person

Digital identity / behavioral biometrics: analyzes human-device interactions and behavioral patterns such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognizing normal user and fraudster behavior ***(Solution examples: authentication by biometrics; e-mail/phone risk assessment; browser/malware tracking; device ID / fingerprinting)***

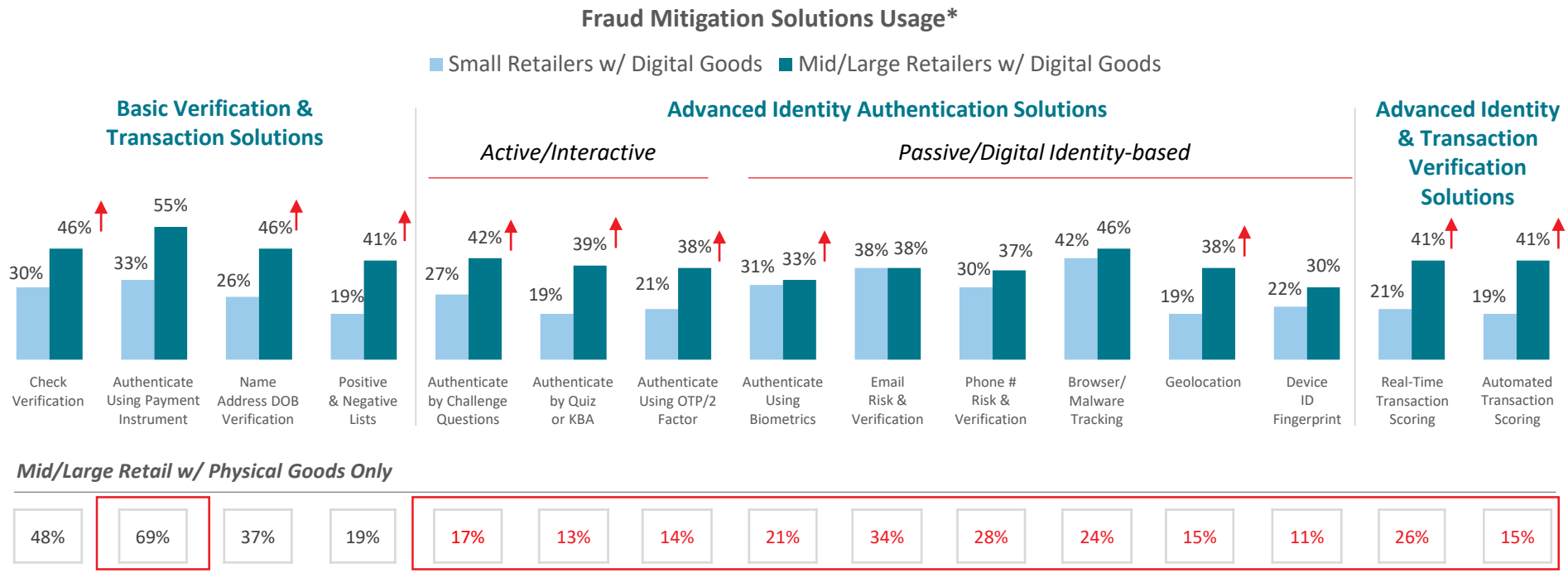
Device assessment: uniquely identify a remote computing device or user ***(Solution examples: device ID / fingerprint; geolocation)***

LexisNexis® RISK SOLUTIONS

Mid/large retailers selling digital goods have been an ongoing fraud target and have invested in more solutions than other segments. But, use of solutions to counter new threats is limited across segments.

The complexity of synthetic identity fraud and botnet attacks requires more sophisticated solutions to assess the whole person from a digital behavioral and physical identity perspective. The limited use of these explains the challenges highlighted earlier with identity verification, botnet attacks and account-related fraud.

Small retailers with digital goods and mid/large retailers with physical goods-only are particularly at risk; more of them have entered the m-Commerce space yet few have invested in solutions to detect the unique risks posed by this channel.



LexisNexis® RISK SOLUTIONS

*Solutions list was modified in 2019, making it difficult to trends from previous waves

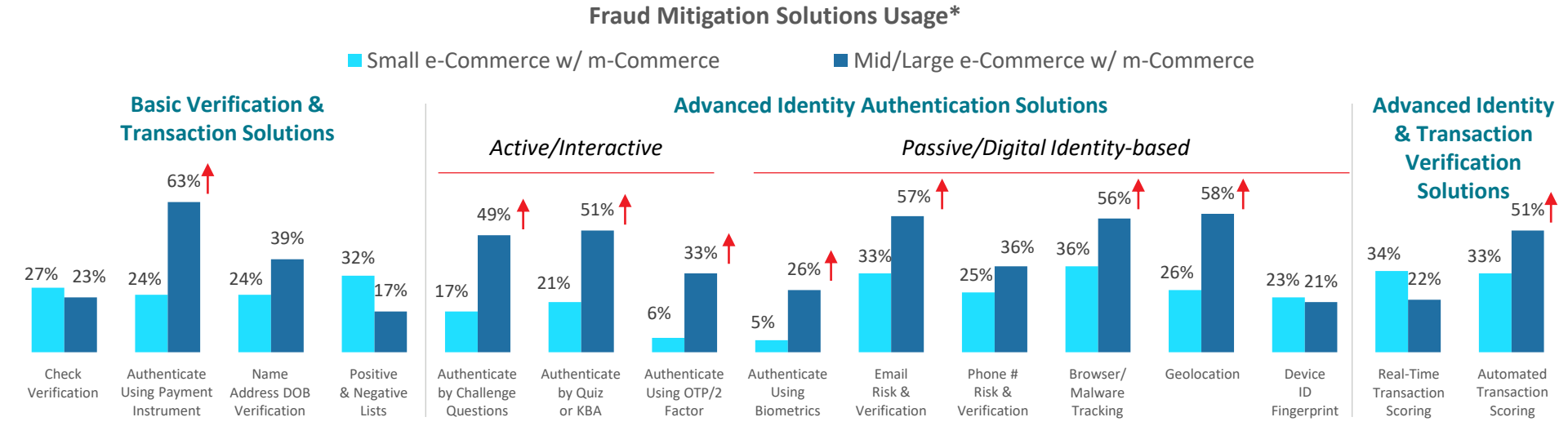
Q27: Which of the following fraud solutions does your company currently use?

↑ Significantly different from other Segment

Mid/large e-Commerce merchants using the mobile channel get hit hardest and are more likely to use a fraud mitigation solution than others, including mid/large retailers.

However, the use of more sophisticated solutions to address the emerging multi-faceted nature of fraud is still limited among these larger e-Commerce merchants, particularly with regard to behavioral biometrics and other digital identity solutions that can fight synthetic identity fraud and botnet attacks. Given similar incidence rates between some of the physical (payment instrument, authenticate by challenge or KBA) and digital authentication solutions (e-mail risk, browser/malware tracking and geolocation), suggests that some of these larger merchants are layering these together for more effective fraud detection. That said, there is still a sizeable portion of merchants who are not doing so.

e-Commerce merchants have been slower to adopt the mobile channel than brick/mortar retailers; lower incidence of solutions that can support this channel, such as device ID/fingerprint and phone number risk, suggests that they are applying solutions from their online channel to the mobile one. However, these are two different types of technology and risk; current solutions may not help detect mobile channel fraud as effectively.



LexisNexis® RISK SOLUTIONS

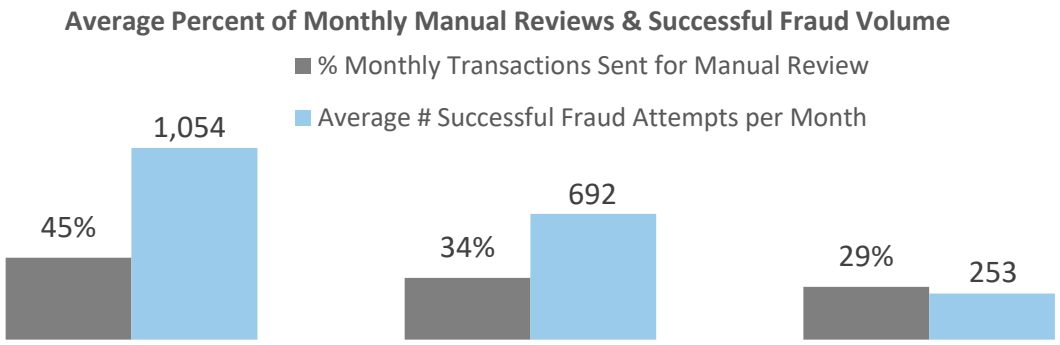
*Solutions list was modified in 2019, making it difficult to trends from previous waves

Q27: Which of the following fraud solutions does your company currently use?

↑ Significantly different from other Segment

It is important to layer both identity authentication and fraud transaction risk assessment solutions, as well as the physical and digital identity factors.

The study findings show that digital m-Commerce retailers and e-Commerce merchants who layer core + identity + fraud transaction solutions which include digital identity data send fewer monthly transactions for manual review and experience fewer successful fraud attacks on average.



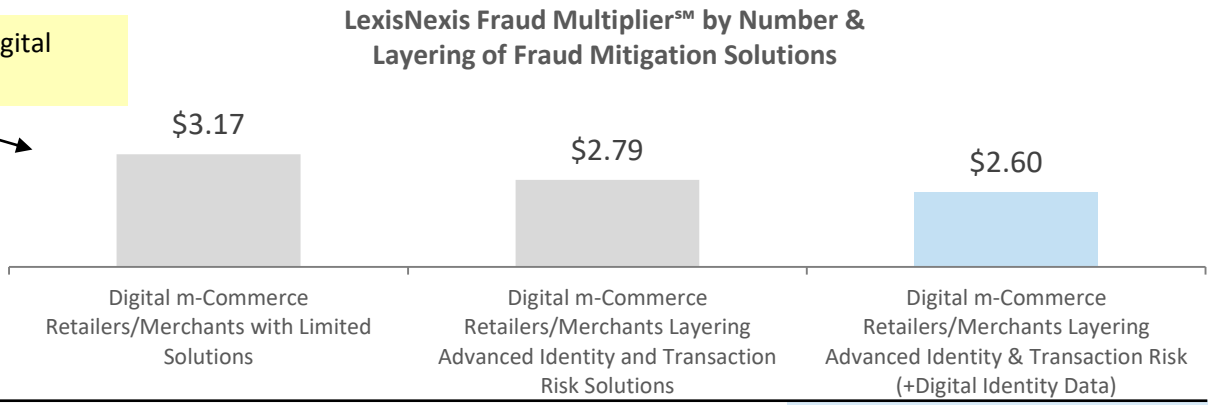
Layers of Protection		Basic	Multi-Layered	Multi-Layered with Digital Identity Data
Common Core Solutions Used Most Often	Check Verification, Authentication by Payment Instrument (CVV), Name/Address/DOB Verification, Positive/Negative Lists	✓	✓	✓
Layering of Advanced Identity Solutions (including Digital Identity Data)	Device ID Fingerprinting, Geolocation, Browser/Malware Tracking, e-Mail/Phone Risk Verification, Authentication by Biometrics, Authentication by OTP/2 Factor, Authentication by Quizzes, Authentication by Challenge Questions		✓	✓
Layering of Fraud Transaction Risk Assessment Solutions	Automated Transaction Scoring, Real-Time Transaction Tracking,		✓	✓

LexisNexis® RISK SOLUTIONS

This can translate into a lower cost of fraud when using a layered solution approach involving digital identity data.

The study findings also show that those using this type of layering approach have lower fraud costs ($2.60 for every $1 of fraud) than those which use only a limited set of core solutions (up to $3.17 per $1 of fraud). The cost is even higher for larger retailers that sell digital goods via the mobile channel and do not layer solutions to address these unique transaction/channel risks.

$3.84 for Mid/Large selling digital goods via the mobile channel



Layers of Protection		Basic	Multi-Layered	Multi-Layered with Digital Identity Data
Common Core Solutions Used Most Often	Check Verification, Authentication by Payment Instrument (CVV), Name/Address/DOB Verification, Positive/Negative Lists	✓	✓	✓
Layering of Advanced Identity Solutions (including Digital Identity Data)	Device ID Fingerprinting, Geolocation, Browser/Malware Tracking, e-Mail/Phone Risk Verification, Authentication by Biometrics, Authentication by OTP/2 Factor, Authentication by Quizzes, Authentication by Challenge Questions		✓	✓
Layering of Fraud Transaction Risk Assessment Solutions	Automated Transaction Scoring, Real-Time Transaction Tracking,		✓	✓

LexisNexis® RISK SOLUTIONS

Recommendations

LexisNexis®
RISK SOLUTIONS

Recommendations

1

Retailers and e-Commerce 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 since the nature of the goods changes the risk.
- ✓ Different challenges and risks are posed by mobile channels versus online, given the difference in technology. Coupled with digital goods, this increases the complexity such that the need for device-specific, real-time / velocity checking and digital behavior solutions become even more important.

2

When implementing unique solutions, it is essential to use a multi-layered approach, particularly when selling digital goods in the mobile channel.

- ✓ Fraud should be assessed for both the identity of the "customer" as well as the risk of the transaction.
  - Identity verification / authentication is important for letting legitimate customers in with the least amount of friction.
  - Transaction verification is about assessing the nature of the activity in order to keep fraudsters out.
- ✓ A layered approach can reduce costs associated with manual reviews and successful fraud attacks.

LexisNexis® RISK SOLUTIONS

Recommendations (cont.)

To effectively fight fraud generated by botnets and synthetic identities, it is important to combine physical and digital identity data *and* analysis to get the full view of the "customer".

- ✓ Botnets and synthetic identities are difficult to detect using traditional risk mitigation solutions because they can mimic real persons and transactions. Using traditional identifiable data alone may miss these.

- ✓ Digital identity and behavioral biometrics data *and* analysis is essential for detecting anomalies based on device use, linkages, remote channel behaviors, locations and patterns. This will also support machine learning in order to prevent fraud before it occurs. Combining digital with physical identification data provides a comprehensive view for distinguishing between the real and synthetic or botnet "customer".

Recommendations (cont.)

4

A multi-layered solution approach is useful to protect retailers and e-Commerce merchants throughout a single buyer experience.

- ✓ Using different solutions to support fraud detection at various points in the shopping journey will strengthen overall protection.

- ✓ An example of this could involve:
  - Velocity checks / real-time scoring at the frontend to determine risk of the transaction; for account access, the use of multiple screening tools, including two-factor authentication, is important since fraudsters are experts at knowing the types of information that can get them through screening;

  - Digital identity and behavioral biometrics can be used to assess the customer "browsing" period (fraudsters tend to know exactly where to go and act more quickly than a typical shopper – this would help to assess anomalies);

  - Upon checkout / authorization, additional authentication checks can assess the individual.

  - The use of passive, analytics-driven solutions will provide a more seamless and frictionless experience for the customer, including reducing the time involved for fraud assessment.

Recommendations (cont.)

Retailers and e-Commerce merchants need to track both payment and channel fraud in terms of costs and successful attempts. This needs to be part of the broader approach alongside fraud mitigation solutions.

- ✓ Since fraud occurs in different ways depending on the type of goods and channels, this creates multiple endpoints that fraudsters can attack.

- ✓ They continue to test for the weakest links. Knowing where they've been successful is important in order to plug the gaps. But, also knowing where they've been thwarted is important too; they will continue to test these access points.

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

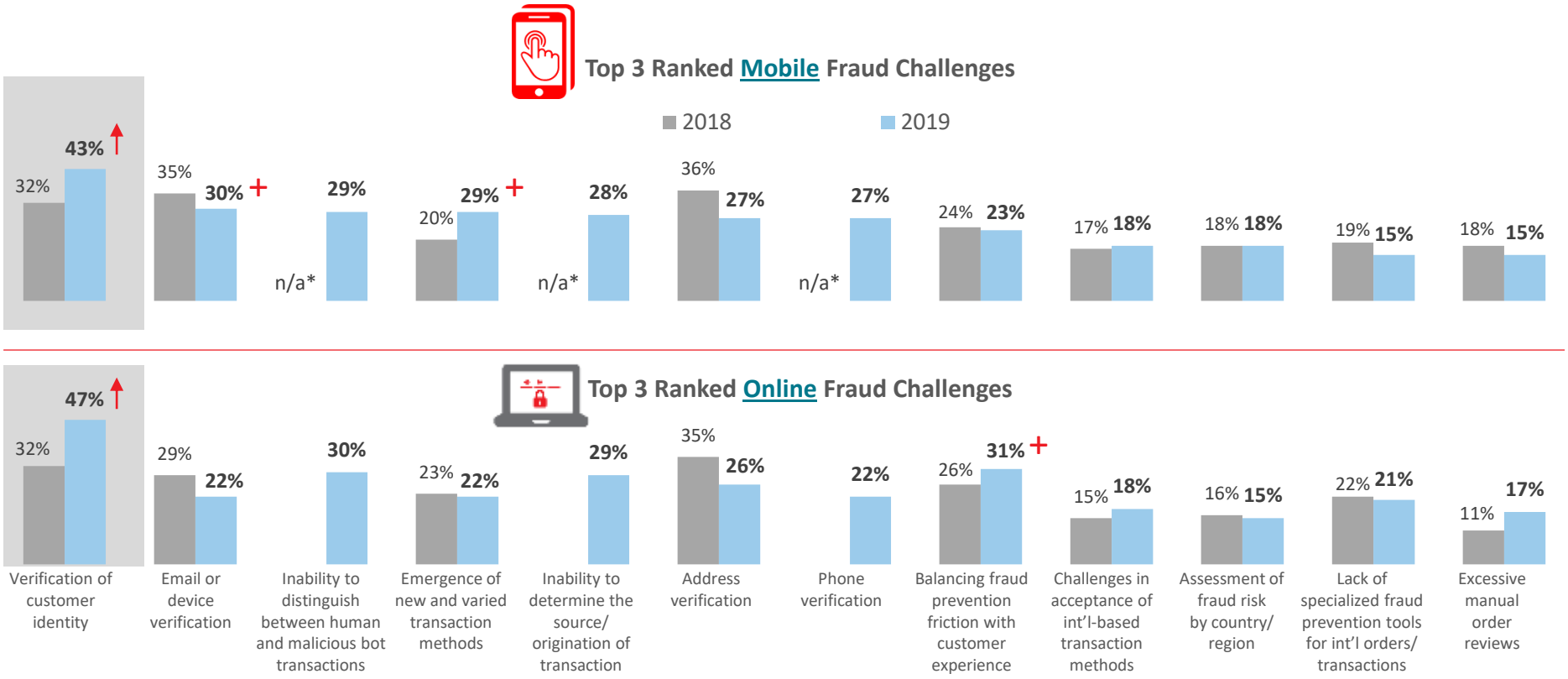
For more information: visit https://www.lexisnexis.com/risk/retail or call 800.869.0751

Appendix

LexisNexis®
RISK SOLUTIONS

There is increased recognition that remote channel transactions make identity verification challenging, with significantly more retailers ranking this as a top issue compared to 2018.

E-mail / device verification and the emergence of new / varied transaction methods are ranked higher as a mobile channel challenge compared on online.



LexisNexis® RISK SOLUTIONS

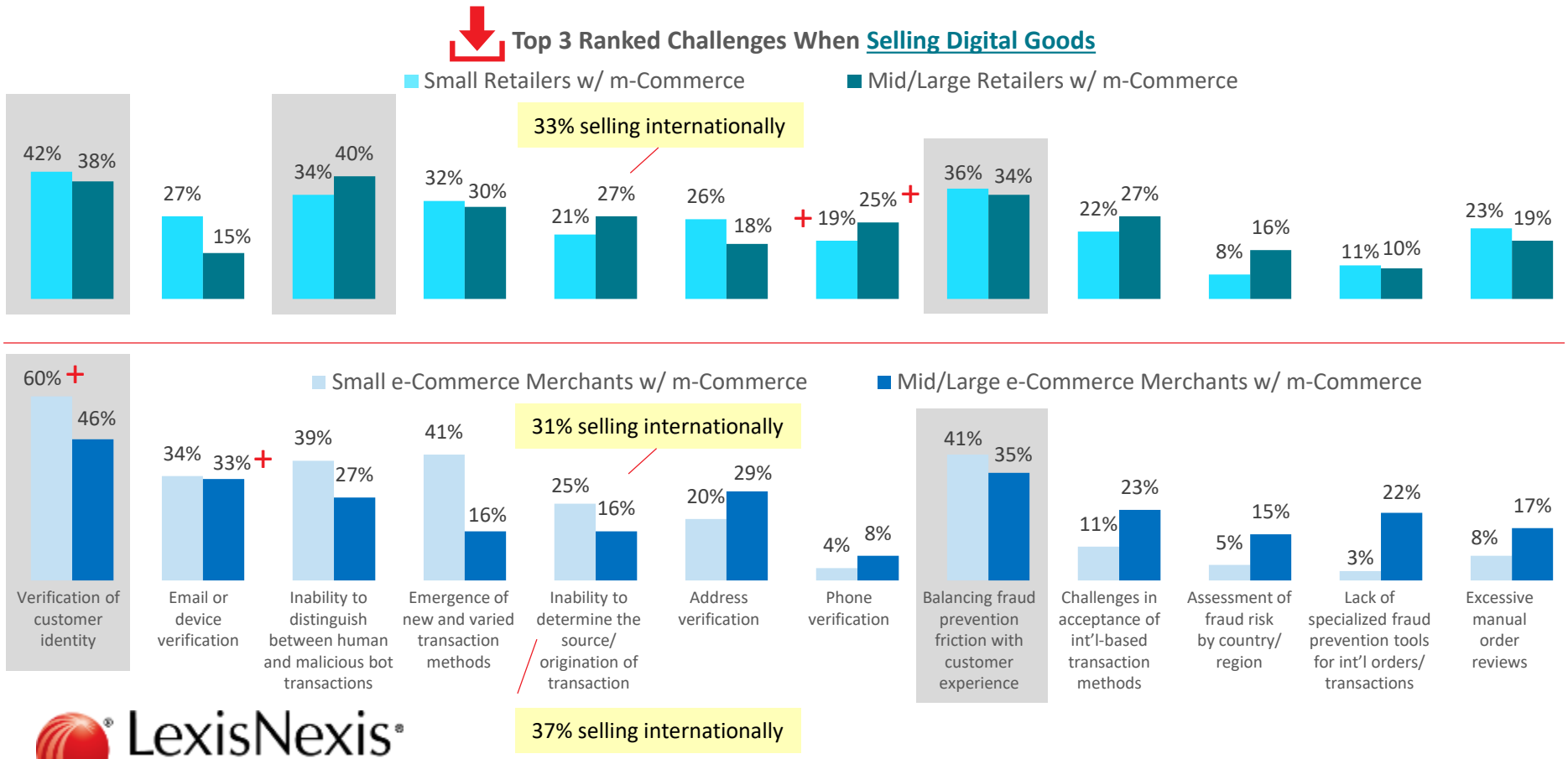
\+ Significantly different from Online or Mobile ↑ Significantly different from 2018

Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers in the Mobile Channel. *Not asked in 2018

Identity verification is a key issue for all retail and e-Commerce segments when selling digital goods in the mobile channel.

This correlates to another commonly top ranked challenge with digital goods, balancing fraud prevention with customer friction. Particularly for retailers, this also impacts the ability to distinguish between legitimate and malicious bot transactions.

But there are also many other challenges that these merchants face. Since the survey question asked respondents to rank only their top 3, and the findings show limited consensus (high percentages) for any one challenge, this indicates that various respondents choose different top issues - suggesting that the combination of mobile and digital goods is a more complex minefield of fraud risks.



LexisNexis® RISK SOLUTIONS

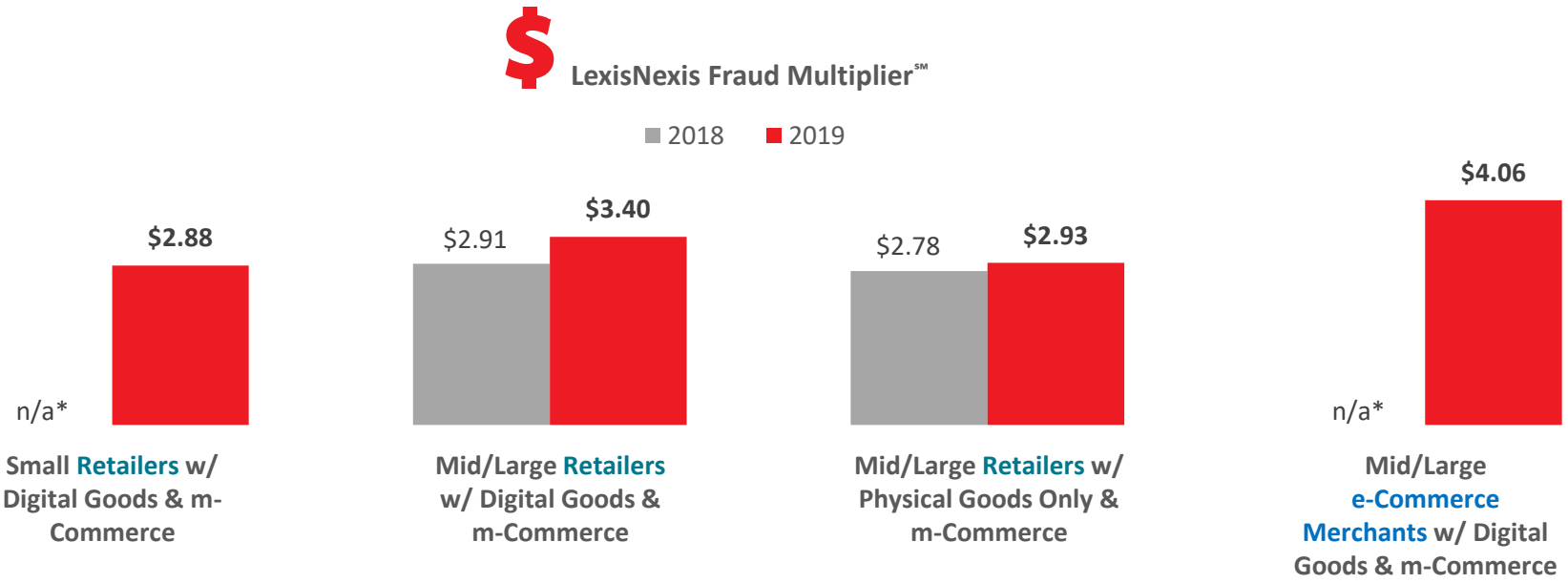
\+ Significantly different between small retail and e-Commerce merchants or between mid/large retail and e-Commerce merchants

Q19aa/bb: Please rank the top 3 challenges related to fraud faced by your company when selling digital goods.

As fraud volumes increase, so too do fraud costs. Those using the mobile channel and selling digital goods have higher fraud costs than non-m-Commerce merchants, particularly mid/large e-Commerce.

Mid/large retailers selling digital goods and using the mobile channel have experienced a significant jump in fraud costs over 2018 (every $1 fraud costs them $3.40 compared to $2.91 previously).

However, mid/large e-Commerce merchants selling digital goods and using the mobile channel have the highest cost of fraud (every $1 of fraud costs them $4.06).



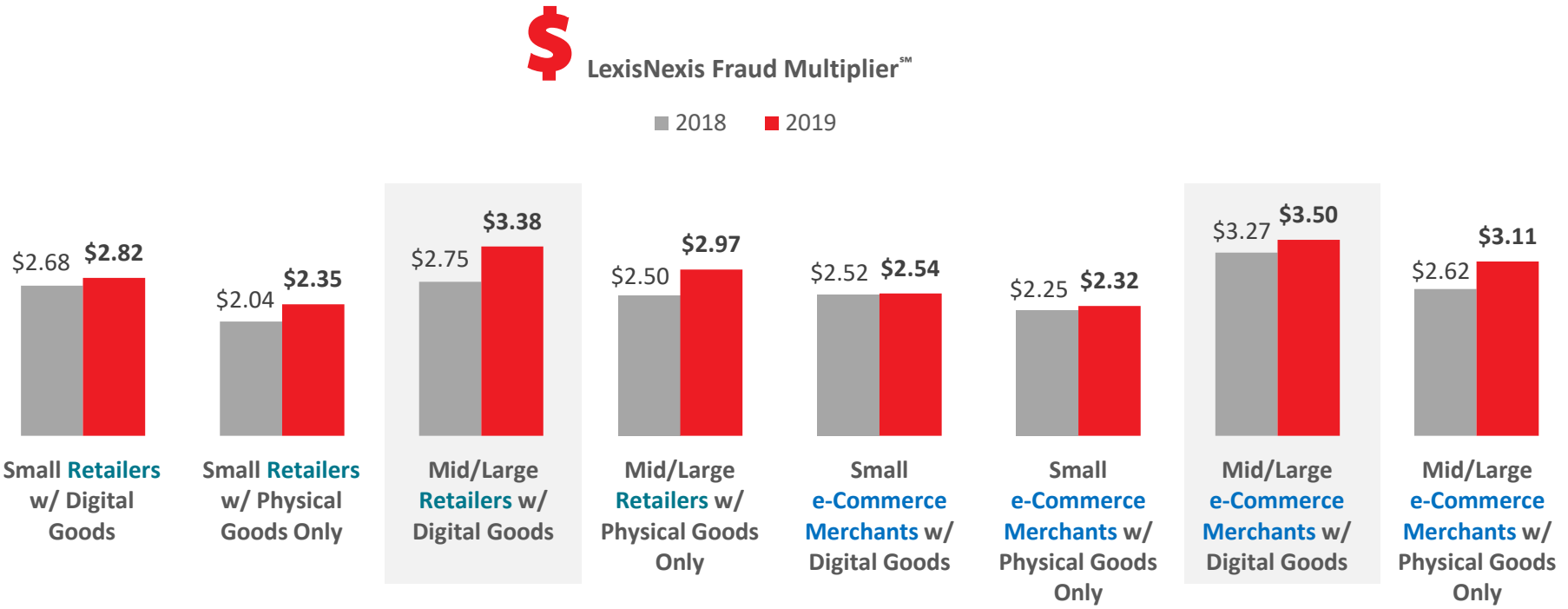
LexisNexis® RISK SOLUTIONS

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.

*N too small to report

Not surprisingly, the cost of fraud is highest for mid/large retailers and e-Commerce merchants that sell digital goods. Other segments have seen spikes since last year as well.

Not only have mid/large retailers and e-Commerce merchants that physical goods-only experienced a nearly 20% year-over-year increase in the cost of fraud, but smaller retailers have experienced sharper rises too.

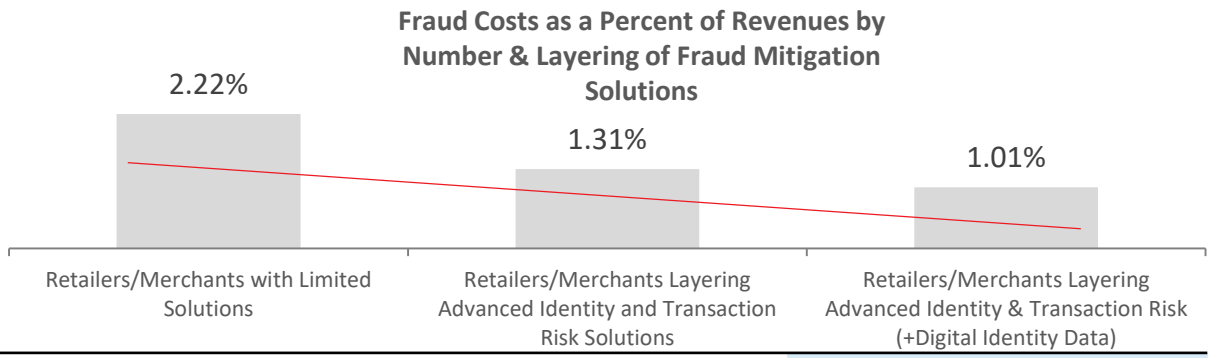


LexisNexis® RISK SOLUTIONS

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.

The lower cost of fraud, based on a layered solution approach, can improve the financial bottom line.

Study findings show that fraud cost as a percent of revenues is significantly lower for retailers and e-Commerce merchants using a layered approach, particularly one that incorporates digital identity data.



Layers of Protection		Basic	Multi-Layered	Multi-Layered with Digital Identity Data
Common Core Solutions Used Most Often	Check Verification, Authentication by Payment Instrument (CVV), Name/Address/DOB Verification, Positive/Negative Lists	✓	✓	✓
Layering of Advanced Identity Solutions (including Digital Identity Data)	Device ID Fingerprinting, Geolocation, Browser/Malware Tracking, e-Mail/Phone Risk Verification, Authentication by Biometrics, Authentication by OTP/2 Factor, Authentication by Quizzes, Authentication by Challenge Questions		✓	✓
Layering of Fraud Transaction Risk Assessment Solutions	Automated Transaction Scoring, Real-Time Transaction Tracking,		✓	✓

LexisNexis® RISK SOLUTIONS