LexisNexis® Risk Solutions 2020 True Cost of Fraud™ Study E-commerce/Retail Report

US & Canada Edition

July 2020

LexisNexis®
RISK SOLUTIONS

The LexisNexis® Risk Solutions True Cost of Fraud™ Study helps companies grow their businesses safely by navigating the growing risk of fraud.

This research provides a snapshot of current fraud trends in the United States and Canada.

It spotlights key pain points that merchants (retail and online/mobile) should be aware of as they add new payment mechanisms and expand channels into online, mobile, and international sectors.

Fraud Definitions

- Fraudulent transactions due to identity fraud, which is the misuse of stolen payments methods (such as credit cards) or personal information
- Fraudulent requests for refunds/returns, bounced checks
- Lost or stolen merchandise, as well as redistribution costs associated with redelivering purchased items

This research covers consumer-facing fraud methods. It does not include insider fraud or employee fraud.

The LexisNexis Fraud Multiplier™

- Estimates the total amount of loss a firm incurs based on the actual dollar value of a fraudulent transaction

LexisNexis® RISK SOLUTIONS

The study included a comprehensive survey of 801 risk and fraud executives in Retail and E-commerce companies in the U.S. and Canada

Retailers and E-commerce Merchants Include a Variety of Categories:

# of Survey Completions
801

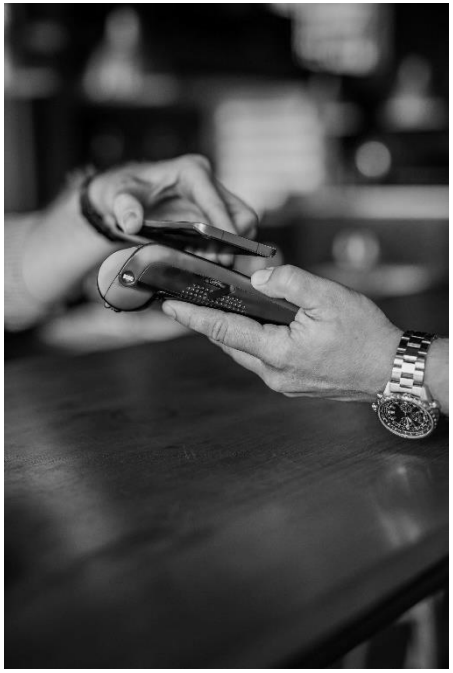
Segments

Segment definitions:	Small Earns less than $10 million in annual revenues	Mid/Large Earns $10 million+ in annual revenues	M-commerce Accept payments through either a mobile browser or app, or "bill to mobile phone"	Digital Goods Sell digital goods
# of Survey Completions	**464**	**337**	**287**	**294**

This research was conducted pre- and during the COVID-19 shutdown. Results have been analyzed by these time periods to understand any impacts on and challenges related to fraud detection and prevention during this unprecedented time.

LexisNexis® RISK SOLUTIONS

Key Findings



1. **Attacks & Costs:** Fraud continues to increase, with significant impacts to Mid / Large retailers and e-commerce merchants.

2. **Trends:** There is increased online / mobile channel activity occurring, which is increasing fraud risks and costs.

3. **Challenges & Impacts:** In addition to identity verification, the ability to distinguish legitimate customers from malicious bots and balance fraud prevention with minimal customer friction is becoming harder.

4. **Potential COVID-19 Impacts:** The shuttering of a number of bricks & mortar retail stores and stay-at-home restrictions during the peak of the COVID-19 pandemic have had an impact on retail fraud.

5. **Solutions Use:** But, as fraud continues to become more sophisticated, the use of more sophisticated solutions remains limited.

6. **Strategic Approaches:** Study findings show that those who use a layered solutions approach, as well as one that integrates cybersecurity, the digital customer experience, and fraud prevention efforts, experience fewer comparable fraud attacks, are better able to detect botnets and minimize customer friction, and realize a lower cost of fraud.

Key Finding #1: Fraud continues to increase, with significant impacts to Mid / Large retailers and E-commerce merchants.

- The cost of fraud has risen 7.3% across US retailers and e-commerce merchants. Every $1 of fraud now costs them $3.36 compared to $3.13 in 2019. This is significantly higher compared to $2.87 (USD) for Canadian retailers overall.
- While rising for Small businesses, the increased average fraud attack volume and cost is being driven by Mid / Large organizations.
- The average number of successful fraud attempts has increased more so for US Mid / Large retailers, by 43% - 48% since 2019.
- As shown later, some of this is based on increased fraud during the shuttering of bricks & mortar retailers during the COVID-19 pandemic. However, attack volumes were trending upward prior to the shutdown.

Survey Questions:
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?

The average volume of monthly fraud attacks, and particularly successful attacks, continues to increase annually for US retailers.

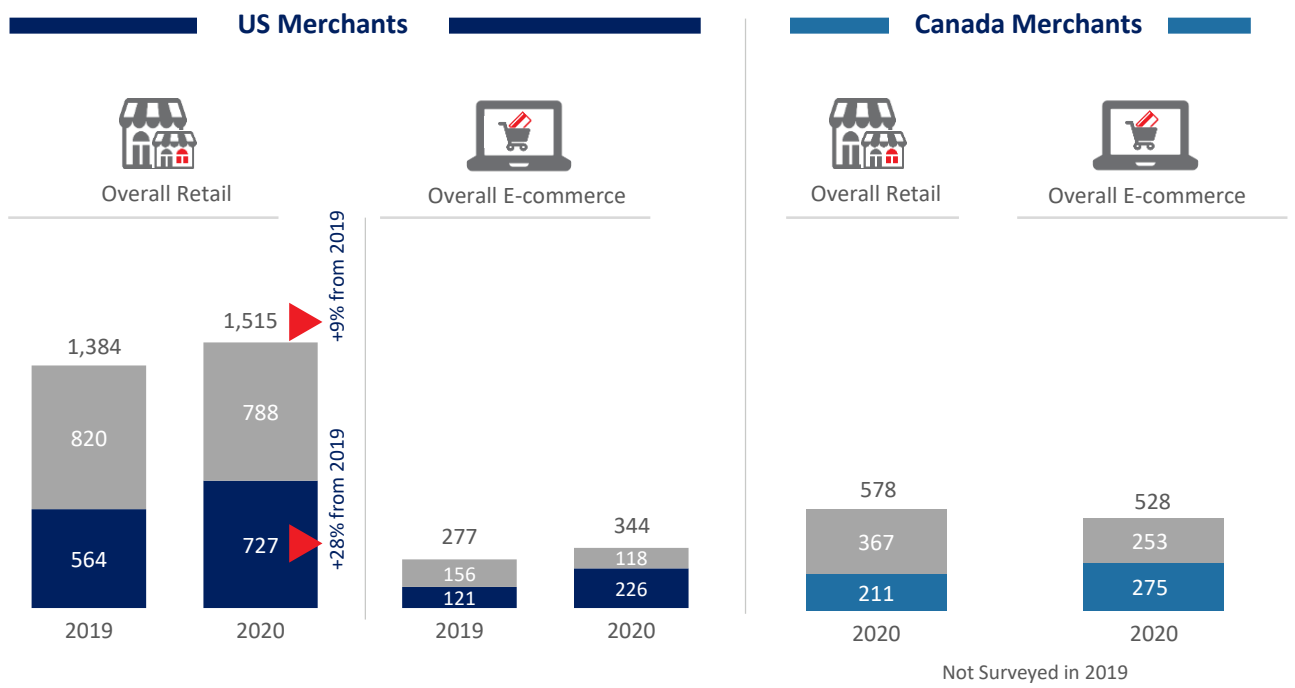
While average monthly fraud volume is comparably higher for US retailers when shown at an overall level, attack volumes are high for Mid / Large e-commerce when analyzing by size of organization.

Average # of Total Fraud Attempts Per Month

Retail & E-commerce Merchants

Average Number of Fraudulent Attempts PREVENTED per Month

Average Number of Fradulent Attempts That SUCCEED per Month



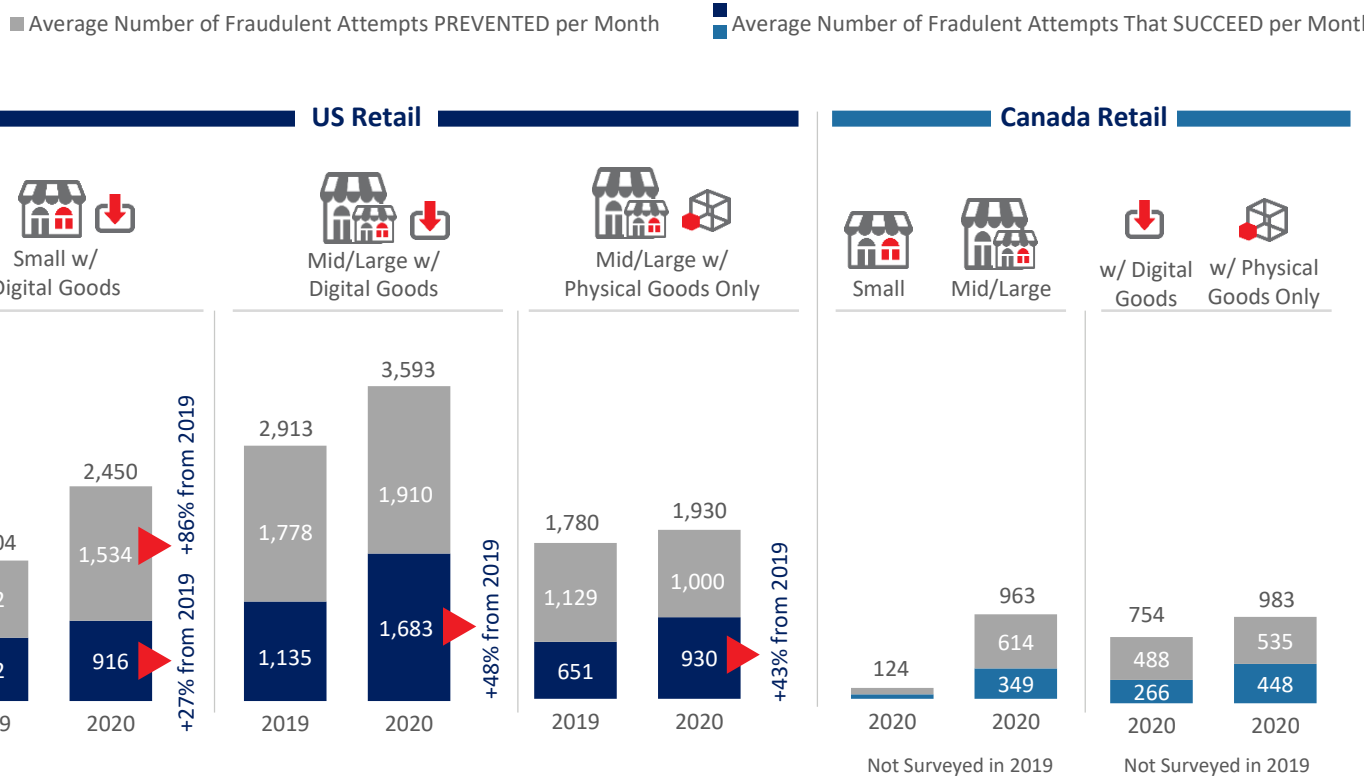
LexisNexis® RISK SOLUTIONS

Survey Questions:
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?

The increase in average monthly fraud attacks among US retailers occurs across small and large organizations, though with significantly bigger jumps in successful attacks among Mid / Large (43% - 48% increases).

Monthly fraud volumes for Canadian retailers is higher for Mid / Large organizations, yet not to the level of that experienced by US retailers.

Average # of Total Fraud Attempts Per Month — *Retail Merchants*

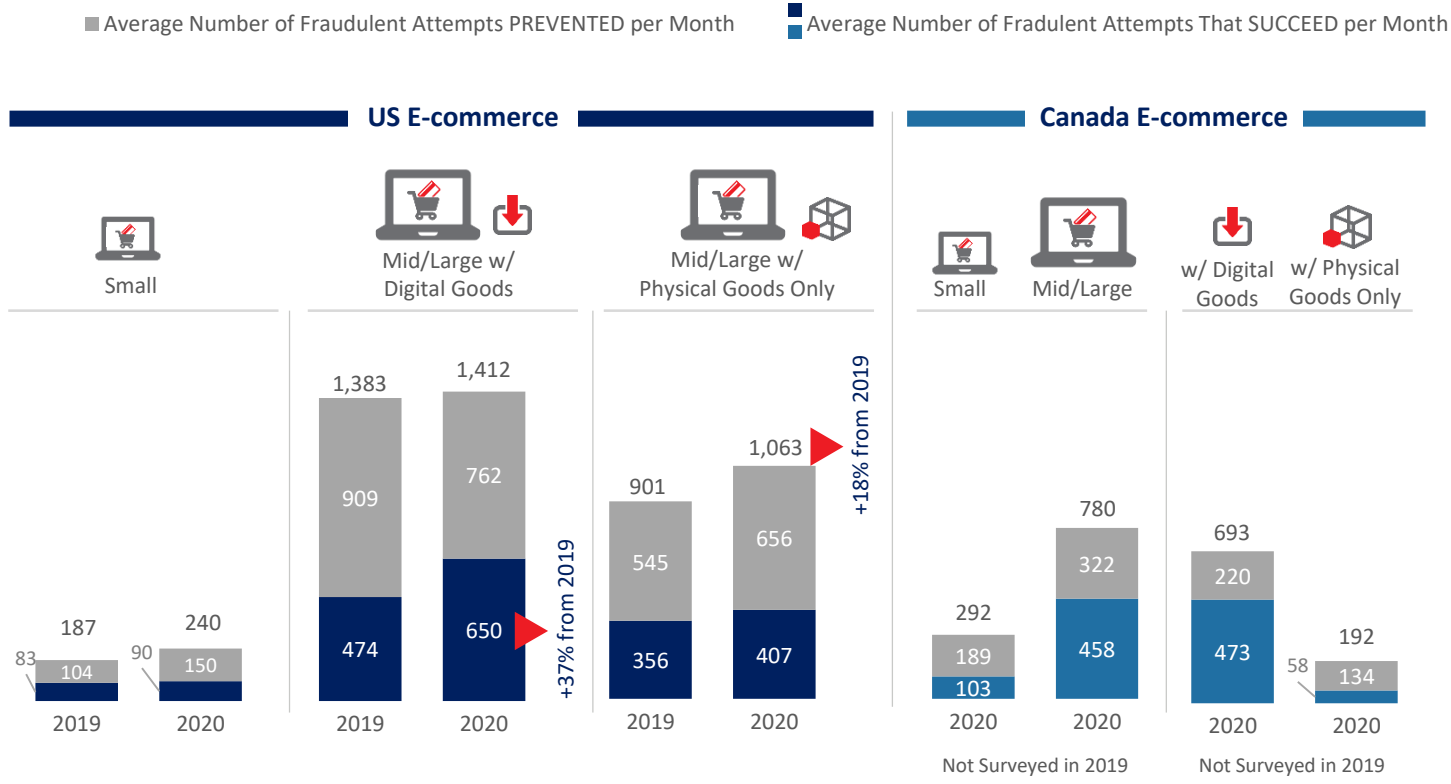


Survey Questions:
Q22: In a typical month, approximately how many fraudulent transactions are prevented by your company? Q24: In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

While overall average monthly fraud volume has not changed dramatically since 2019 for US E-commerce merchants, successful attacks have increased for larger US merchants that sell digital goods.

Average monthly fraud volumes are high for larger Canadian e-commerce merchants selling digital goods, though not quite to the level experienced by larger US merchants.

Average # of Total Fraud Attempts Per Month — *E-commerce Merchants*



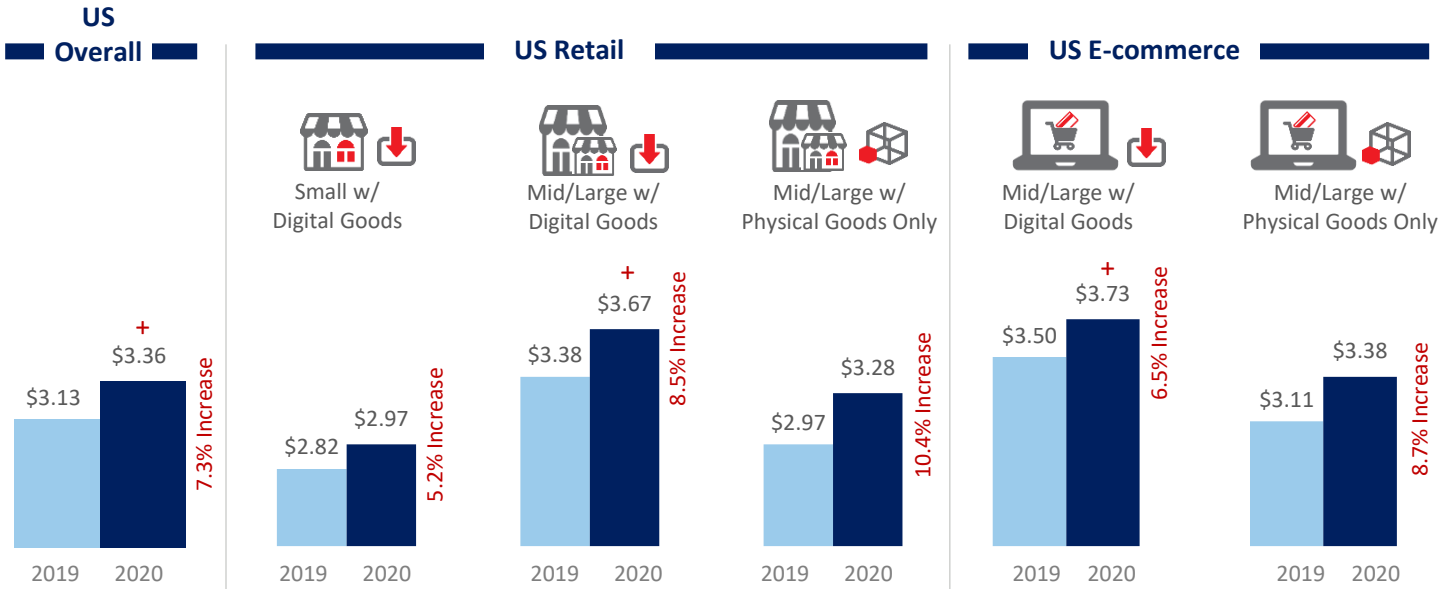
LexisNexis® RISK SOLUTIONS

Survey Question:
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 result of increased fraud volumes and trends / challenges presented in this report translate into a sizeable increase in the cost of fraud for larger US retailers and E-commerce merchants.

Overall, every $1 of fraud costs US retailers and e-commerce merchants 7.3% more in 2020 compared to 2019, from $3.13 to $3.36. This is driven by Mid / Large organizations. Those selling Digital goods have traditionally had a higher cost of fraud, given higher risks of fraud. And while there is a difference in costs between them and businesses that sell only physical goods, the latter has experienced somewhat higher cost jumps given the heightened issues shown later.

Cost of Fraud: LexisNexis Fraud Multiplier™ — *Retail & E-commerce Merchants*



+ = significantly higher than the segment counterpart

LexisNexis® RISK SOLUTIONS

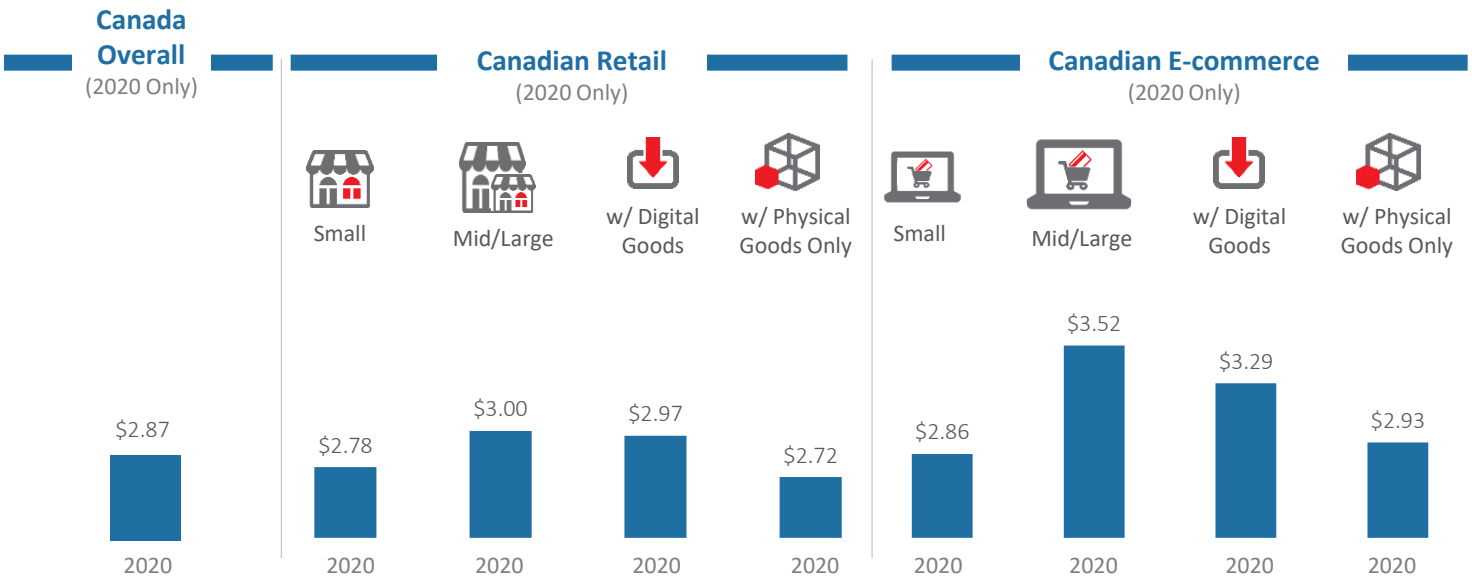
Survey Question:
Q16a: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.

Every $1 (US) of fraud costs Canadian retailers and E-commerce merchants $2.87 (USD) at an overall level. It is much higher for Mid / Large Canadian E-commerce merchants selling digital goods compared to other segments.

This is consistent with the US, given that both the channel (anonymous online) and type of transactions (digital generally means faster, more real-time) generate higher risk.

Cost of Fraud: LexisNexis Fraud Multiplier™ — *Retail & E-commerce Merchants*

All figures in U.S. Dollars



LexisNexis® RISK SOLUTIONS

Key Finding #2: There is increased online / mobile channel activity occurring, which is increasing fraud risks and costs.

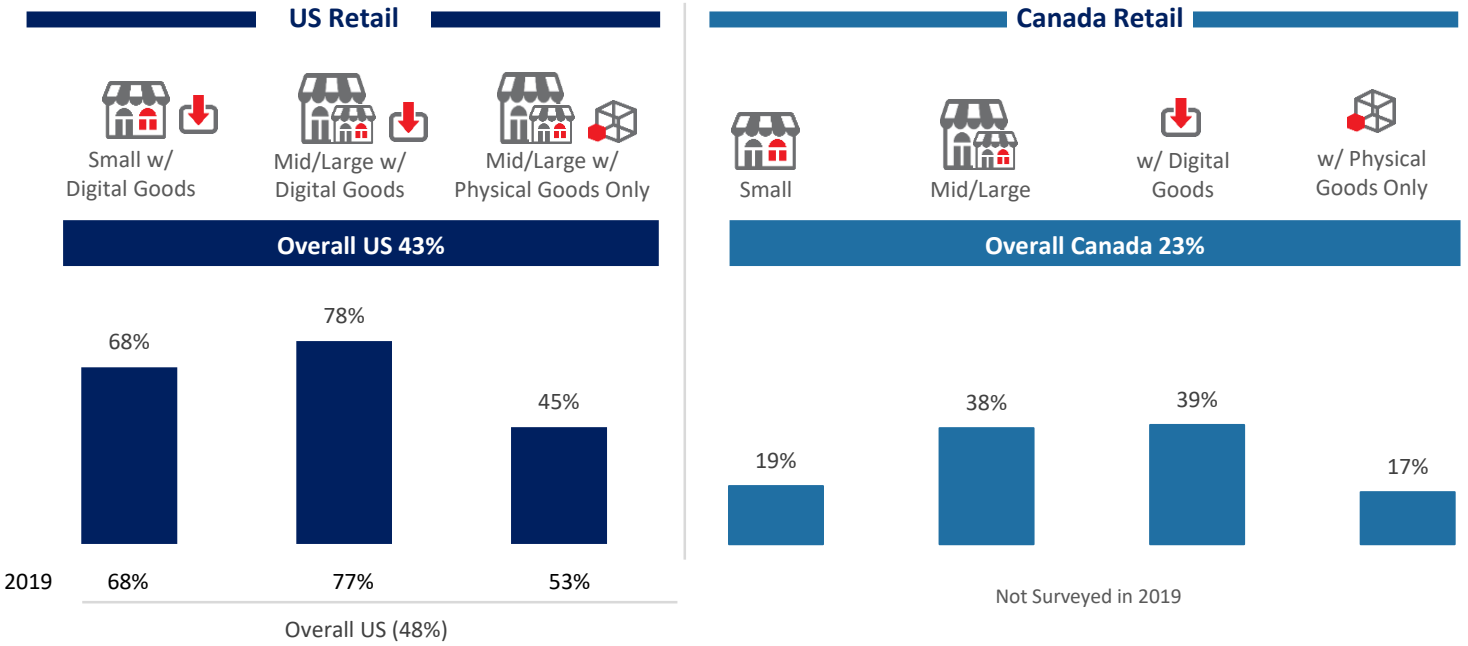
- Online transaction volume has increased for retailers, along with being a source of fraud costs. While some of this relates to the COVID-19 shutdown, there was an upward trend prior to that.
- Mobile transactions volume has increased among e-commerce merchants; this does appear to be related to the COVID-19 shutdown period.
    - Mobile browsers account for a larger share of mobile channel fraud costs compared to 2019.
    - Those conducting international transactions with m-commerce have experienced a significant increase in the percent that cross-border transactions account for among all fraud losses.
- Identity-related fraud remains a sizeable part of fraud losses, involving account takeover and fraudulent account creation. This relates to increased payment / card fraud based on CNP and identity theft.
- Much of the above involves Mid / Large organizations, particularly retailers selling only physical goods.

The number of US retailers allowing M-commerce remains steady from 2019, with significantly more use of this channel among those who sell digital goods.

The use of m-commerce is still emerging among Canadian retailers.

Use of M-commerce Transactions

Retail Merchants Conducting M-commerce



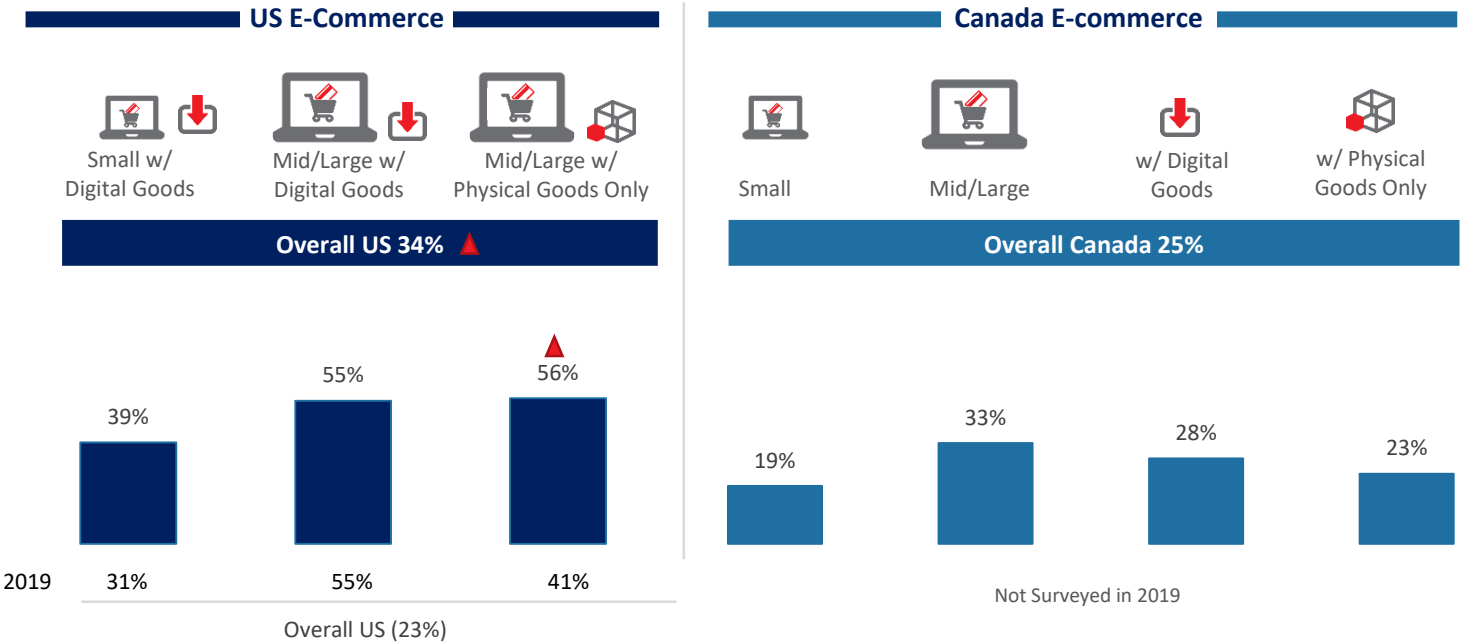
Survey Question:
Q4: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment channels currently accepted by your company.

The use of M-commerce has increased among Mid / Large US E-commerce merchants that sell only physical goods, with a directional increase among smaller US merchants who sell digital goods.

As with Canadian retailers, the use of m-commerce is still emerging among Canadian e-commerce merchants.

Use of M-commerce Transactions

E-commerce Merchants Conducting M-commerce



Survey Question:
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 higher or lower than 2019

LexisNexis® RISK SOLUTIONS

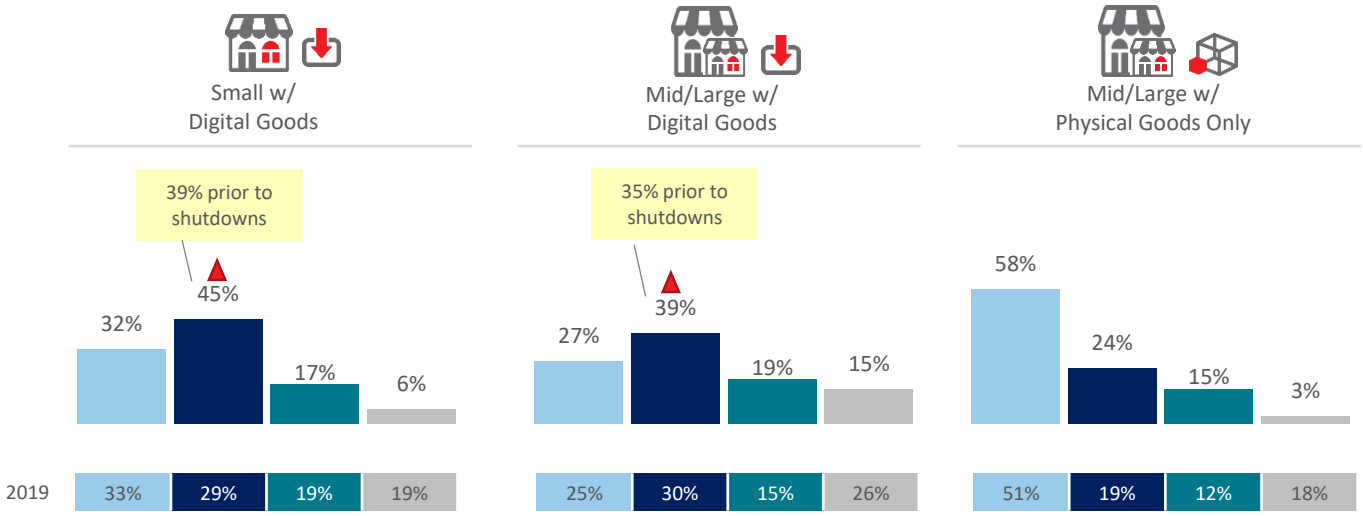
US retailers that sell digital goods and use the online channel have experienced an increase in online transaction volume.

While some of this is based on the impact of pandemic shutdowns, there was an upward trend prior to that.

% Transaction Volume by Channel

US Retail Merchants

In-Person | Online | Mobile | Other (Phone, Mail, Kiosk)



Survey Question:
Q2: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following channels used by your company. Please estimate to the best of your knowledge.

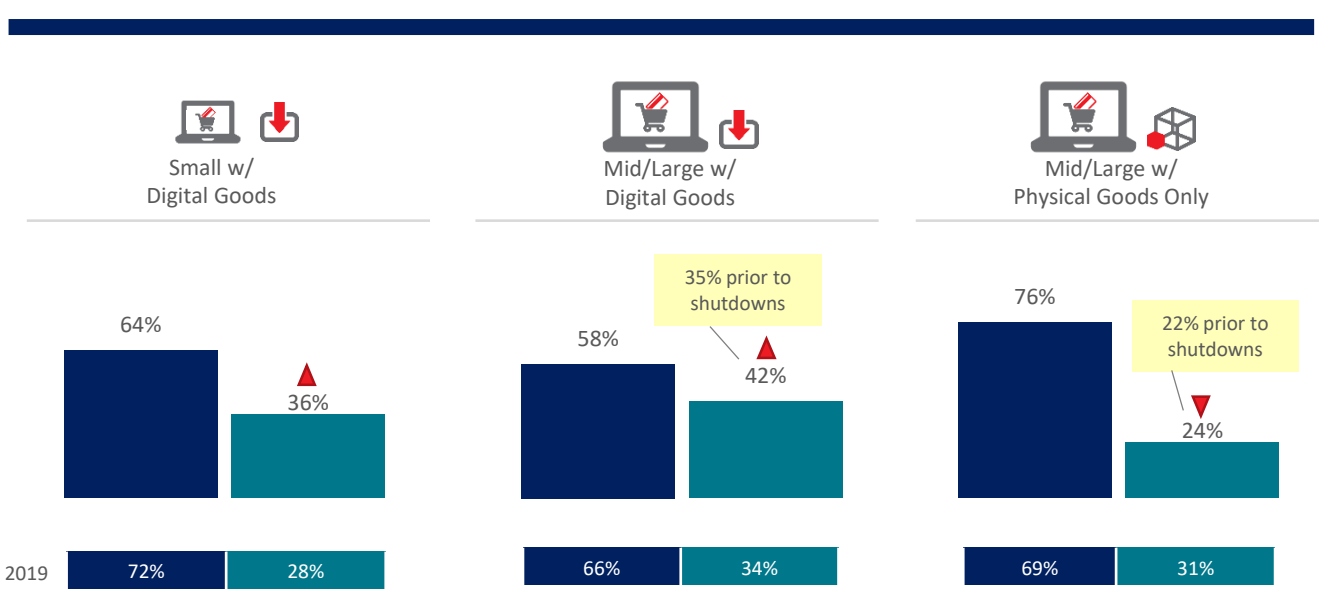
▲▼ = significantly higher or lower than 2019

The volume of transactions through the mobile channel has increased for US E-commerce merchants selling digital goods; some of this is based on the impact of pandemic shutdowns.

For Mid / Large US e-commerce merchants that sell digital goods, the trend was fairly constant from 2019 for those answering the survey prior to the shutdown. Therefore, the overall increase is based on responses during the pandemic shutdown period.

% Transaction Volume by Channel

US E-commerce Merchants w/ M-commerce



Survey Question:
Q2: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following channels used by your company. Please estimate to the best of your knowledge.

▲▼ = significantly higher or lower than 2019

LexisNexis® RISK SOLUTIONS

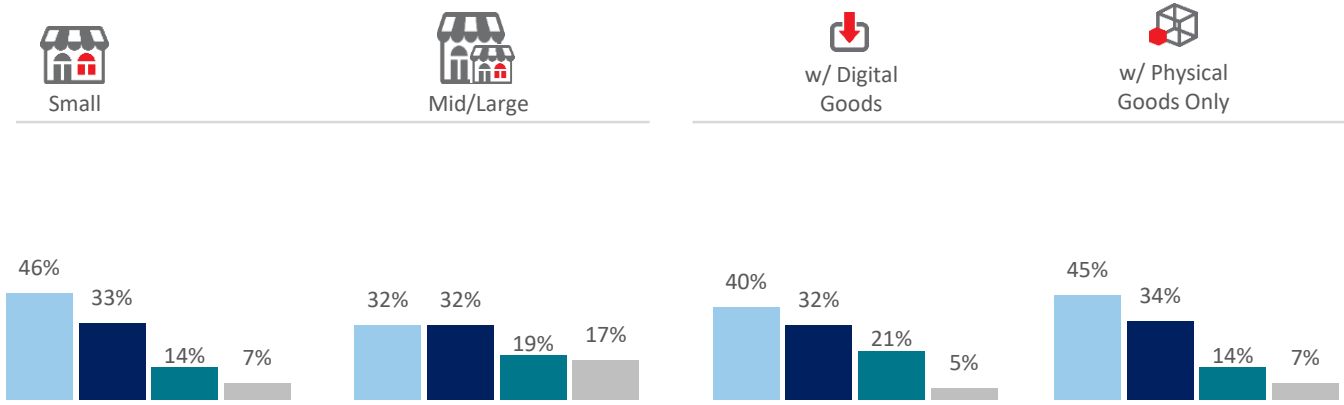
The online channel represents a sizeable portion of transactions for Canadian retailers, based on responses obtained prior to the shutdown period.

While fewer Canadian retailers allow m-commerce, the percent of mobile transactions among those who do is similar to the level of US retailers.

% Transaction Volume by Channel

Canada Retail Merchants

In-Person | Online | Mobile | Other (Phone, Mail, Kiosk)



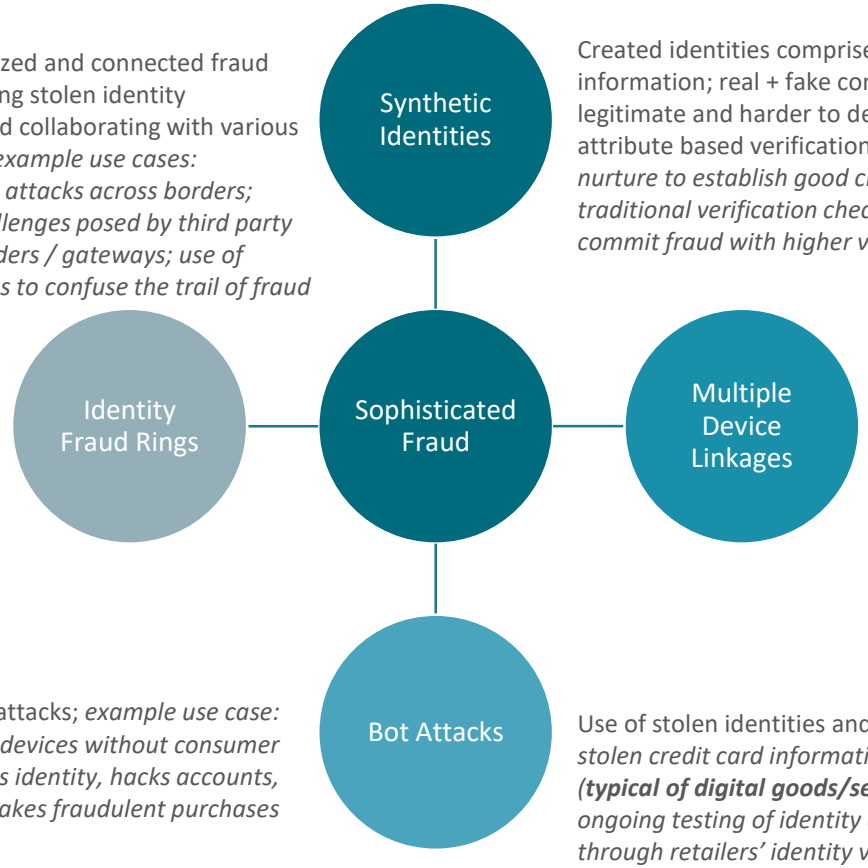
Survey Question:
Q2: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following channels used by your company. Please estimate to the best of your knowledge.

LexisNexis® RISK SOLUTIONS

Fraud is becoming more sophisticated and complex.

Traditional verification checkpoints, using physical attributes (physical address, date of birth, social security number, etc…), are less effective at detecting and preventing these types of organized fraud. This is particularly challenging for transactions conducted online or through m-commerce.

Sophisticated methods shown below not only impact identity risk assessment, but also transactional risk. One of these impacts is the limited ability to determine the transaction source / location.



Globally organized and connected fraud networks sharing stolen identity information and collaborating with various fraud attacks; *example use cases: conducting bot attacks across borders; leveraging challenges posed by third party payment providers / gateways; use of multiple devices to confuse the trail of fraud*

Created identities comprised of real and/or fake personal information; real + fake combination makes identity seem legitimate and harder to detect using traditional, physical attribute based verification methods; *example use cases; nurture to establish good credit standing, ability to pass traditional verification checkpoints and then breakout to commit fraud with higher value items*

Fraudulent device linked to multiple other devices via a unique shopping address; *example use case: purchase via mobile and pick-up at store*

Several devices associated with multiple e-mail addresses and locations; *example use case: create new fraudulent accounts, takeover of accounts and loyalty programs using proxy IP addresses*

Mobile botnet attacks; *example use case: malware infects devices without consumer knowledge; steals identity, hacks accounts, makes fraudulent purchases*

Use of stolen identities and credentials; *example use case: test stolen credit card information with lower value goods/services (**typical of digital goods/services**) tend to arouse less suspicion; ongoing testing of identity credentials to find those which pass through retailers' identity verification checks*

LexisNexis® RISK SOLUTIONS

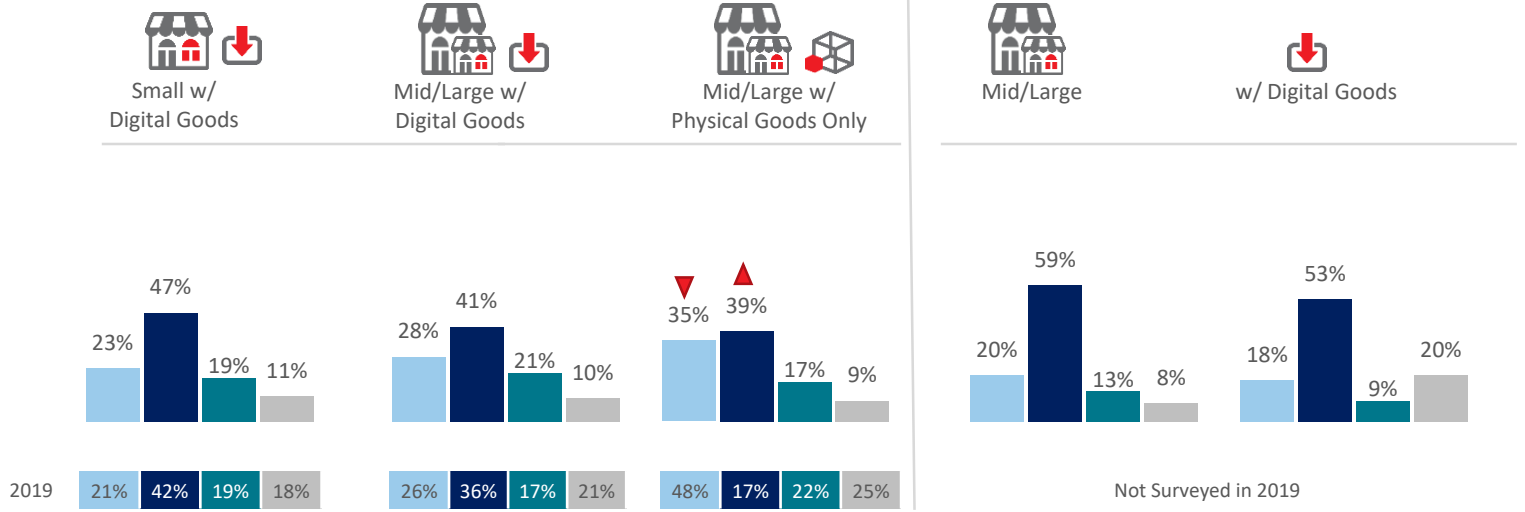
A first case in point with sophisticated fraud is that the online channel continues to represent the largest share of fraud costs for US and Canadian retailers.

The distribution of fraud costs across transaction channels remains similar year-over-year for US digital retailers that allow m-commerce. For Mid / Large US retailers that sell only physical goods, online has increased significantly as a source of fraud costs. As shown later, this is based on the impact of the shuttering of many bricks & mortar retailers during the COVID-19 pandemic; but this could also be impacted by increased identity spoofing and multiple device linkages noted earlier.

% Fraud Costs by Channel

US & Canada Retail Merchants Allowing M-commerce

In-Person | Online | Mobile | Other (Phone, Mail, Kiosk)



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

▲▼ = significantly higher or lower than 2019

LexisNexis® RISK SOLUTIONS

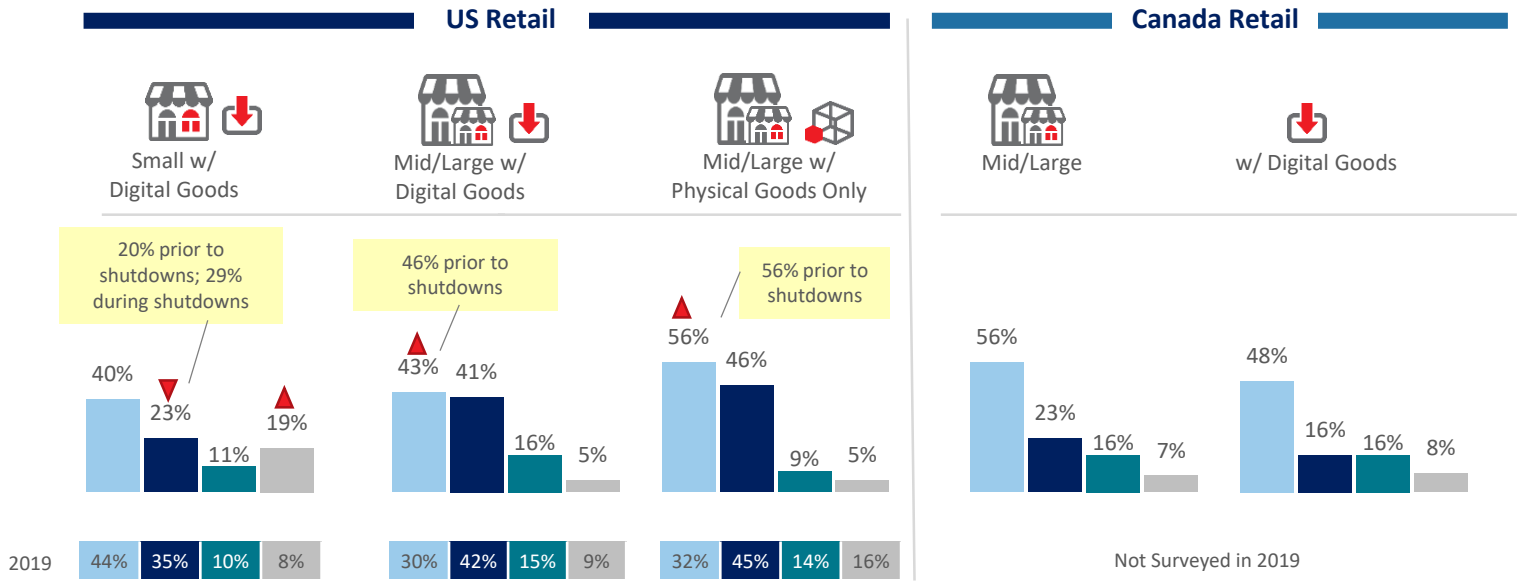
Survey Question:
Q17: Please indicate the distribution of fraud across the various mobile channels you use/accept. Please estimate to the best of your knowledge.

Within the mobile channel, mobile browsers continue to represent a sizeable portion of retail fraud losses, with related fraud losses increasing for Mid / Large US retailers, even prior to the pandemic shutdowns.

That said, mobile apps also continue to represent a similar portion of mobile channel fraud losses for larger US retail merchants, but less so among Canadian ones – not surprising since m-commerce is still in a growth stage.

This is also an area where fraudsters can use multiple device linkages to slip past traditional verification checks that are designed more for assessing fraud in-store or through non-digital attributes.

% Distribution of Fraud Losses within Mobile Channels



▲▼ = significantly higher or lower than 2019

LexisNexis® RISK SOLUTIONS

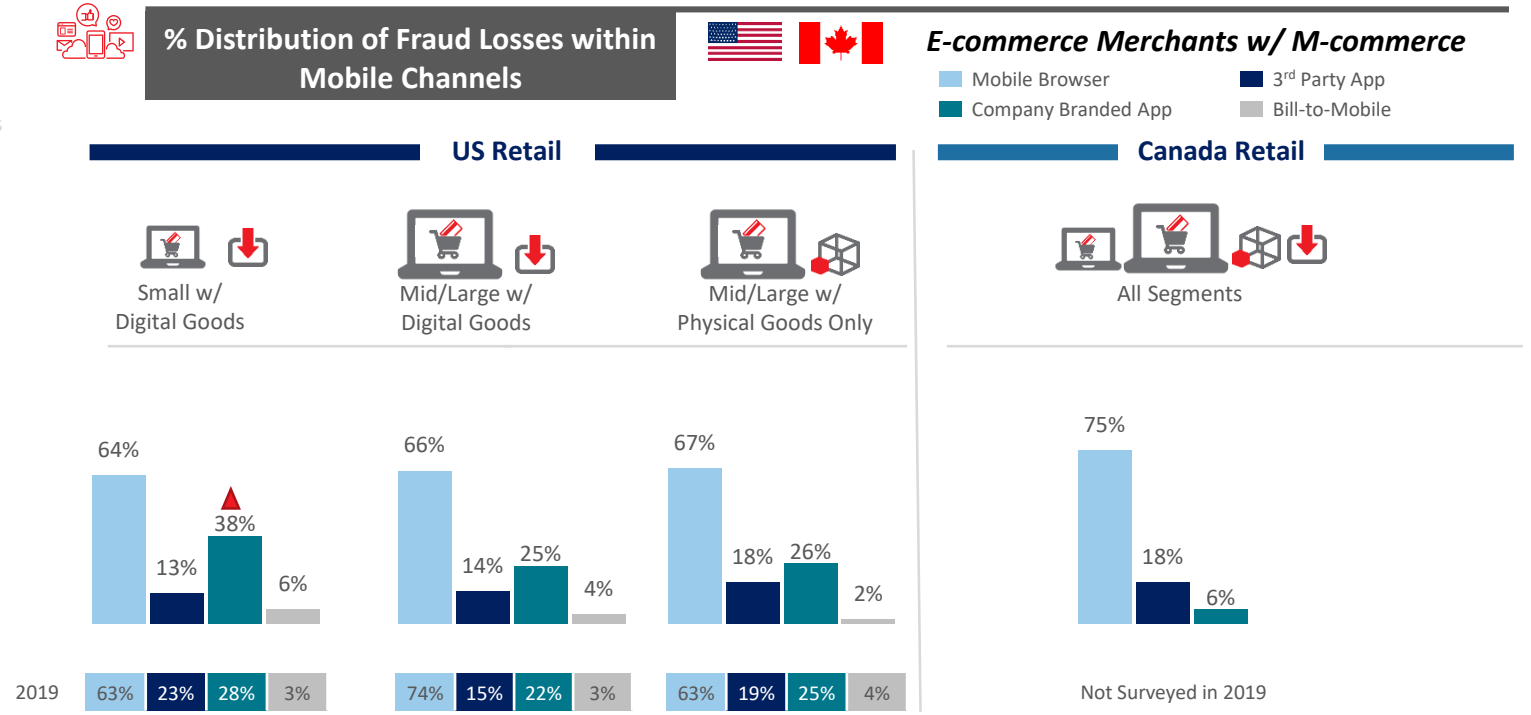
Mobile browsers also continue to represent a sizeable portion of E-commerce fraud losses within the mobile channel, even more so among US E-commerce selling digital goods than compared to their US retail counterparts.

Fraud losses related to company-branded mobile apps has risen significantly for small US e-commerce merchants that sell digital goods.

% Distribution of Fraud Losses within Mobile Channels

E-commerce Merchants w/ M-commerce

Mobile Browser | 3rd Party App | Company Branded App | Bill-to-Mobile



Survey Question:
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 higher or lower than 2019

LexisNexis® RISK SOLUTIONS

Survey Question:
Q13: Please indicate the percent of fraud costs generated through domestic orders compared to international orders in the last 12 months.

Fraud losses related to international transactions have increased for US E-commerce merchants that use the mobile channel.

This does not appear to have been a result of bricks & mortar shuttering during the pandemic; survey takers prior to that period reported similar findings. As shown later, those with international transactions report a larger percentage of transactions related to bot attacks; sophisticated global fraud networks with multiple linked devices can also confuse the original transaction source and location.

% Distribution of Fraud Losses by Domestic / International Transactions

US Retail / E-commerce
DOMESTIC TRANSACTIONS
INTERNATIONAL TRANSACTIONS

US Retail

SMALL
W/ DIGITAL GOODS & M-COMMERCE

	Domestic	International
2019	73%	27%
2020	76%	24%

MID / LARGE
W/ DIGITAL GOODS & M-COMMERCE

	Domestic	International
2019	69%	31%
2020	72%	28%

MID / LARGE
W/ PHYSICAL GOODS ONLY & M-COMMERCE

	Domestic	International
2019	69%	31%
2020	78% ▲	21%

US E-commerce

SMALL
W/ DIGITAL GOODS & M-COMMERCE

	Domestic	International
2019	85%	15%
2020	73%	**27%** ▲

MID / LARGE
W/ DIGITAL GOODS & M-COMMERCE

	Domestic	International
2019	86%	14%
2020	78%	**22%** ▲

MID / LARGE
W/ PHYSICAL GOODS ONLY & M-COMMERCE

	Domestic	International
2019	74%	26%
2020	69%	**31%** ▲

▲▼ = significantly higher or lower than 2019

LexisNexis® RISK SOLUTIONS

Survey Question:
Q13: Please indicate the percent of fraud costs generated through domestic orders compared to international orders in the last 12 months.

A sizeable portion of Mid / Large Canadian retailers' fraud losses are related to international transactions; this is significantly higher compared to smaller Canadian retailers that also conduct cross-border transactions.

Canadian retailers and e-commerce merchants that sell digital goods, in particular, experience a higher average percent of fraud losses related to international transactions.

% Distribution of Fraud Losses by Domestic / International Transactions

Canada Retail / E-commerce

DOMESTIC TRANSACTIONS
INTERNATIONAL TRANSACTIONS

Canada Retail
(2020 Only)

SMALL RETAIL

2020	87%	13%

MID / LARGE RETAIL

2020	68%	32% +

W/ DIGITAL GOODS

2020	60%	40% +

W/ PHYSICAL GOODS ONLY

2020	70%	30%

Canada E-commerce
(2020 Only)

SMALL RETAIL

2020	61%	33%

MID / LARGE RETAIL

2020	63%	37%

W/ DIGITAL GOODS

2020	54%	46% +

W/ PHYSICAL GOODS ONLY

2020	73%	27%

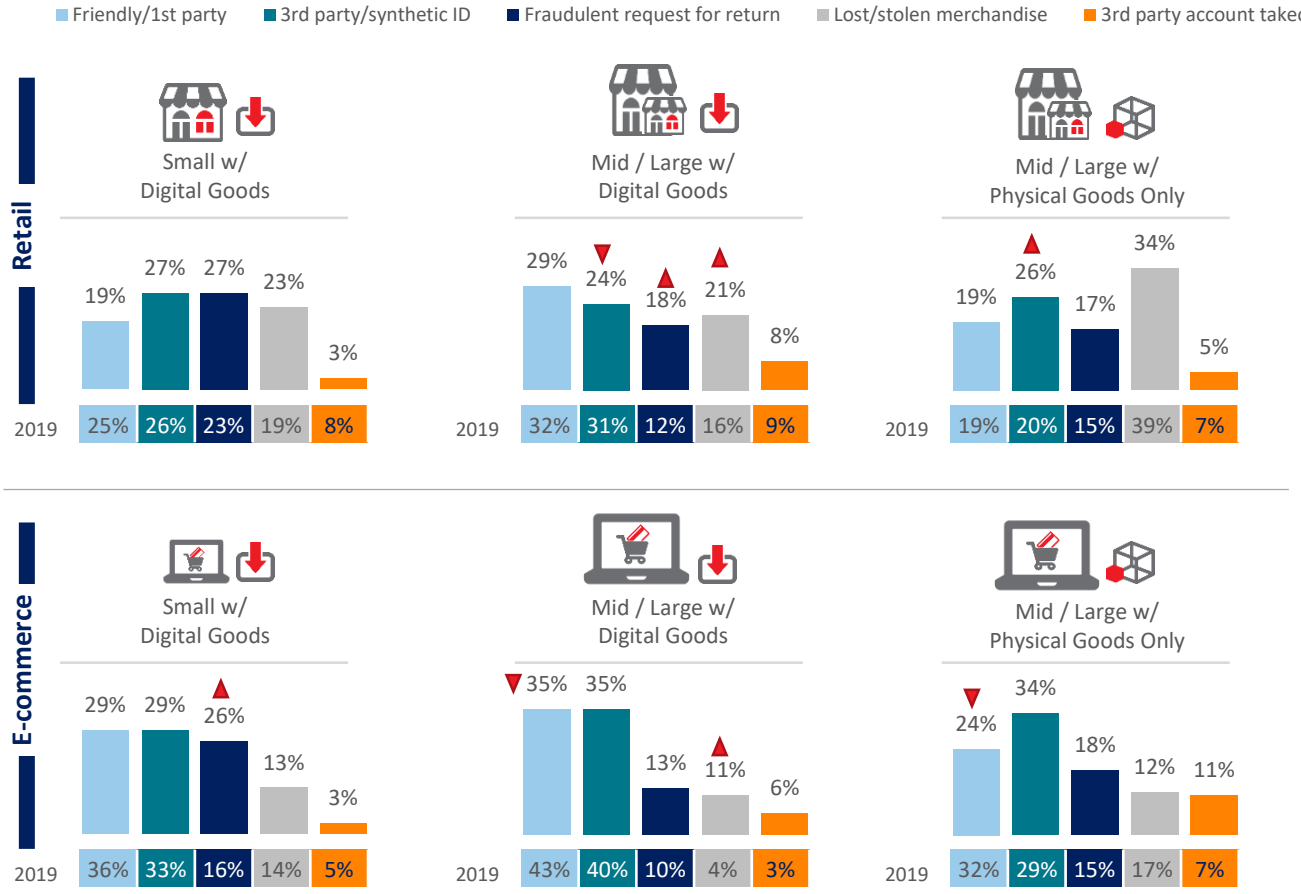
+ = significantly higher than the segment counterpart

Survey Question:
Q12: Please indicate the percentage distribution of the following fraud methods, as they are attributed to your total annual fraud loss over the past 12 months.

Identity fraud continues to be a sizeable portion of fraud losses and remains higher for Mid / Large pure E-commerce compared to others.

It has increased for Mid / Large US retailers that sell only physical goods; this segment reports less usage of solutions designed to authenticate identities in the online / mobile channels.

% Distribution of Losses by Fraud Type — *US Retail & E-commerce Merchants*



▲▼ = significantly higher or lower than 2019
+ = significantly higher than the segment counterpart

LexisNexis® RISK SOLUTIONS

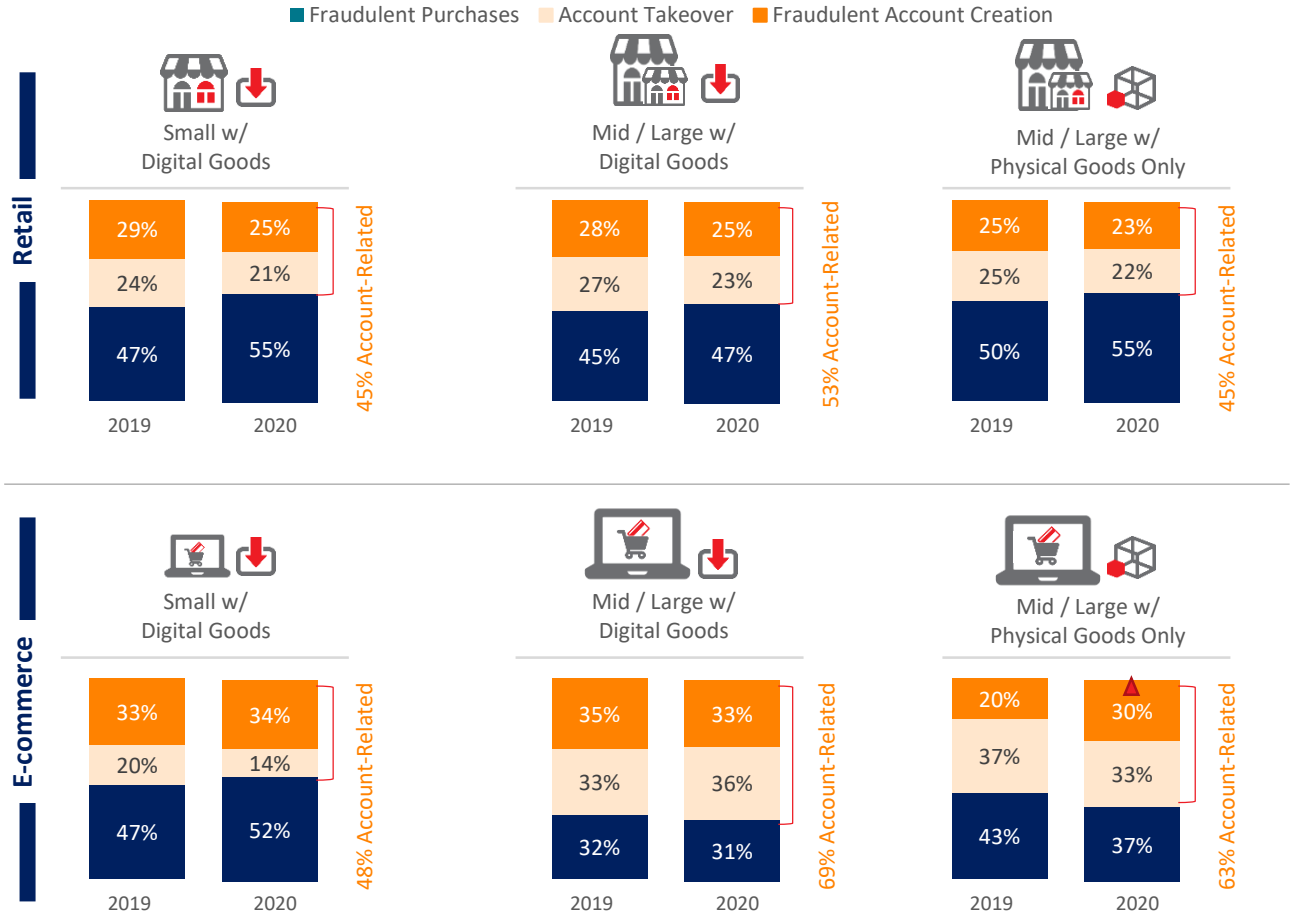
Survey Question:
Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?

Account-related takeover / fraudulent creation continues to represent a sizeable portion of identity-based fraud, particularly for larger US E-commerce.

In fact, the representation of fraudulent new account creation has increased among Mid / Large e-commerce merchants that focus only on physical goods.

Identity-Related Fraud: % Distribution by Activity

US Retail & E-commerce Merchants



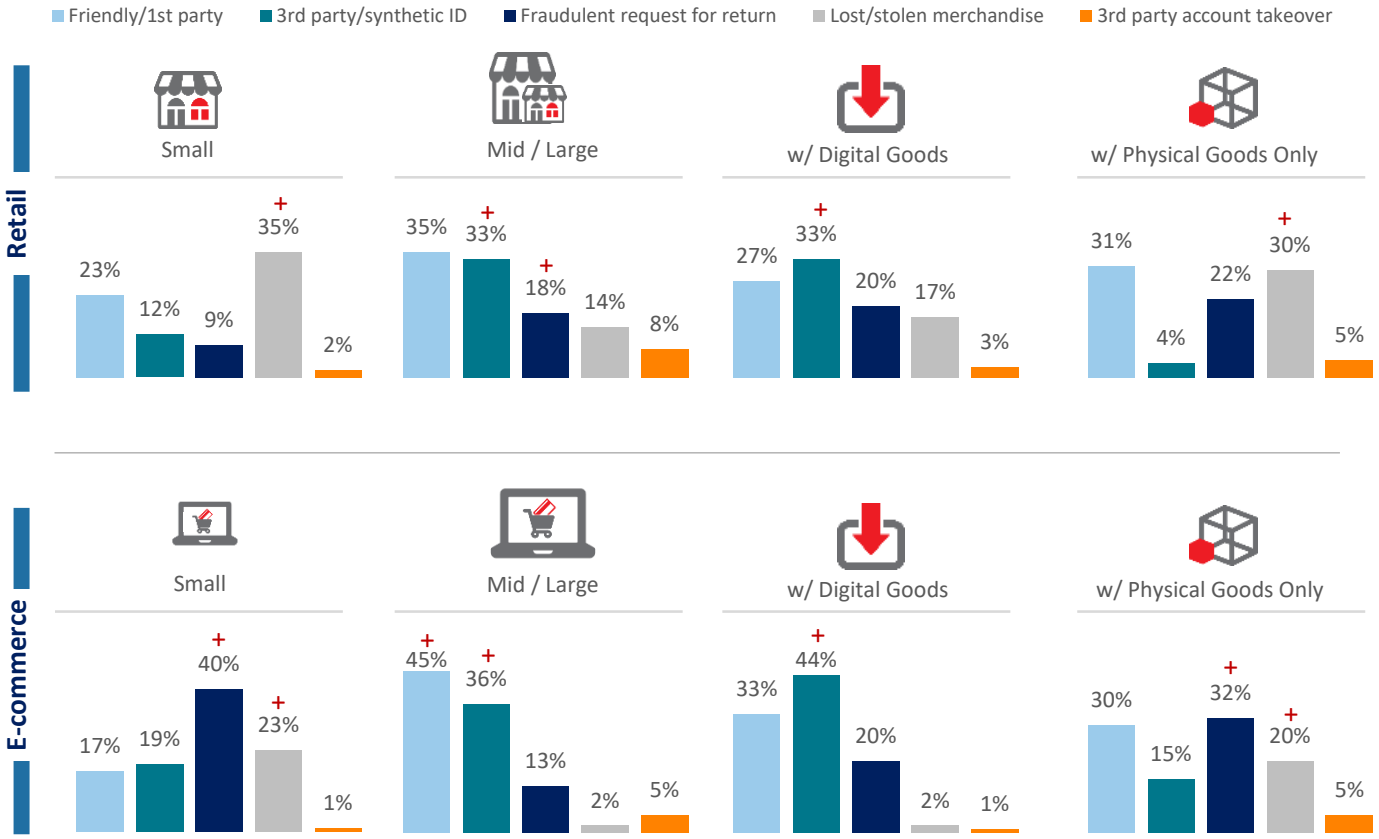
▲▼ = significantly higher or lower than 2019

LexisNexis® RISK SOLUTIONS

Identity fraud is also a sizeable proportion of fraud losses for Canadian Mid / Large retailers and E-commerce merchants selling digital goods.

% Distribution of Losses by Fraud Type

Canada Retail & E-commerce Merchants
(2020 Only)



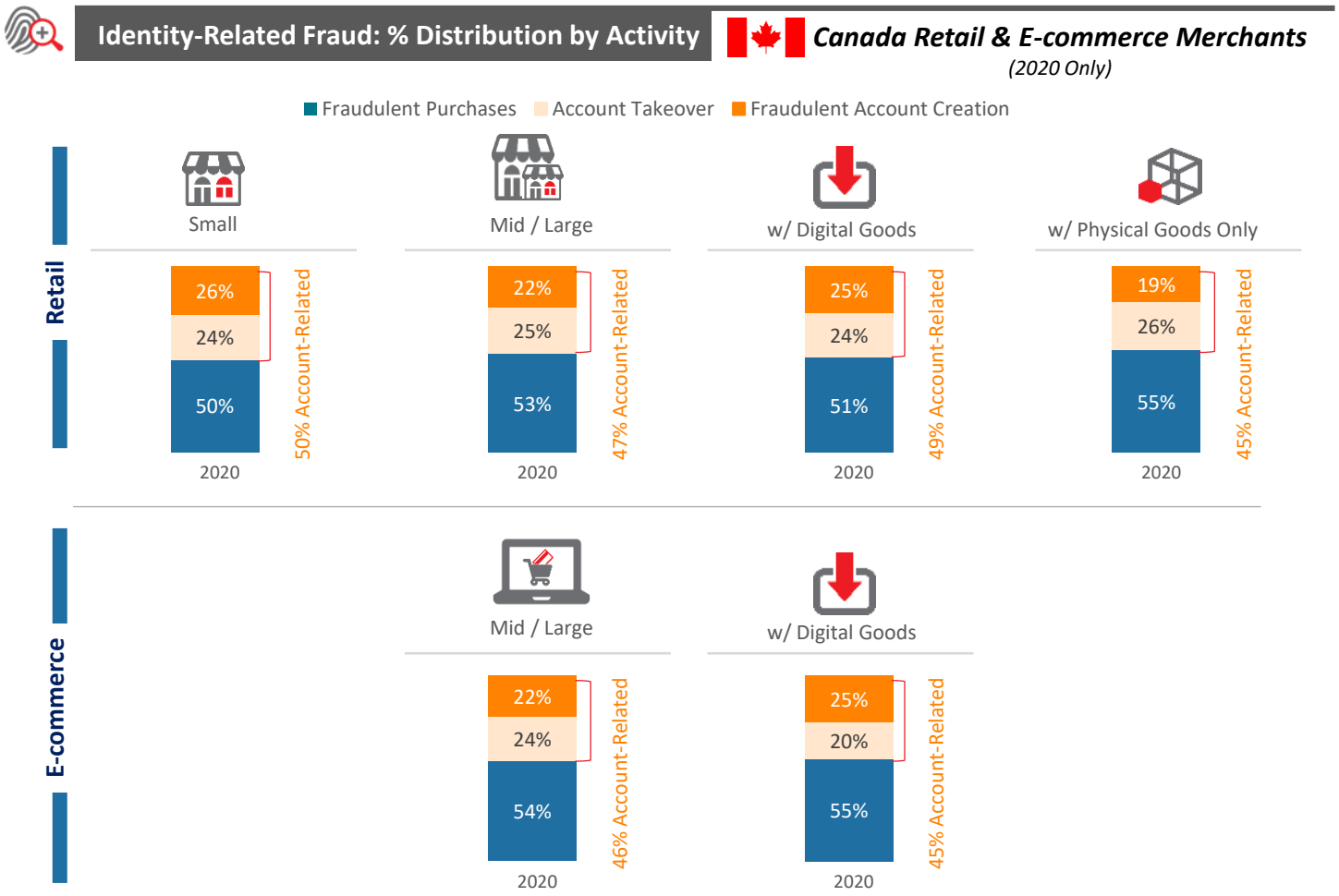
Survey Question:
Q12: Please indicate the percentage distribution of the following fraud methods, as they are attributed to your total annual fraud loss over the past 12 months.

+ = significantly higher than the segment counterpart

LexisNexis® RISK SOLUTIONS

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

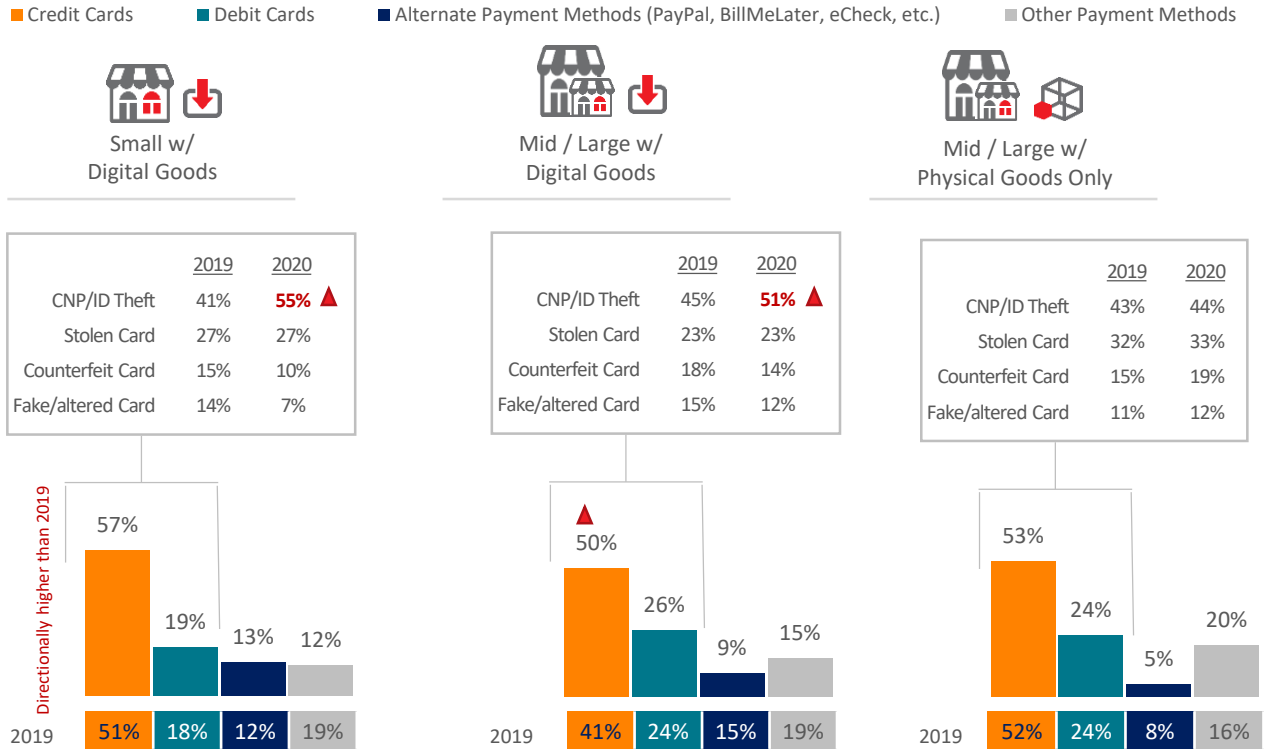
Account-related takeover / fraudulent creation also represents a sizeable portion of identity-based fraud for Canadian retailers and E-commerce merchants.



Payment / credit card fraud remains high and has increased for US retailers that sell digital goods, based on increased leverage of CPN and stolen identities.

As mentioned earlier, the use of stolen identities and credit card information is a favorite tool for fraudsters to obtain lower value goods/services often associated with digital (e-gift cards, subscriptions, games, etc…) and which can be more easily sold for a profit.

% Distribution of Losses by Payment Method — *US Retail Merchants*



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

Survey Question:
Q18: In thinking about the total fraud losses suffered by your company during the past 12 months, please indicate the distribution of various fraud costs for each of the payment methods used by your company. Of your credit or debit card-related fraud losses, please indicate the distribution across the following types of card fraud.

▲▼ = significantly higher or lower than 2019

Payment / credit card fraud also remains high for US E-commerce merchants, particularly for Mid / Large that sell digital goods.

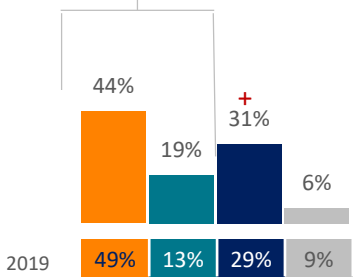
CNP / Identity theft continues to be the major reason for this, related to reasons similarly stated with US retailers, and has increased in activity for a number of US e-commerce merchants.

% Distribution of Losses by Payment Method — *US E-commerce Merchants*

Credit Cards | Debit Cards | Alternate Payment Methods (PayPal, BillMeLater, eCheck, etc.) | Other Payment Methods

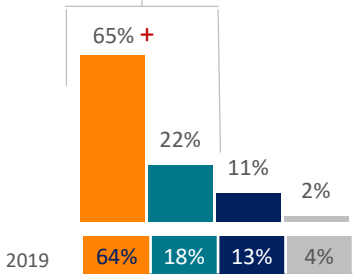
Small w/ Digital Goods

	2019	2020
CNP/ID Theft	53%	63% ▲
Stolen Card	28%	23%
Counterfeit Card	5%	5%
Fake/altered Card	3%	9%



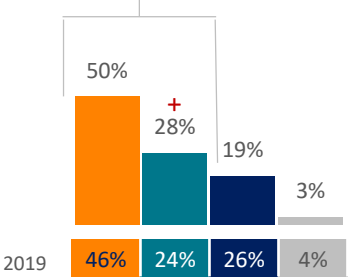
Mid / Large w/ Digital Goods

	2019	2020
CNP/ID Theft	62%	58%
Stolen Card	17%	20%
Counterfeit Card	13%	15%
Fake/altered Card	9%	7%



Mid / Large w/ Physical Goods Only

	2019	2020
CNP/ID Theft	43%	52% ▲
Stolen Card	24%	22%
Counterfeit Card	27%	21%
Fake/altered Card	6%	5%



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

Survey Question:
Q18: In thinking about the total fraud losses suffered by your company during the past 12 months, please indicate the distribution of various fraud costs for each of the payment methods used by your company. Of your credit or debit card-related fraud losses, please indicate the distribution across the following types of card fraud.

▲▼ = significantly higher or lower than 2019
\+ = significantly higher than the segment counterpart

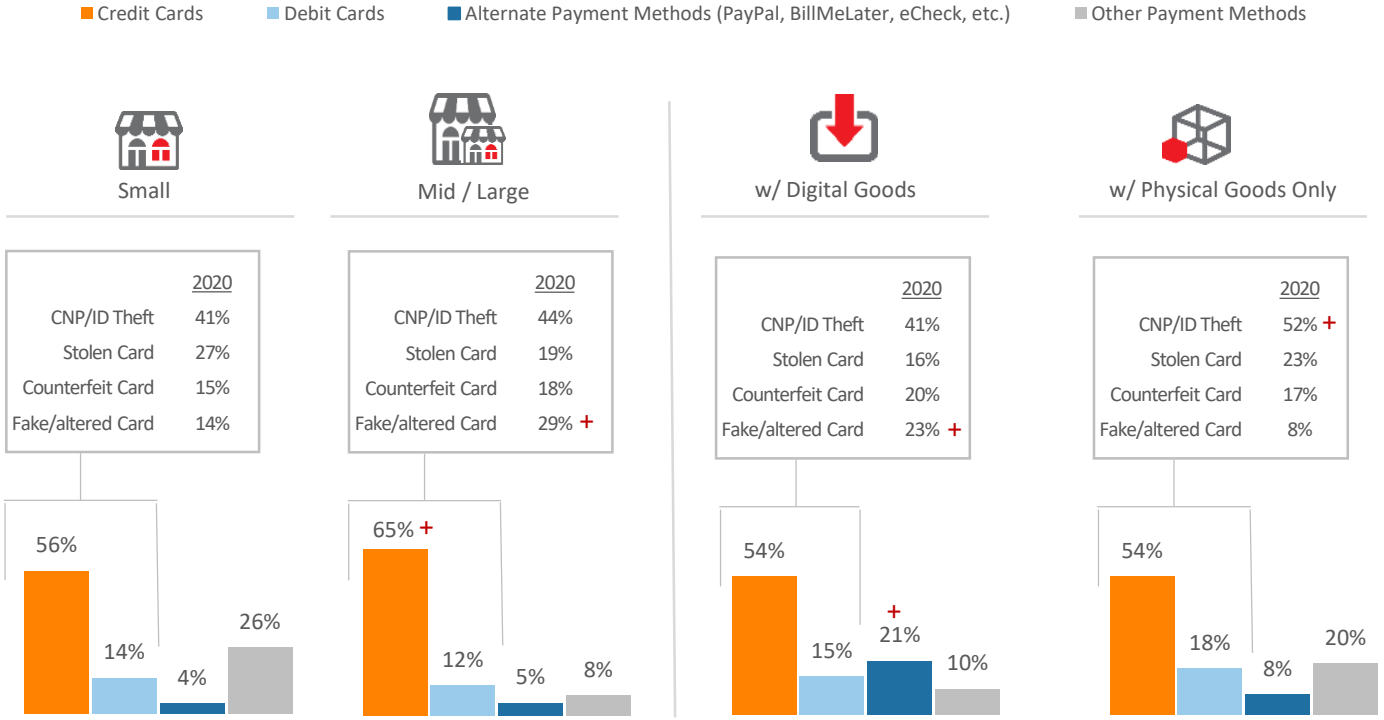
LexisNexis® RISK SOLUTIONS

Payment / credit card fraud is the primary type of payment fraud among Canadian retailers, based on CNP / Identity theft.

Those selling digital goods experience a higher percentage of fraud involving alternate payment methods.

% Distribution of Losses by Payment Method

Canada Retail Merchants *(2020 Only)*



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

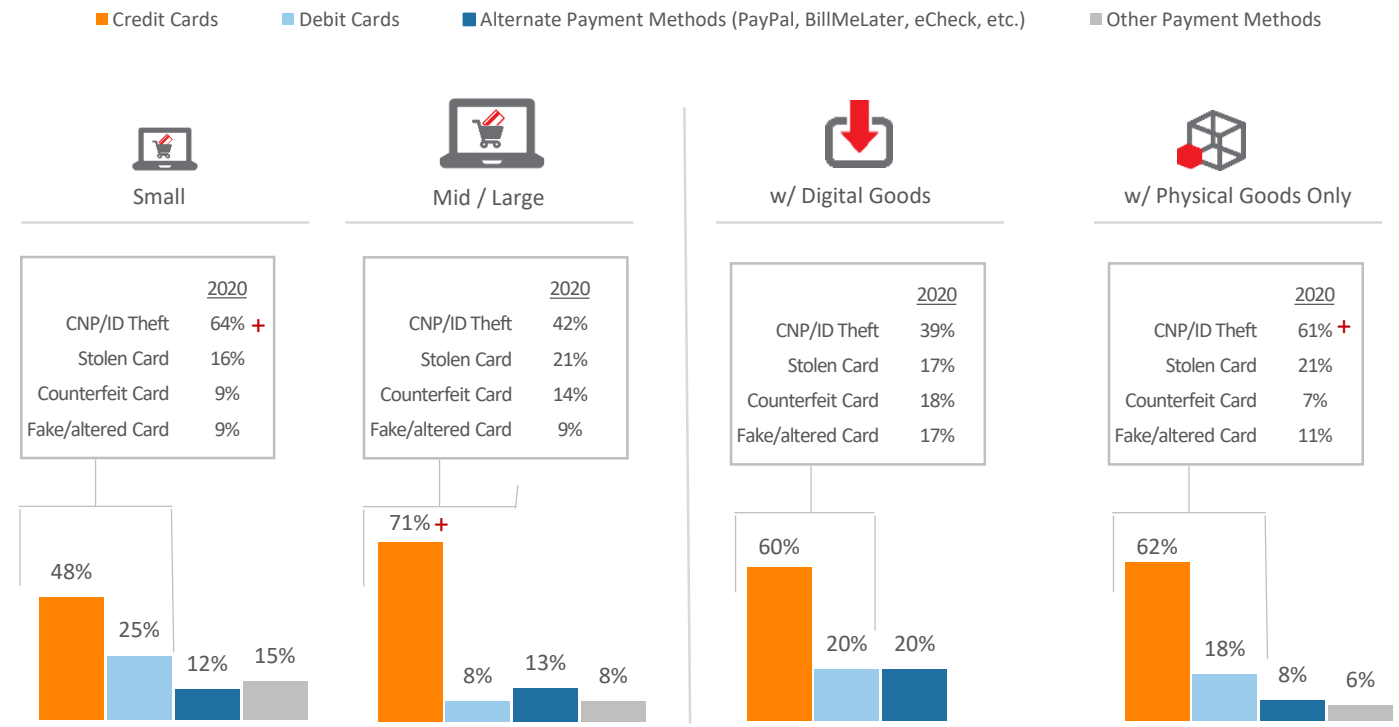
Survey Question:
Q18: In thinking about the total fraud losses suffered by your company during the past 12 months, please indicate the distribution of various fraud costs for each of the payment methods used by your company. Of your credit or debit card-related fraud losses, please indicate the distribution across the following types of card fraud.

\+ = significantly higher than the segment counterpart

And, payment / credit card fraud is the primary type of payment fraud among Canadian E-commerce merchants, particularly larger ones.

% Distribution of Losses by Payment Method

Canada E-commerce Merchants *(2020 Only)*



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

Survey Question:
Q18: In thinking about the total fraud losses suffered by your company during the past 12 months, please indicate the distribution of various fraud costs for each of the payment methods used by your company. Of your credit or debit card-related fraud losses, please indicate the distribution across the following types of card fraud.

\+ = significantly higher than the segment counterpart

Key Finding #3: In addition to identity verification, the ability to distinguish legitimate customers from malicious bots and balance fraud prevention with minimal customer friction is becoming harder.

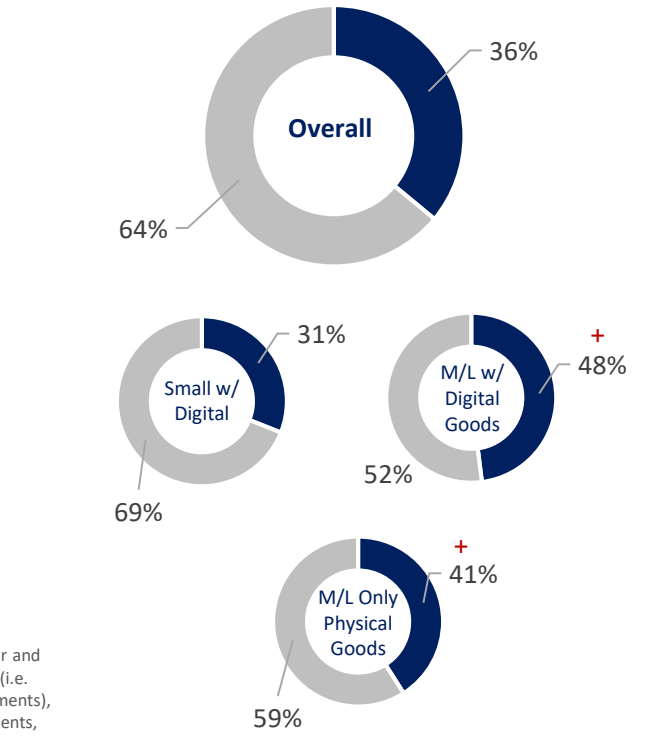
- These are complicated when purchases involve third-party, non-bank payment providers, especially where transaction speed and volume is high and transparency into complex payment chains and end customer profiles is low.
- The rise of synthetic identities and increased botnet volumes aggravate the ability to stop fraudsters while not alienating legitimate customers.
- Those newer to m-Commerce struggle with the above issues more so than others, especially those who have not invested in fraud detection / mitigation solutions designed specifically for the unique risks and threats from the mobile channel and digital transactions. There is particular need for more real-time data and fraud detection.

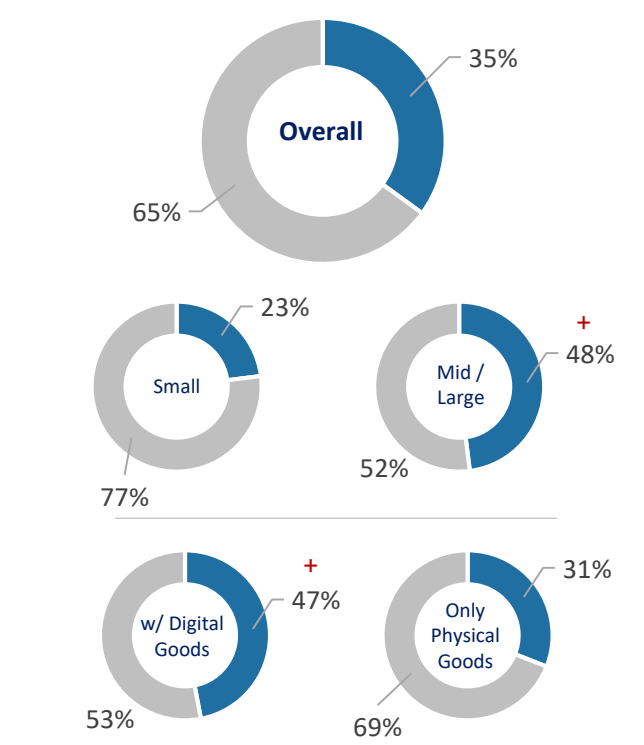
A sizeable portion of Mid / Large US and Canadian retailers have been significantly challenged with transactions flowing through third-party, non-bank payment providers, particularly those selling digital goods.

Impact of Non-Bank / 3rd Party Payment Providers*

Retail Merchants

Moderate / Large Degree of Challenges
No or Minimal Degree of Challenges





Survey Question:
Q42a: To what degree have non-bank payment service providers and systems created challenges to your business's fraud detection and prevention processes/operations during the past year?

* Non-bank payment can involve a variety of different provider and systems types, such as Mobile and Internet Payment Systems (i.e. mobile wallets, peer-to-peer payments, and social media payments), payment services providers (i.e., PayPal, Stripe, Amazon Payments, Authorize.net, etc.) and FinTech companies. First asked in 2020.

+ = significantly higher than the segment counterpart

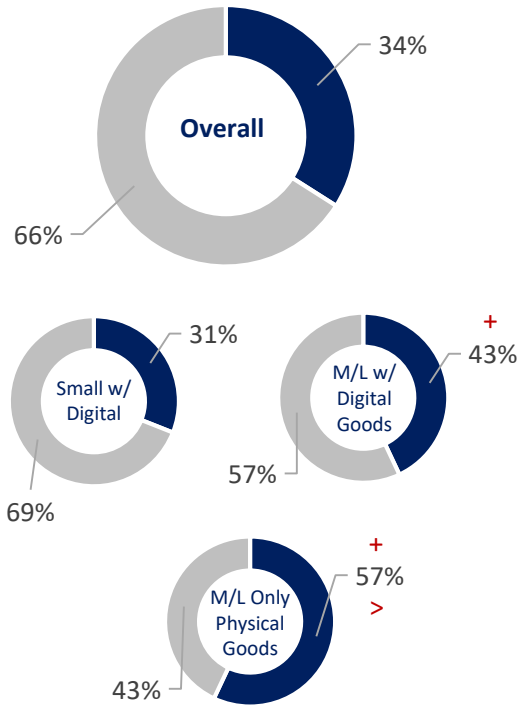
Larger, pure E-commerce merchants are not only more challenged by non-bank payment providers compared to smaller merchants, but they are more challenged than their retail counterparts that operate online and/or mobile commerce channels.

Impact of Non-Bank / 3rd Party Payment Providers*

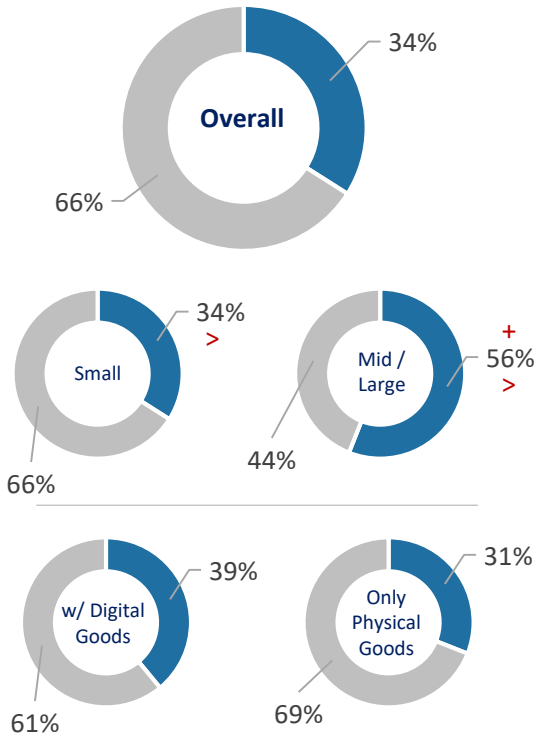
E-commerce Merchants

Moderate / Large Degree of Challenges
No or Minimal Degree of Challenges

US E-commerce



Canada E-commerce



Survey Question:
Q42a: To what degree have non-bank payment service providers and systems created challenges to your business's fraud detection and prevention processes/operations during the past year?

* Non-bank payment can involve a variety of different provider and systems types, such as Mobile and Internet Payment Systems (i.e. mobile wallets, peer-to-peer payments, and social media payments), payment services providers (i.e., PayPal, Stripe, Amazon Payments, Authorize.net, etc.) and FinTech companies. First asked in 2020.

+ = significantly higher than the segment counterpart
> = significantly higher than Retail with e-commerce channel within segment

LexisNexis® RISK SOLUTIONS

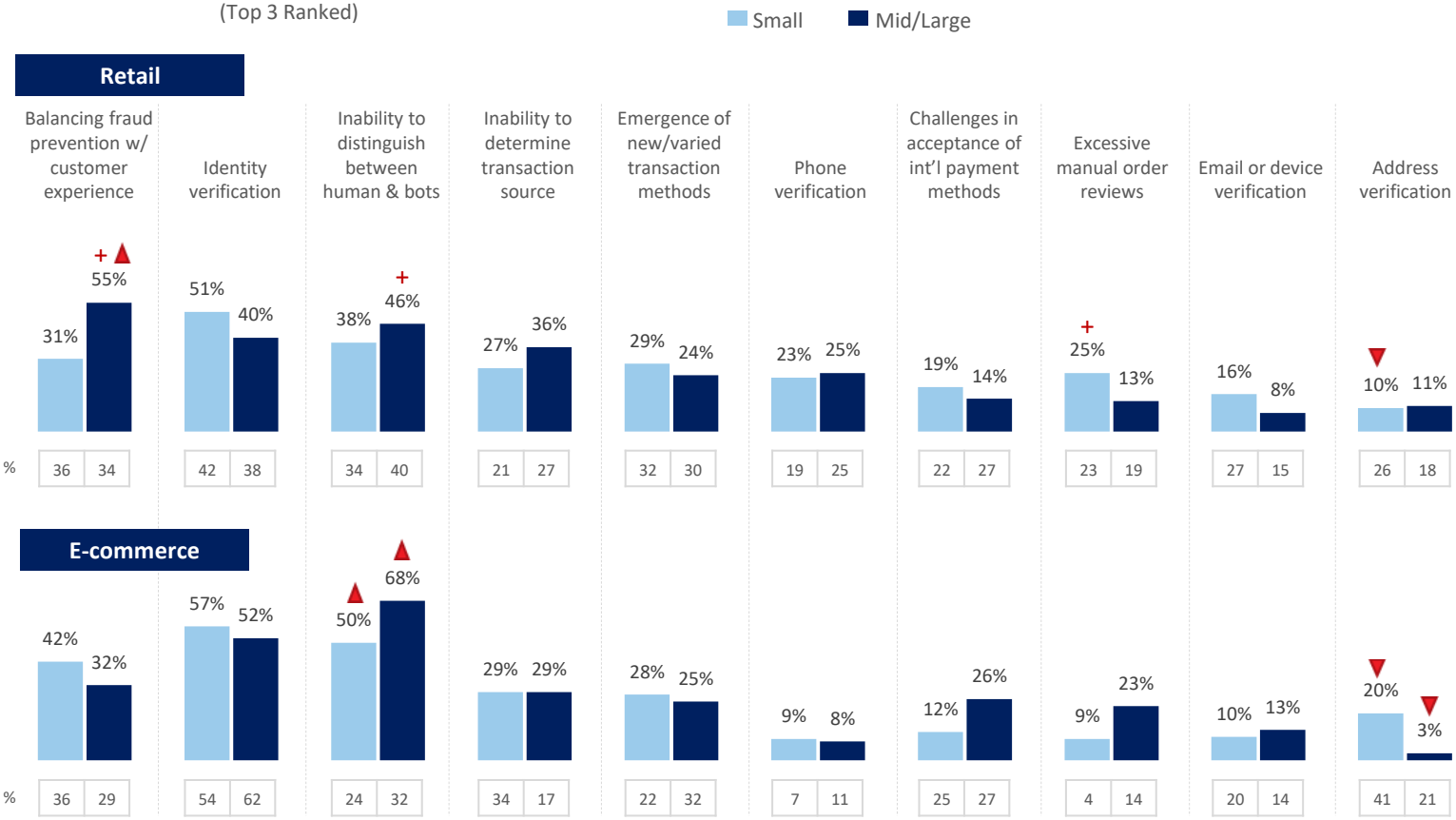
While identity verification remains a top challenge when selling digital goods, balancing fraud prevention with customer friction has become a larger issue for Mid / Large US retailers.

The ability to distinguish between legitimate human and malicious botnet attacks is also a key challenge when selling digital goods, and has become an issue for more e-commerce merchants.

Challenges When Selling Digital Goods

US Retail & E-commerce Merchants

(Top 3 Ranked)



Survey Questions:
Q19: Please rank the top 3 factors are a challenge when selling DIGITAL goods .

▲▼ = significantly higher or lower than 2019 + = significantly higher than the segment counterpart

 |

LexisNexis® RISK SOLUTIONS

Survey Questions:
Q19: Please rank the top 3 factors are a challenge when selling DIGITAL goods .

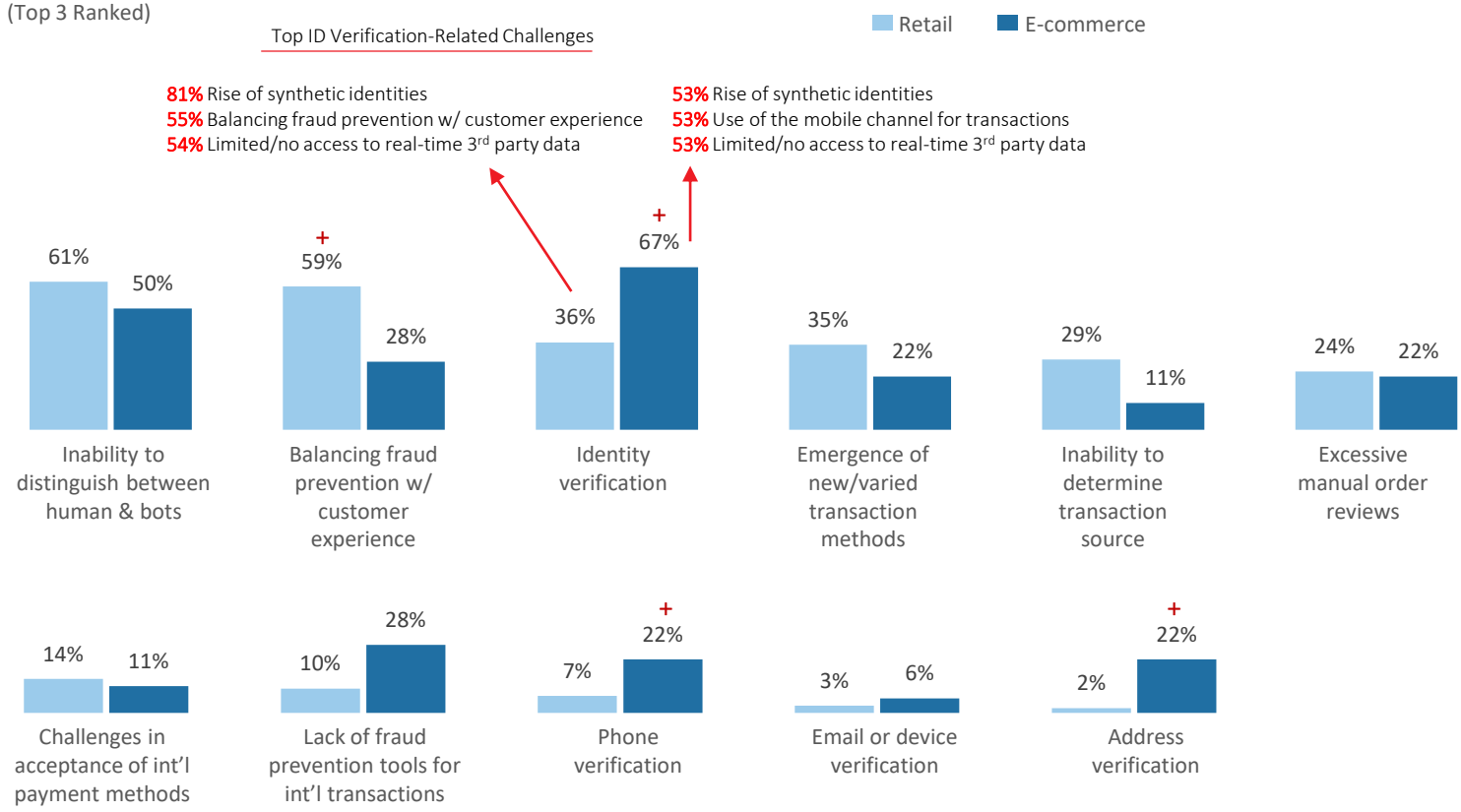
Identity verification is a particular challenge for Canadian E-commerce merchants that sell digital goods, based on the rise of synthetic identities, use of the mobile channel, and limited access to real-time third-party data.

Since the survey question allows for selecting only three choices as top challenges, the lower percentage for identity verification among retailers doesn't necessarily mean that it is not a challenge. Rather, more retailers concentrated on the impact of botnets and minimizing customer friction.

Challenges When Selling Digital Goods

Canada Retail & E-commerce Merchants

(Top 3 Ranked)



+ = significantly higher than the segment counterpart

LexisNexis® RISK SOLUTIONS

Small US retailers that sell digital goods are becoming more challenged by identity verification with both online and mobile transactions.

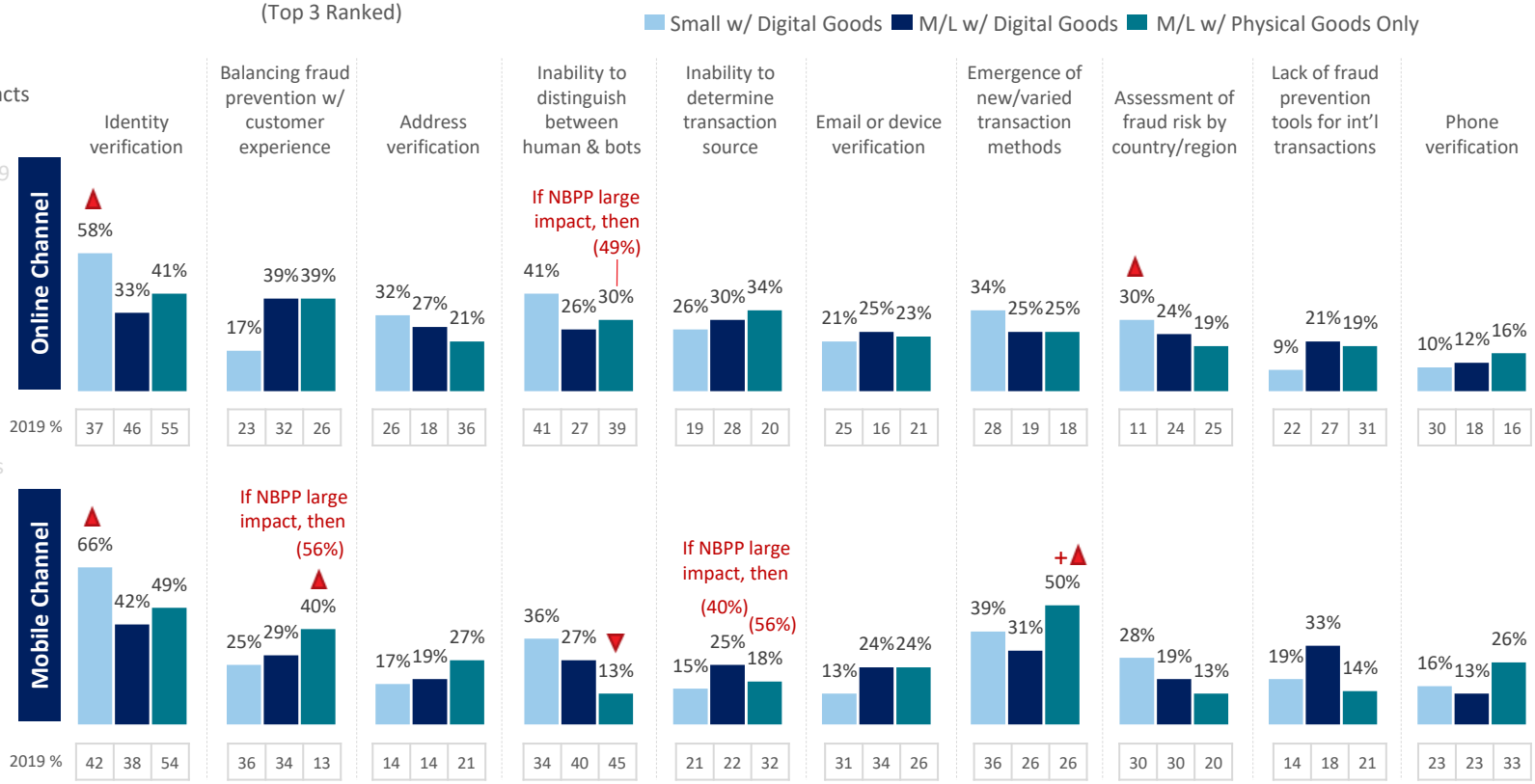
Balancing fraud prevention with minimizing customer friction is a mobile channel challenge for more Mid / Large US retailers that sell only physical goods; this has changed significantly since 2019. This segment has many new entrants to m-commerce during the past two years, though – as shown later – many have not adopted risk mitigation solutions designed to effectively assess fraud in the mobile channel. This challenge increases among those being negatively impacted by non-bank payment providers.

Fraud Challenges by Transaction Channel

US Retail Merchants

(Top 3 Ranked)

Survey Questions:
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online/mobile channel.



▲▼ = significantly higher or lower than 2019 + = significantly higher than the segment counterpart

LexisNexis® RISK SOLUTIONS

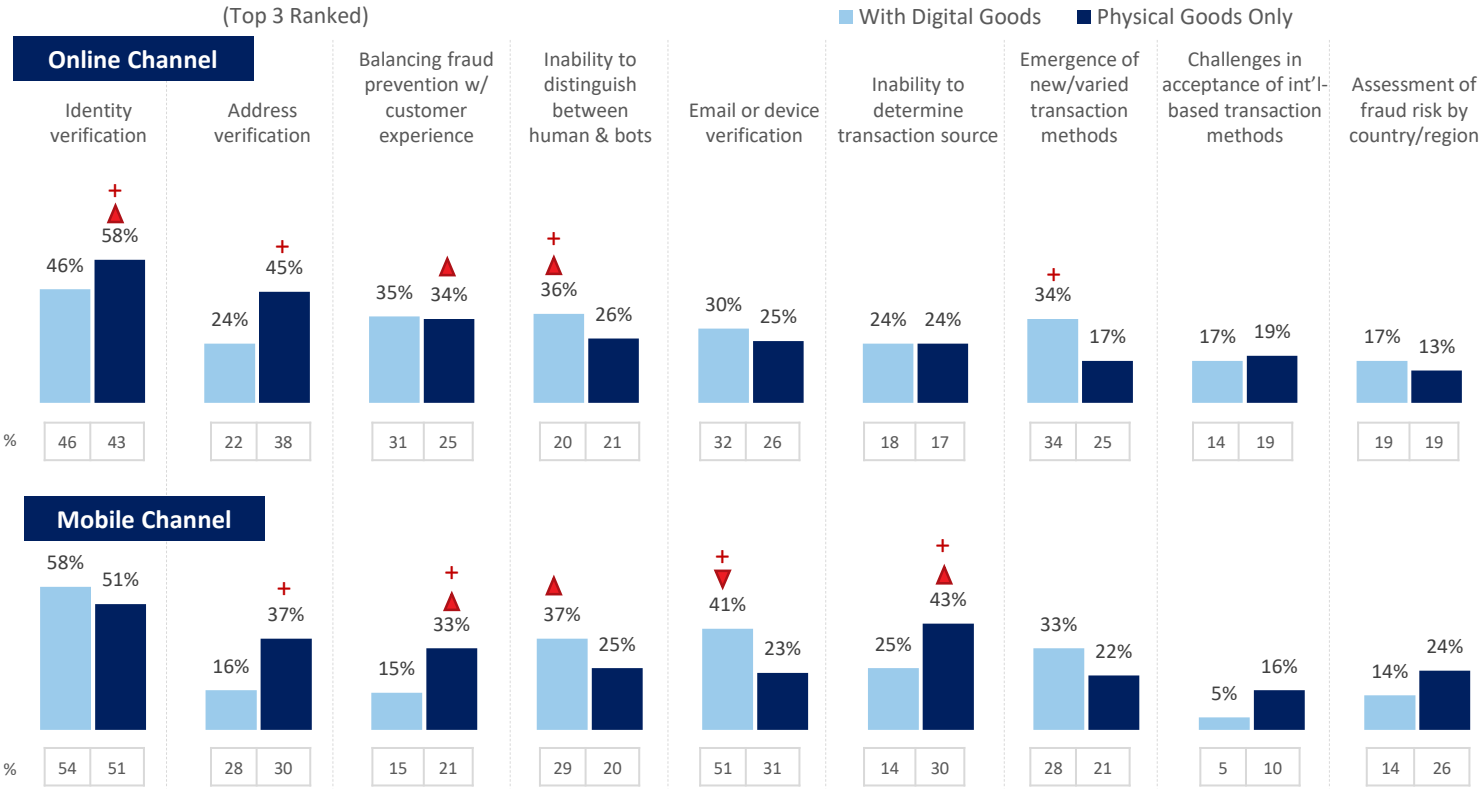
Identity verification remains a key online and mobile channel challenge for US E-commerce merchants, along with being able to balance fraud prevention and customer friction, while distinguishing legitimate from bot-related transactions.

E-commerce merchants that sell only physical goods are less likely to have implemented advanced identity authentication solutions, including those that can provide a holistic view of physical and online/mobile behavioral attributes of customers, while requiring minimal effort on their part. These types of solutions can help to also distinguish between legitimate customers and botnets.

Fraud Challenges by Transaction Channel

US E-commerce Merchants: Digital vs. Physical Goods

(Top 3 Ranked)



Survey Questions:
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online/mobile channel.

▲▼ = significantly higher or lower than 2019 + = significantly higher than the segment counterpart

LexisNexis® RISK SOLUTIONS

Survey Questions: Q19/Q20c/d: Please rank the top 3 factors that make customer identity a challenge when selling digital goods/servicing customers through the online/mobile channel.

Common reasons for identity verification challenges include the rise of synthetic identities, limited ability to confirm order location, and balancing transaction speed with fraud assessment and customer friction.

A number retailers and e-commerce merchants add the lack of real-time transaction tracking tools as a barrier, which becomes critical for digital goods transactions -- they are faster by nature, given no buffer period between the purchase and delivery (as with physical goods).

The need for real-time transaction tracking tools also underscores the importance of not just assessing individual identities, but also the risk of the transaction and prior purchaser behavioral patterns.

Top Identity Verification-Related Challenges

US Retail & E-commerce Merchants

	When Selling Digital Goods	When Serving Customers Though ONLINE Channel	When Serving Customers Though MOBILE Channel
Retail	58% Rise of synthetic identities 48% Limited/no real-time tracking tools 43% Limited ability to confirm order location	50% Balancing speed of approval w/ friction 47% Rise of synthetic identities 46% Limited ability to confirm order location	64% Rise of synthetic identities 52% Balancing speed of approval w/ friction 46% Limited/no real-time tracking tools 45% Limited ability to confirm order location
E-commerce	67% Rise of synthetic identities 43% Use of mobile channel for transactions 43% Limited/no real-time tracking tools	50% Balancing speed of approval w/ friction 50% Limited/no access to real-time 3rd party data 49% Limited ability to confirm order location 49% Rise of synthetic identities	67% Rise of synthetic identities 58% Balancing speed of approval w/ friction 44% Limited/no access to real-time 3rd party data

LexisNexis RISK SOLUTIONS

Identity verification and detecting malicious bots are key challenges for Canadian retailers with both the online and mobile channels. Significantly more Canadian retailers rank these as issues than do their US counterparts.

This impacts a number of merchants that sell digital goods through the mobile channel as they try to balance fraud assessment with minimizing customer friction.

Ability to determine the transaction origination source tends to be a challenge for Mid / Large as well.

Fraud Challenges by Transaction Channel

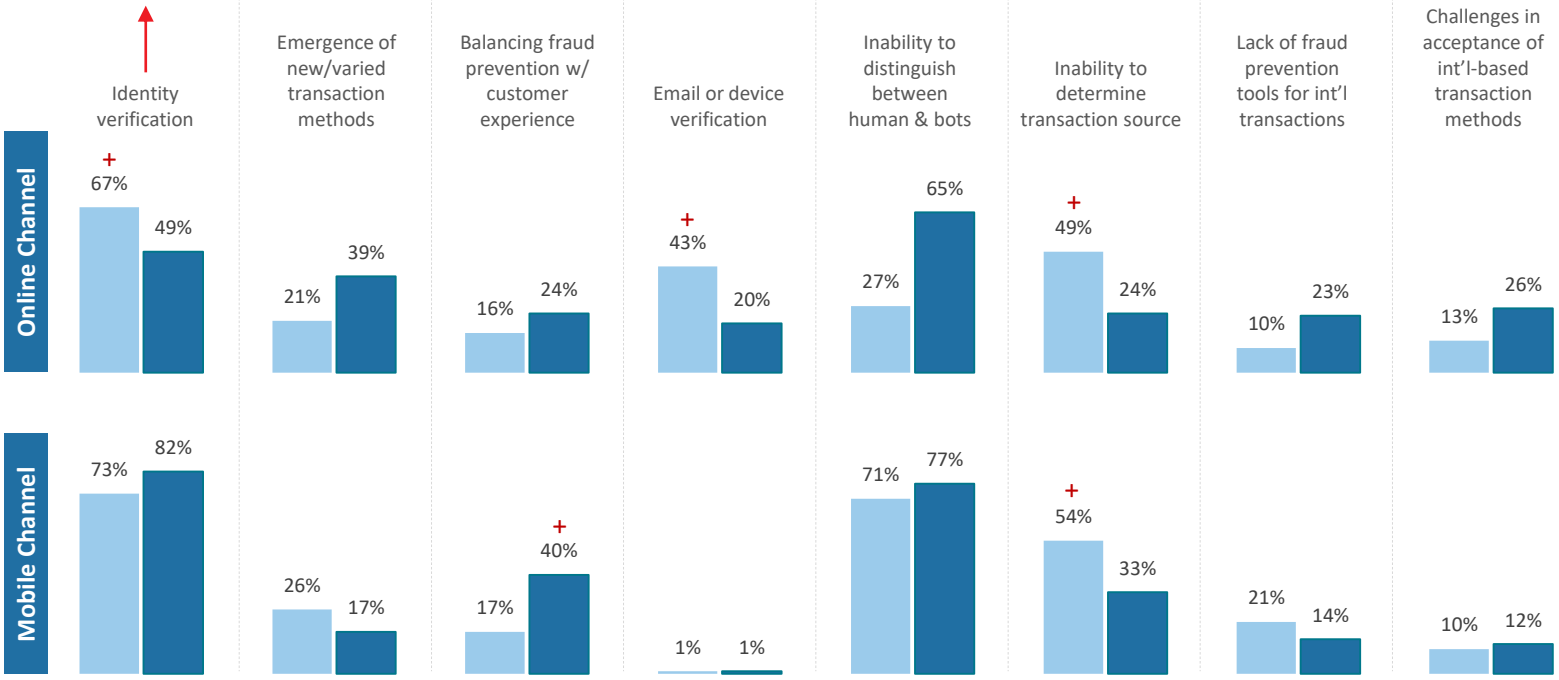
Canada Retail Merchants

(Top 3 Ranked)

Mid/Large w/ Digital Goods

Top ID Verification-Related Challenges

60% Rise of synthetic identities
50% Limited/no access to real-time 3rd party data
44% Balancing speed of approval w/ friction



Survey Questions:
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online/mobile channel.

+ = significantly higher than the segment counterpart

 |

LexisNexis® RISK SOLUTIONS

Survey Questions:
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online channel.

Identity verification is THE top online channel challenge for Canadian E-commerce merchants.

After that, merchants are fragmented across other top challenges, suggesting that there are many issues being faced by e-commerce organizations.

Fraud Challenges Through Online Channel

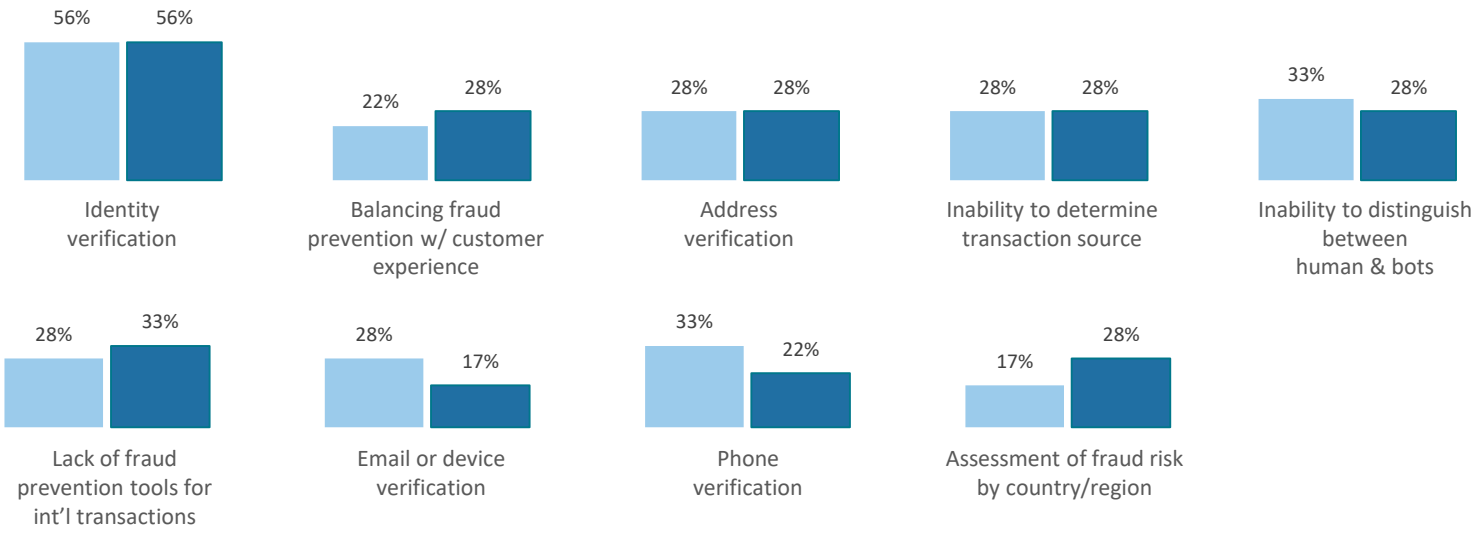
Canada E-commerce Merchants

(Top 3 Ranked)

Mid/Large w/ Digital Goods

Top ID Verification-Related Challenges

60% Rise of synthetic identities
50% Limited/no access to real-time 3rd party data
44% Balancing speed of approval w/ friction



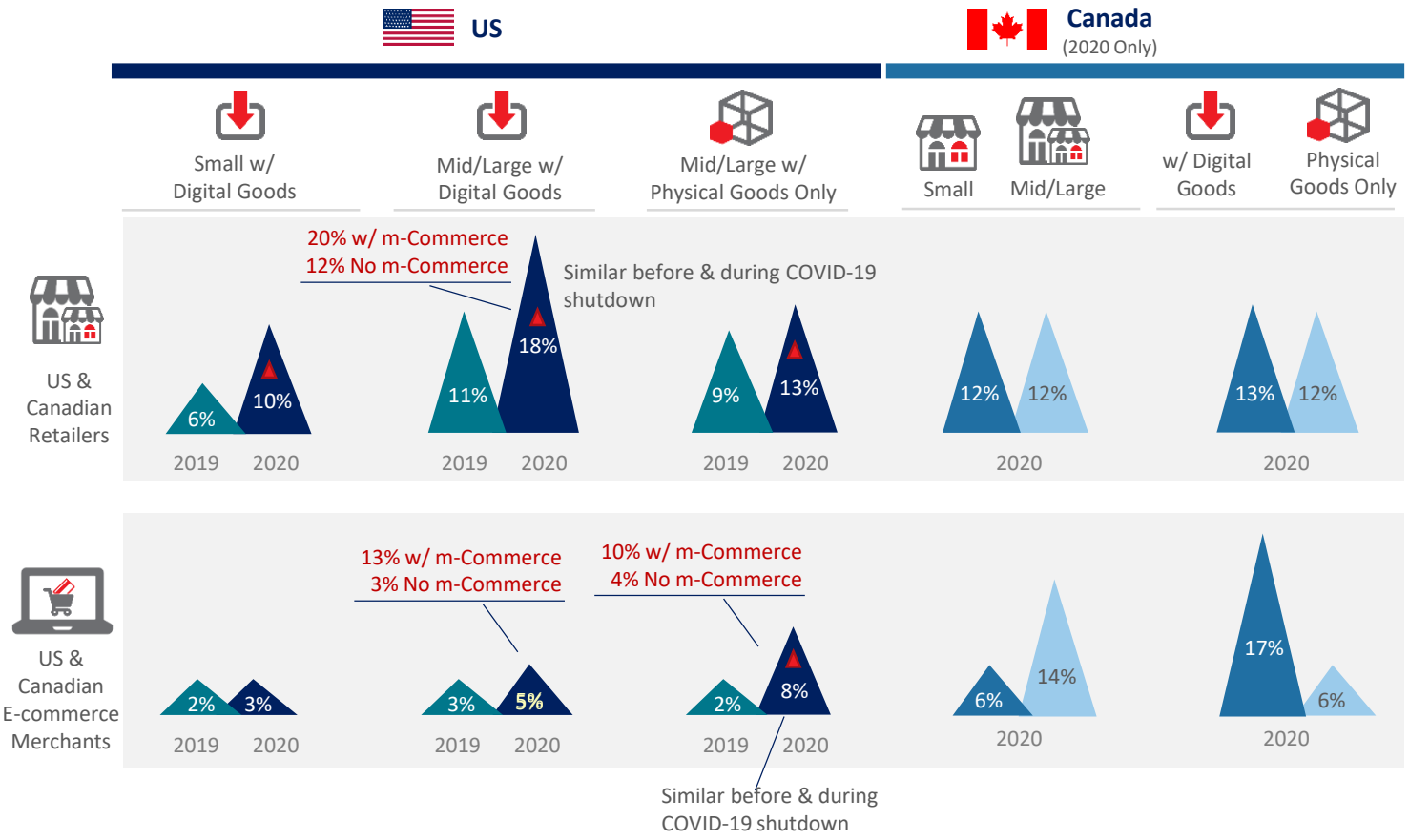
LexisNexis® RISK SOLUTIONS

While the ability to distinguish between legitimate customers and botnets remains a challenge, those able to detect them indicate a rise in the number of transactions involving them.

This is consistent with reported increased mobile botnet attacks in the LexisNexis® Risk Solutions Cybercrime Report.

Mid / Large US retailers that sell digital goods and use m-commerce report the highest average percentage of bot-related transactions, more so than their counterparts.

Average % of Transactions Determined as Malicious Bot Attacks — *Retail & E-commerce Merchants*



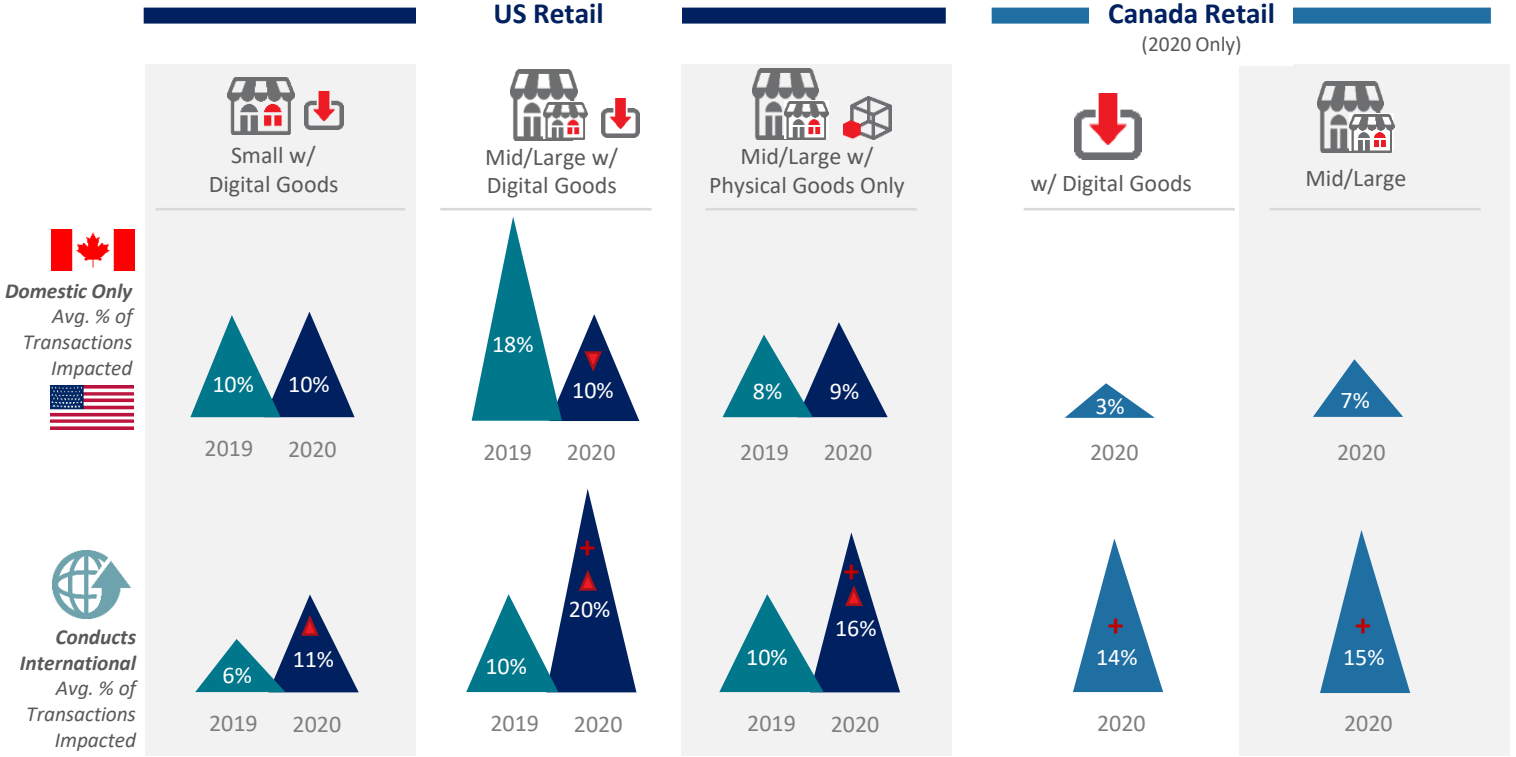
Survey Question:
Q25B1: In a typical month, what percent of your transactions are determined to be malicious automated bot attacks (i.e. rapid creation and placement of hundreds of orders / transactions by fraudulent automated Bots at the same time)?

▲▼ = significantly higher or lower than 2019

LexisNexis® RISK SOLUTIONS

Retailers with international transactions have experienced more botnet attacks, especially those which sell digital goods.

Estimated % of Botnet Activity — ***Retail Merchants w/ International Transactions***



Survey Question:
Q25B1: In a typical month, what percent of your transactions are determined to be malicious automated bot attacks (i.e. rapid creation and placement of hundreds of orders / transactions by fraudulent automated Bots at the same time)?

▲▼ = significantly higher or lower than 2019

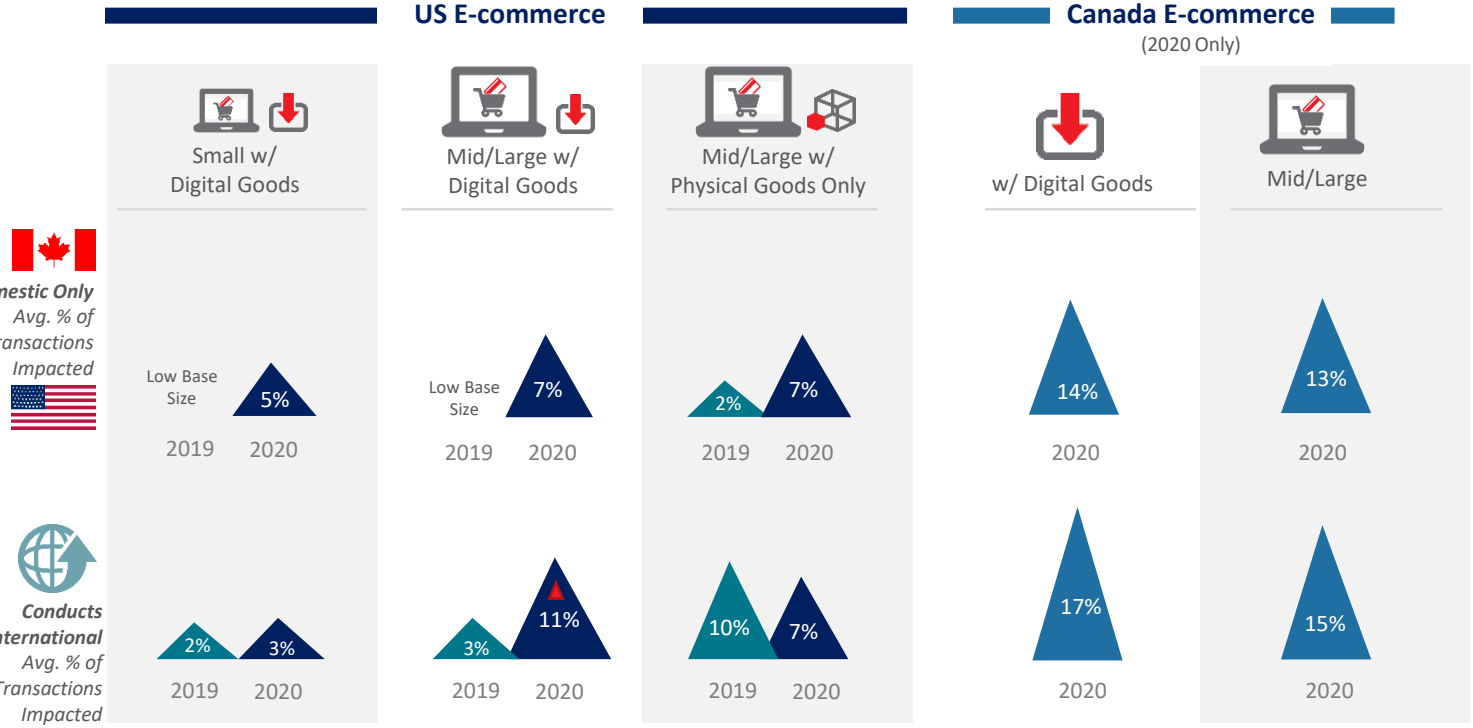
\+ = significantly higher than Domestic-Only

LexisNexis® RISK SOLUTIONS

US E-commerce merchants with international transactions also report higher levels of botnet activity than those without cross-border sales.

For Canadian e-commerce merchants, botnets represent a similar portion of transactions, regardless of their origination.

Estimated % of Botnet Activity — ***E-commerce Merchants w/International Transactions***



Survey Question:
Q25B1: In a typical month, what percent of your transactions are determined to be malicious automated bot attacks (i.e. rapid creation and placement of hundreds of orders / transactions by fraudulent automated Bots at the same time)?

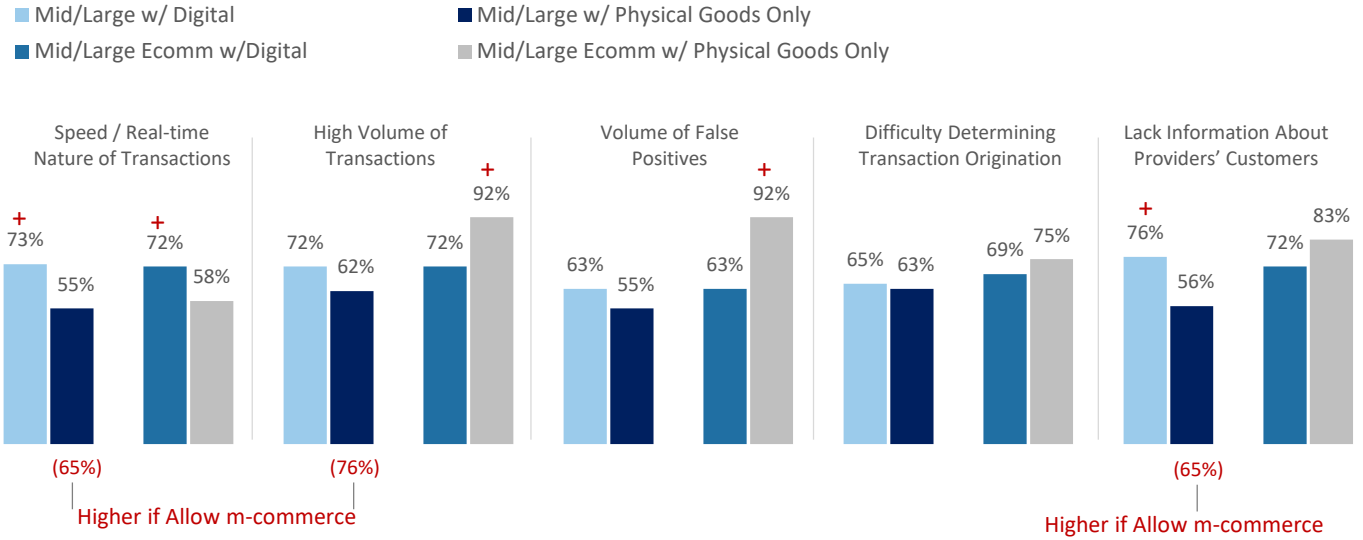
▲▼ = significantly higher or lower than 2019

Mid / Large US retailers and E-commerce merchants experience many challenges with non-bank payment provider (NBPP) transactions, involving speed / complexity, overwhelming volume, and lack of transparency.

Lack of transparency about providers' customers complicates matters when having to deal with increased transaction volumes and false positives, while needing to minimize customer friction. For digital goods sellers, the speed of the transaction adds an additional challenge.

Impact of Non-Bank / 3rd Party Payment Providers*

Retail & E-commerce Merchants



Survey Question:
Q42b: Over the past year, to what degree have the following been challenging to your fraud detection and prevention processes/operations when receiving transactions made through non-bank payment service providers and systems?

* Non-bank payment can involve a variety of different provider and systems types, such as Mobile and Internet Payment Systems (i.e. mobile wallets, peer-to-peer payments, and social media payments), payment services providers (i.e., PayPal, Stripe, Amazon Payments, Authorize.net, etc.) and FinTech companies. First asked in 2020.

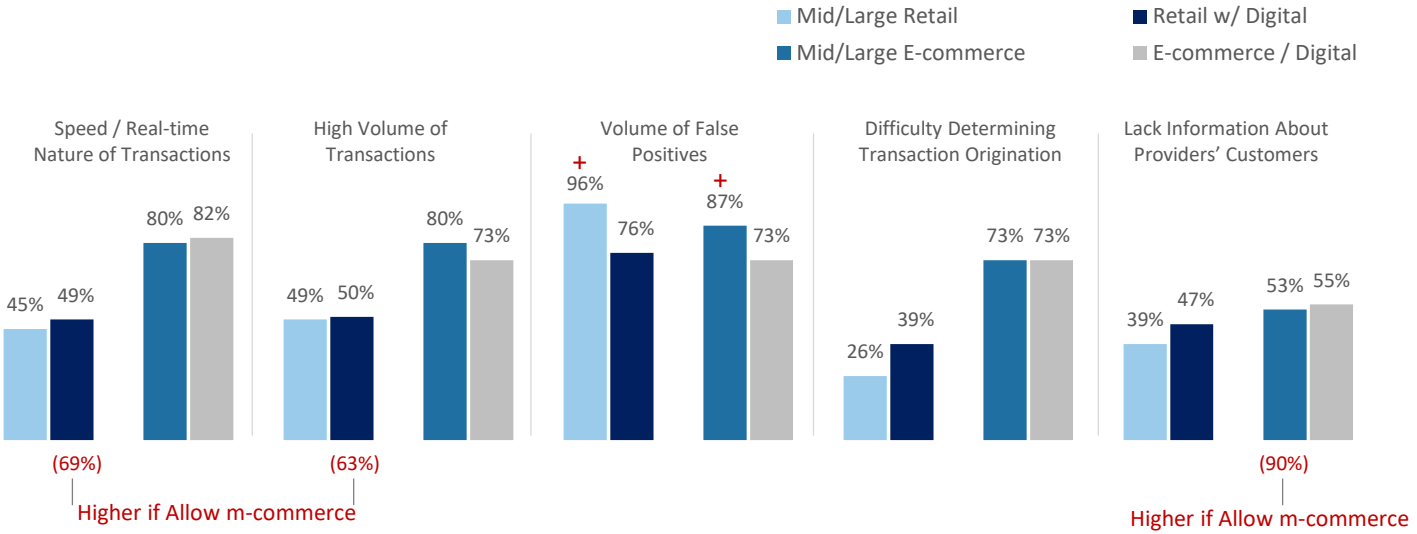
+ = significantly higher than the segment counterpart

Canadian E-commerce merchants experience significantly more non-bank payment provider challenges than retailers, with regard to transaction speed, volume, and determination of origin.

False positives are an issue across Canadian retailers and e-commerce merchants, but particularly larger ones. Where m-commerce is allowed, retailers can feel overwhelmed with the speed and volume of transactions that need to be monitored.

Impact of Non-Bank / 3rd Party Payment Providers*

Retail & E-commerce Merchants



Survey Question:
Q42b: Over the past year, to what degree have the following been challenging to your fraud detection and prevention processes/operations when receiving transactions made through non-bank payment service providers and systems?

* Non-bank payment can involve a variety of different provider and systems types, such as Mobile and Internet Payment Systems (i.e. mobile wallets, peer-to-peer payments, and social media payments), payment services providers (i.e., PayPal, Stripe, Amazon Payments, Authorize.net, etc.) and FinTech companies. First asked in 2020.

+ = significantly higher than the segment counterpart

Key Finding #4: The shuttering of a number of bricks & mortar retail stores and stay-at-home restrictions during the peak of the COVID-19 pandemic have had an impact on retail fraud.

- Analysis was conducted by comparing responses from those answering our survey *prior* to the shutdown period with those answering *during* the shutdown period.
- Comparison analysis showed that:
  - Average monthly fraud attack volumes are significantly higher among those answering during the shutdown.
  - Those allowing mobile channel transactions were particularly impacted during the shutdown.
    - While identity-fraud and fraudulent request for returns represent a sizeable portion of fraud losses, regardless of survey time period, the percent of losses attributed to friendly fraud and account takeover were higher during the shutdown.
    - There was a shift of fraud costs to the mobile channel.
    - Those selling digital goods were more likely to rank balancing fraud prevention and customer friction as a mobile channel challenge, as well as the need for real-time transaction scoring data, e-mail / device risk assessment, and the ability to determine origination source of a transaction.

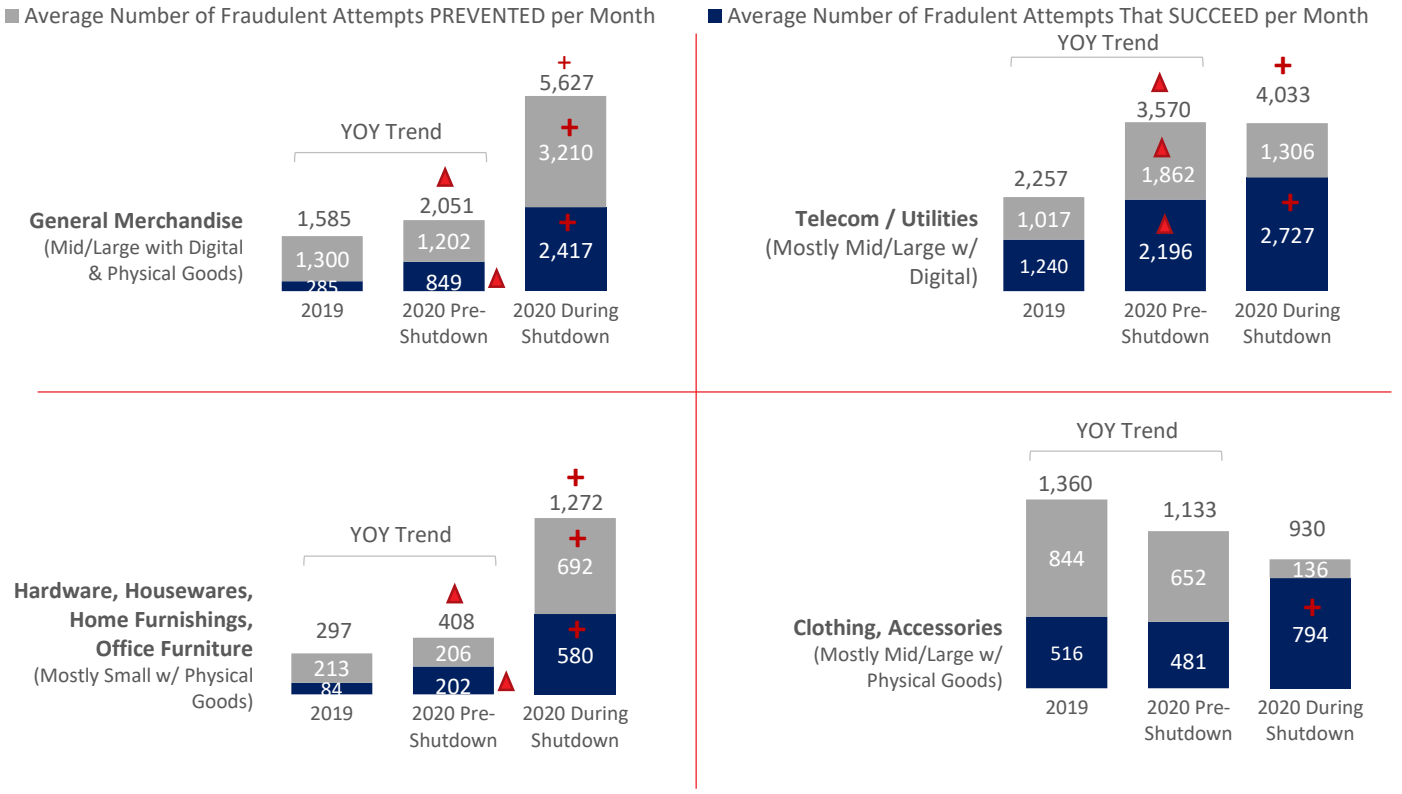
Survey Questions:
Q22: In a typical month, approximately how many fraudulent transactions are prevented by your company? Q24: In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

While trending upward year-over-year, select retail segments appear to have experienced a spike in fraud during the pandemic shutdown period.

Those answering the survey during the shutdown period indicated higher average monthly fraud volumes compared to those taking the survey prior to that timeframe. These sectors include the types of essential products and services in demand as people moved to remote working and PPE.

Average Monthly Fraud Attempts: Pre & During COVID-19 Shutdown

US Retail / Select Segments



▲▼ = significantly higher or lower than 2019

\+ = significantly higher than 2020 Pre-Shutdown

 |

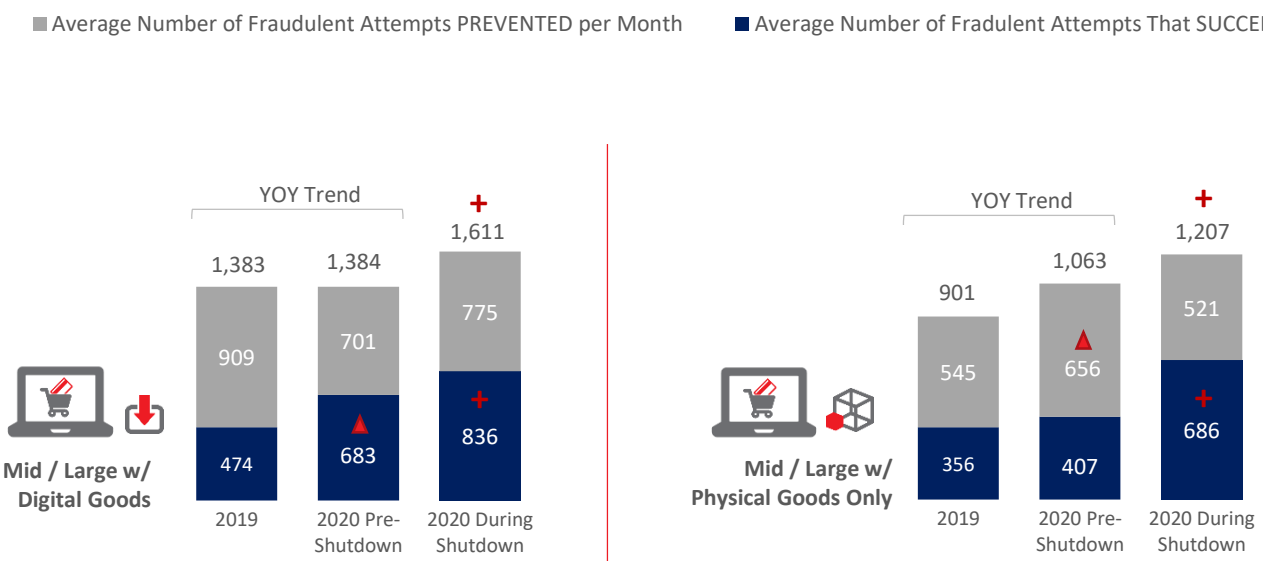
LexisNexis® RISK SOLUTIONS

Survey Questions:
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?

Mid / Large US E-commerce merchants appear to have experienced a spike in fraud during the shutdown period as well.

Those answering the survey during the shutdown period indicated higher average numbers of successful fraud attempts compared to those taking the survey prior to that timeframe.

Average Monthly Fraud Attempts: Pre & During COVID-19 Shutdown — US E-commerce



▲▼ = significantly higher or lower than 2019
+ = significantly higher than 2020 Pre-Shutdown

LexisNexis® RISK SOLUTIONS

Survey Questions:
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?

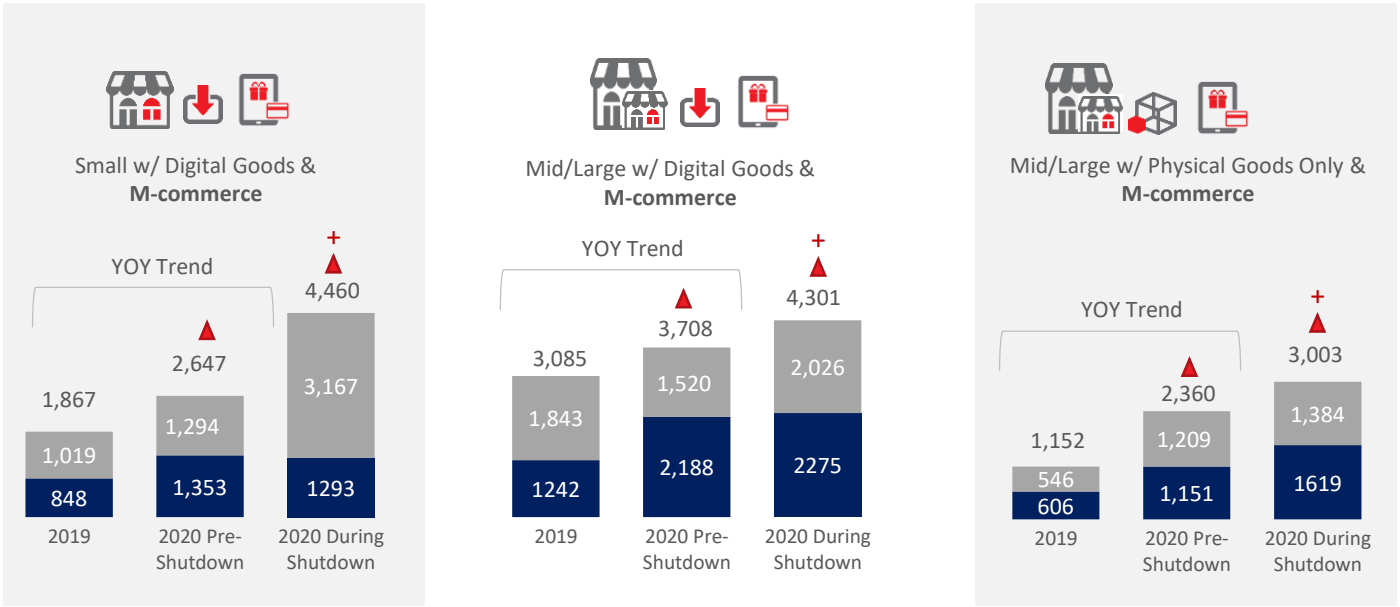
Those with M-commerce transactions appear to have been impacted during the COVID-19 shutdown period, with significantly higher average fraud volumes.

Respondents who completed the survey during the shutdown period reported much higher average monthly fraud volumes compared to those completing it prior to that period.

Average Monthly Fraud Attempts: Pre & During COVID-19 Shutdown

US Retail w/ M-commerce

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



▲▼ = significantly higher or lower than 2019
+ = significantly higher than the segment counterpart

LexisNexis® RISK SOLUTIONS

Survey Questions:
Q2b/c: Thinking of your online store/online transactions, what percent can be attributed to the following? Thinking of your mobile web browser/mobile app transactions, what percent can be attributed to the following?

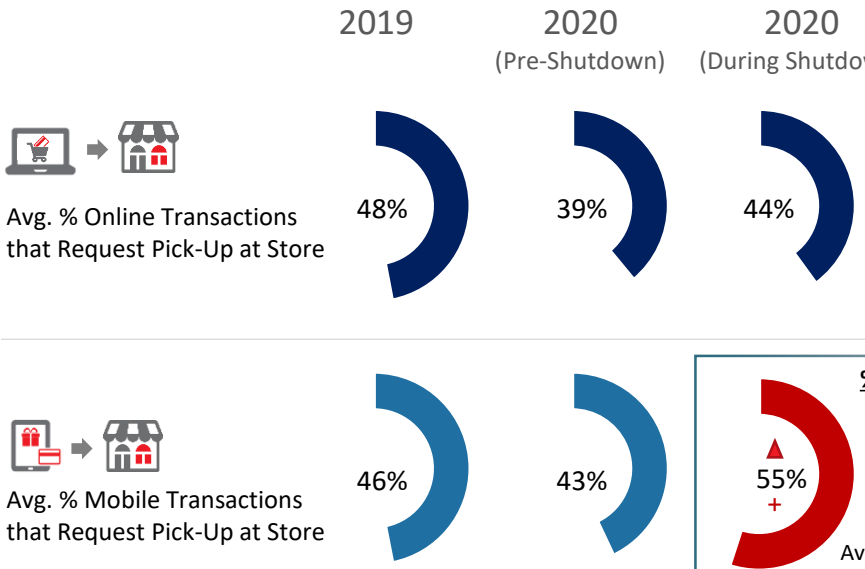
The average percent of mobile transactions involving pick-up at store increased significantly during the shutdown, leading to higher fraud attacks and costs.

Mid / Large US retailers that had more than average mobile purchase / in-store pick-up transactions experienced more fraud and higher fraud costs compared to others.

In-store pick-up carries an inherent risk of fraud where store employees are less trained regarding identity authentication. Given no significant changes with online purchasing / in-store pick-up, it suggests that fraudsters recognize the increased fraud opportunities with mobile and that a number of retailers have not fully invested in solutions designed to detect mobile channel fraud.

Mobile Purchase & Delivery Channels

US Mid/Large Retail w/ Online or Mobile Transactions – Physical Goods Only



% of Mobile Purchases with Store Pick-Up

	Less than Avg. (<43%)	More than Avg. (=>43%)
Avg. # Mo. Fraud Attacks	1,330	3,439 +
Avg. # Mo. ***Successful*** Fraud Attacks (% of Total Attacks)	305 (23%)	2,219 + (65%)
Every $1 of fraud costs	$2.89	$3.17 +

▲▼ = significantly higher or lower than 2019

+ = significantly higher than the segment counterpart

 |

LexisNexis® RISK SOLUTIONS

Survey Question:
Q12: Please indicate the percentage distribution of the following fraud methods, as they are attributed to your total annual fraud loss over the past 12 months. Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?

Among the select industries noted earlier, identity and fraudulent returns contribute most to losses. But differences emerge depending on the use of M-commerce.

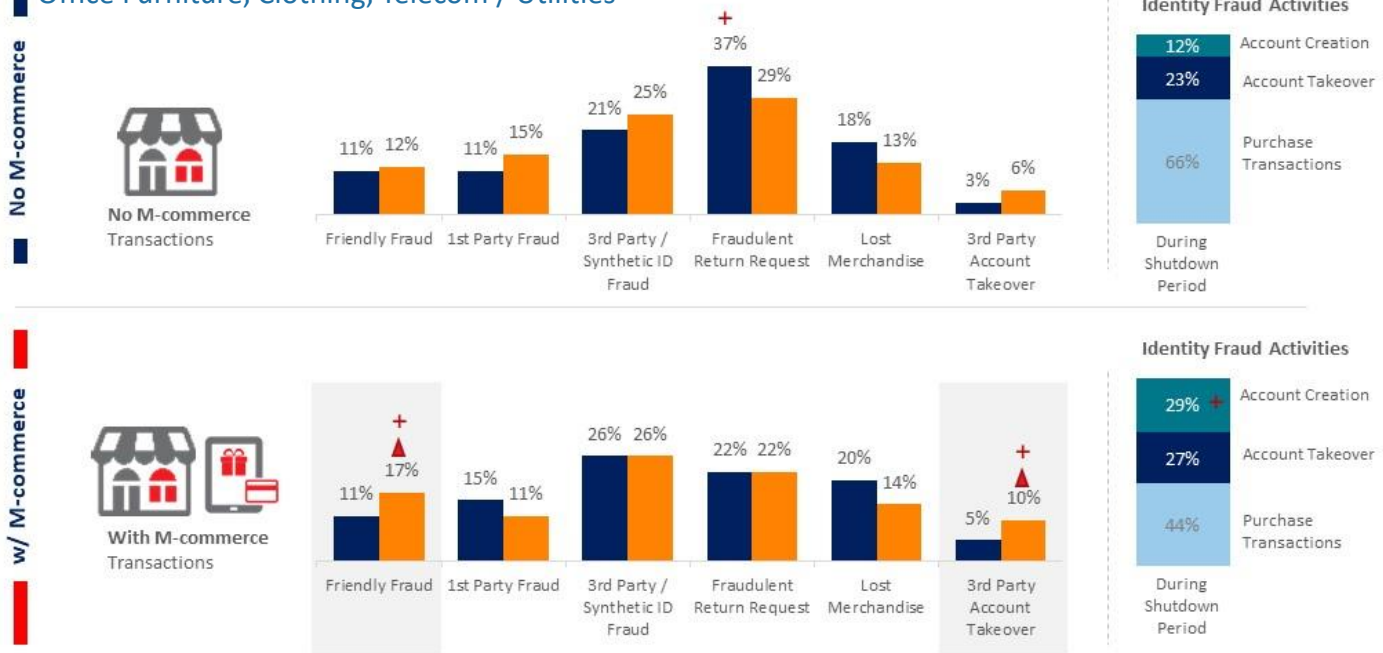
Those with m-commerce were more likely to report friendly fraud and account takeover during the shutdown and compared to those not conducting m-commerce. They were also more likely to report new account creation as an identity fraud activity.

Average Monthly Fraud Attempts: Pre & During COVID-19 Shutdown

US Retail / Select Segments

Pre-Shutdown Period
During Shutdown Period

General Merchandise, Hardware / Home Furnishings / Office Furniture, Clothing, Telecom / Utilities



▲▼ = significantly higher than Pre-Shutdown Period
\+ = significantly higher than the segment counterpart

LexisNexis RISK SOLUTIONS

Survey Question:
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the mobile channel. Q20d: Please rank the top 3 factors that make customer identity verification a challenge when serving customers through the mobile channel.

Select Mid / Large retailers using the mobile channel ranked identity verification as their top challenge. Those answering during the shutdown were more likely to add digital device and international risk assessment.

Digital goods sellers appear to have been further impacted via m-commerce during the shutdown period.

- Lack of real-time transaction risk assessment is a key factor for identity verification challenges among those answering during the shutdown.
- If selling digital goods, determining transaction origination source, while dealing with increasing botnet volume, has added to these challenges.

Top Mobile & Digital Challenges: Pre & During COVID-19 Shutdown — *US Retail / Select Segments*

General Merchandise, Hardware / Home Furnishings / Office Furniture, Clothing, Telecom / Utilities

Mid / Large w/ M-commerce

Top Factors Making Identity Verification a Challenge via the Mobile Channel

- Rise of Synthetic Identities (76%)
- Balancing Speed with Risk Assessment (77%)

Those Answering Before Shutdown		Those Answering During Shutdown
47%	Verifying Customer Identities	45%
47%	Balancing Fraud Assessment with Customer Friction	21% 63% digital goods sellers
35%	Distinguishing Legitimate Humans from Malicious Bots	25% 56% digital goods sellers
19%	Lack Specialized Tools to Assess International Risk	39% ▲
15%	E-mail / Device Risk Assessment	34% ▲

Red font = highest ranked

Top Factors Making Identity Verification a Challenge via the Mobile Channel

- Limited or No Real-time Transaction Tracking Tools (i.e., velocity checking) (76%)
- (Among Digital Sellers) Limited Ability to Determine Transaction Origination (57%)
- (Among Digital Sellers) Volume of Malicious Bot Attacks (56%)

▲▼ = significantly higher than Pre-Shutdown Period

LexisNexis RISK SOLUTIONS

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

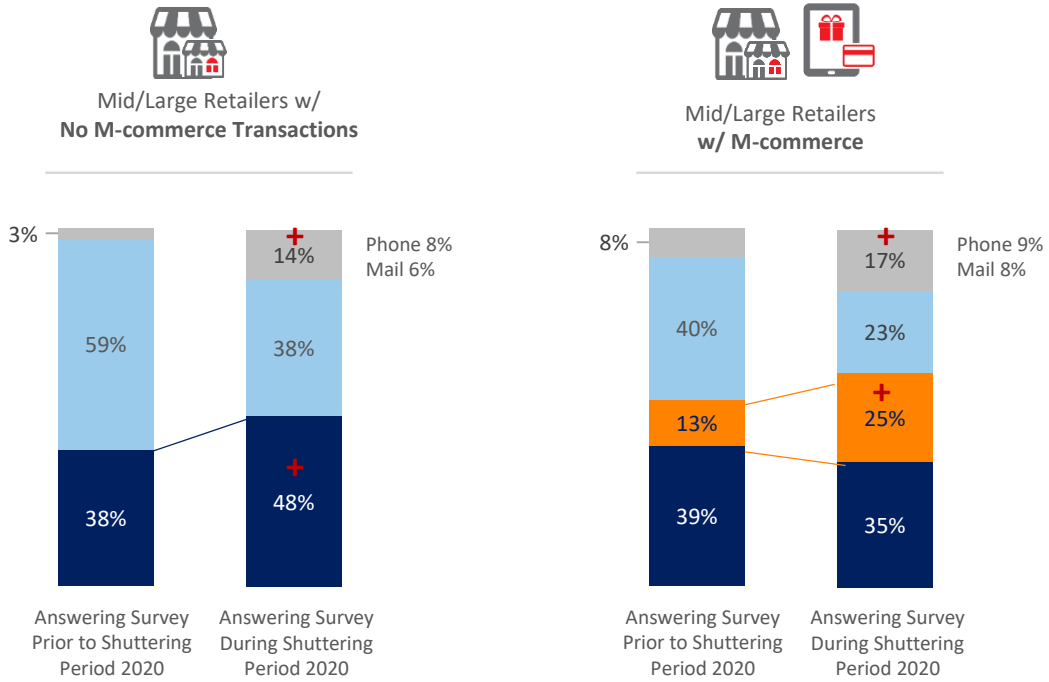
Not surprisingly, fraud costs shifted to online channels during the period when many physical locations were shuttered. For those allowing M-commerce, fraud costs shifted from in-person and online to the mobile channel.

As a result, the mobile channel accounts for one-quarter of fraud costs among those answering the survey during the shuttering period, while fraud costs attributed to the online channel remained a fairly constant, yet still a sizeable, portion.

% Fraud Costs by Channel: Pre & During COVID-19 Shutdown

US Retail Merchants

Online
In-Person
Mobile
Other (Phone, Mail, Kiosk)



+ = significantly higher than 2020 Pre-Shutdown

Key Finding #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 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 e-commerce merchants still appear to be using a limited set of solutions to cover all channel and transaction risks. Those newer to m-commerce are more at risk; they tend to have embraced this channel without investing in solutions to meet specific mobile threats.

There is a directional increase in the adoption of digital identity-based solutions among Mid / Large US retailers that sell digital goods. That said, there is still limited use by other segments that are fraud targets.

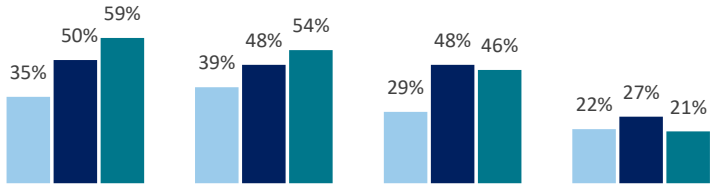
The complexity of synthetic identity fraud and botnet attacks requires more sophisticated solutions to assess the whole person from a digital behavior and physical identity perspective. The limited use of these explains the challenges highlighted earlier with identity verification, botnet attacks, and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

Fraud Mitigation Solutions Usage

US Retail Merchants

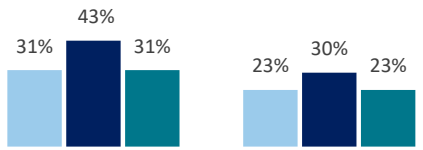
Small w/ Digital Goods | M/L w/ Digital Goods | M/L w/ Physical Goods Only

Basic Verification & Transaction



2019 %			
Check Verification	30	46	48
Authenticate Using Payment Instrument	33	55	69
Name Address DOB Verification	26	46	37
Positive & Negative Lists	19	41	19

Advanced ID & Transaction Verification

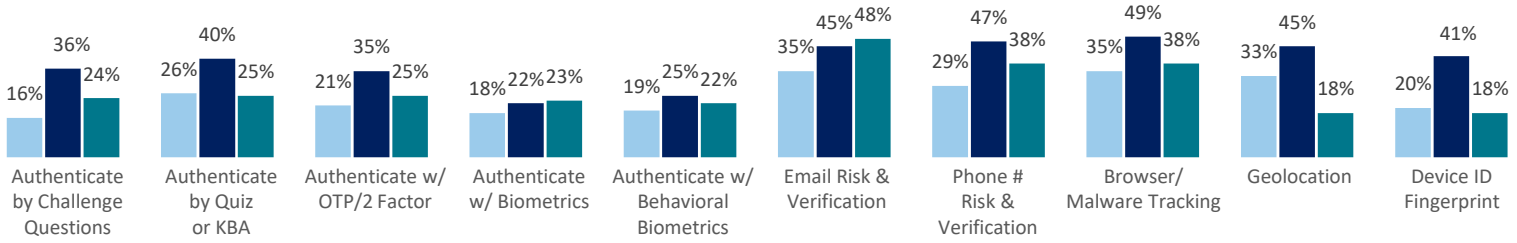


2019 %			
Real-Time Transaction Scoring	21	41	26
Automated Transaction Scoring	19	41	15

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

Advanced ID Authentication

Active/Interactive | *Passive/Digital Identity-based*



2019 %			
Authenticate by Challenge Questions	27	42	17
Authenticate by Quiz or KBA	19	39	13
Authenticate w/ OTP/2 Factor	21	38	14
Authenticate w/ Biometrics	31	33	21
Authenticate w/ Behavioral Biometrics	n/a		
Email Risk & Verification	38	38	34
Phone # Risk & Verification	30	37	28
Browser/ Malware Tracking	42	46	24
Geolocation	19	38	15
Device ID Fingerprint	22	30	11

 |

LexisNexis® RISK SOLUTIONS

Solutions usage is limited among Canadian retailers, even among those who sell digital goods, and despite the various challenges they face around identity verification.

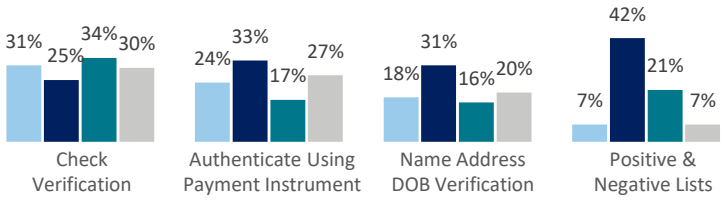
Use of passive / digital identity-based solutions is limited. These are designed to provide a fuller view of both the physical and digital attributes of a person, quickly and seamlessly, in order to effectively assess fraud while minimizing friction.

Fraud Mitigation Solutions Usage

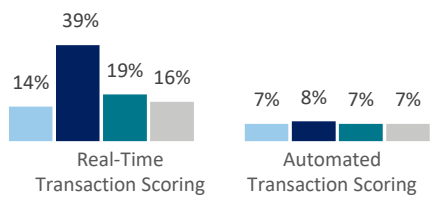
Canada Retail Merchants

Small | Mid/Large | w/ Digital Goods | w/ Physical Goods Only

Basic Verification & Transaction



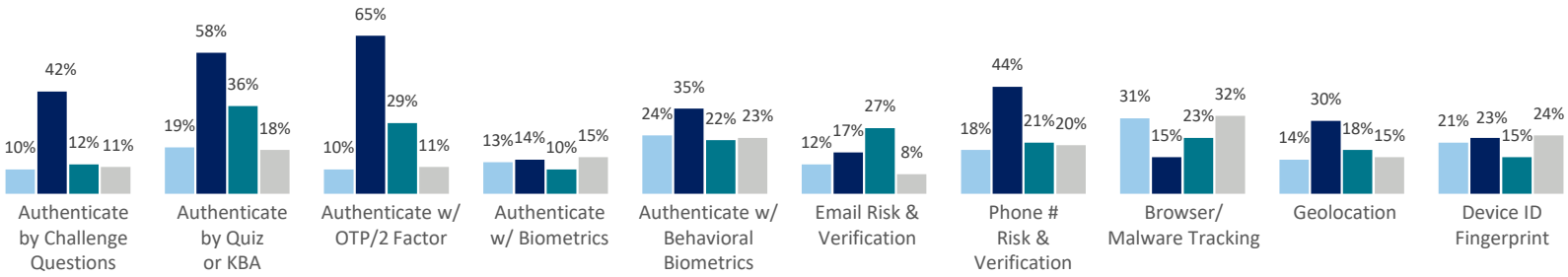
Advanced ID & Transaction Verification



Active/Interactive | *Passive/Digital Identity-based*

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

Advanced ID Authentication



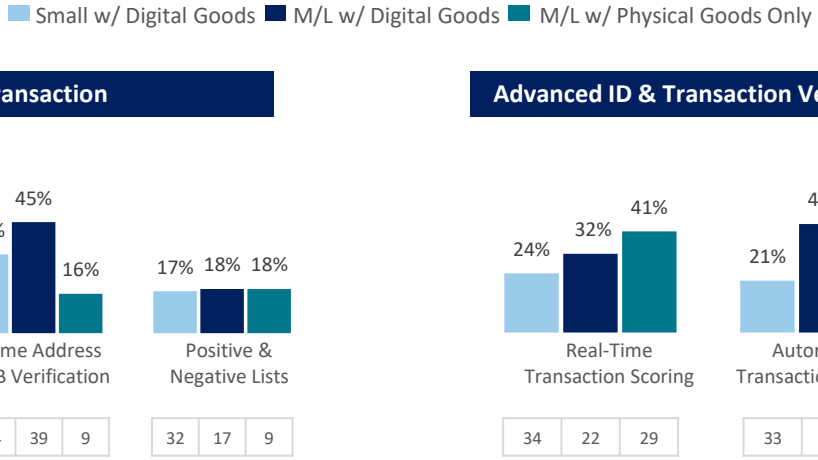
LexisNexis® RISK SOLUTIONS

A number of Mid / Large digital goods E-commerce merchants have invested in advanced identity authentication solutions, particularly passive / digital identity ones that improve fraud assessment while minimizing friction.

These solutions also support mobile channel fraud assessment. Use of these are more limited among Mid / Large e-commerce that sell only physical goods, which have come to experience more fraud challenges and issues – particularly as this segment has integrated m-commerce into its channel strategy.

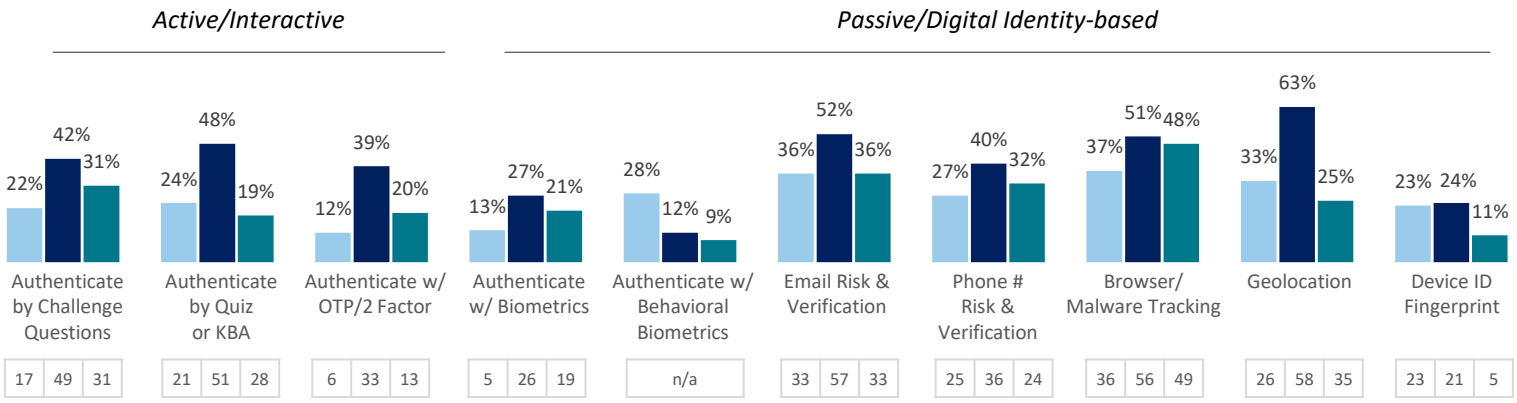
Fraud Mitigation Solutions Usage

US E-commerce Merchants



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

Advanced ID Authentication



LexisNexis® RISK SOLUTIONS

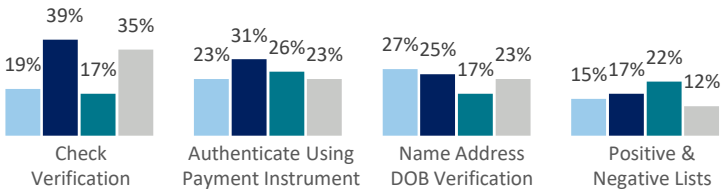
Solutions usage is also limited among Canadian E-commerce merchants, even as they face the impact of synthetic identities on verification efforts.

Fraud Mitigation Solutions Usage

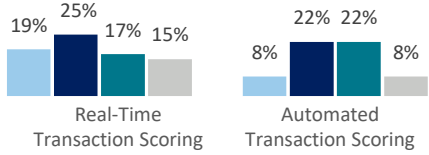
Canada E-commerce Merchants

Small | Mid/Large | w/ Digital Goods | w/ Physical Goods Only

Basic Verification & Transaction



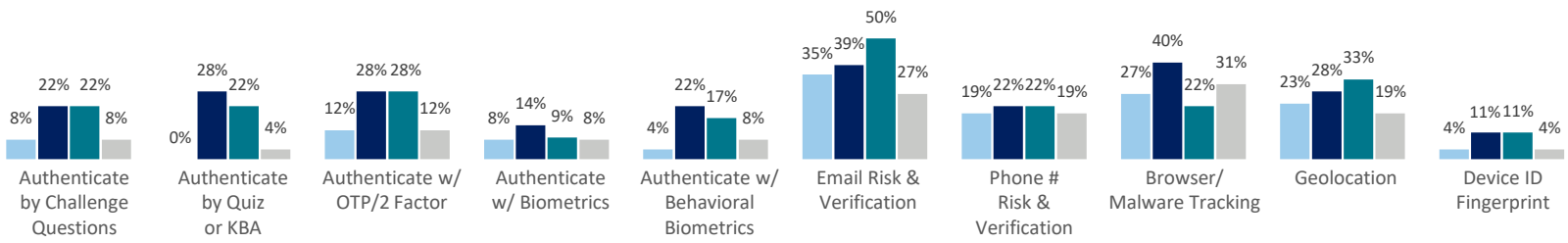
Advanced ID & Transaction Verification



Active/Interactive | *Passive/Digital Identity-based*

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

Advanced ID Authentication



LexisNexis® RISK SOLUTIONS

Survey Questions:
Q28a: Are your fraud solutions:

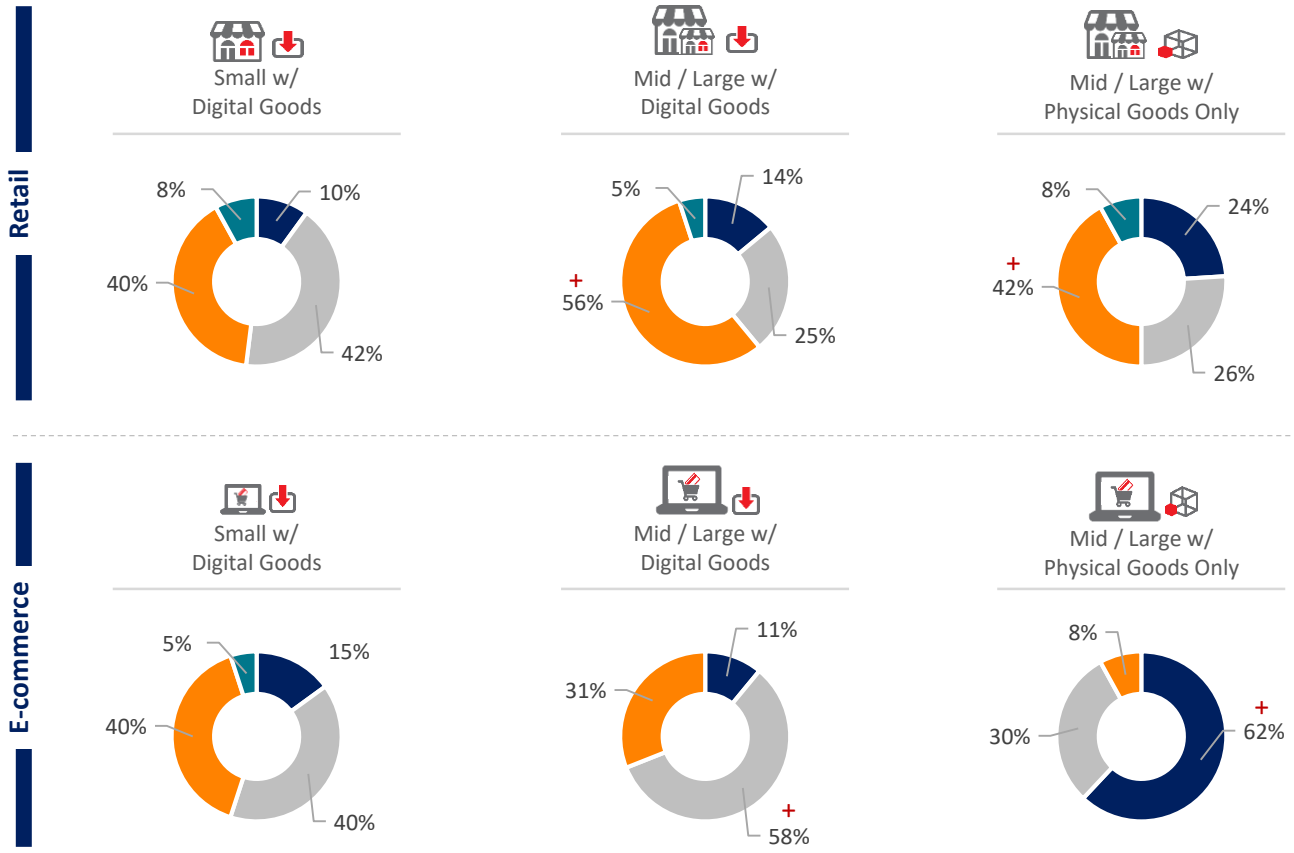
Cloud-based fraud mitigation solutions are prevalent among US retailers and E-commerce merchants, even among those that also use premise-based ones.

This differs among Mid / Large e-commerce merchants that sell only physical goods; they are more likely to use premise-based solutions.

Premise vs. Cloud-based Solutions

US Retail & E-commerce Merchants

Premise-based | Cloud-based | Mix of both | Not sure



+ = significantly higher than the segment counterpart

LexisNexis® RISK SOLUTIONS

Survey Questions:
Q28a: Are your fraud solutions:

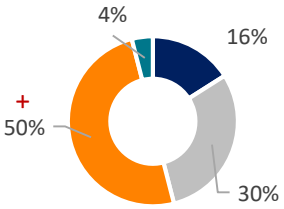
Cloud-based fraud mitigation solutions are also prevalent among Canadian retailers and E-commerce merchants.

Premise vs. Cloud-based Solutions

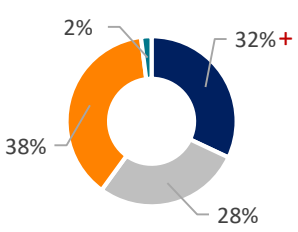
Canada Retail & E-commerce Merchants

Retail

Mid / Large

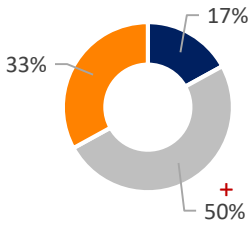


w/ Digital Goods

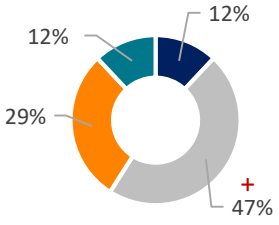


E-commerce

Mid / Large



w/ Digital Goods



+ = significantly higher than the segment counterpart

LexisNexis® RISK SOLUTIONS

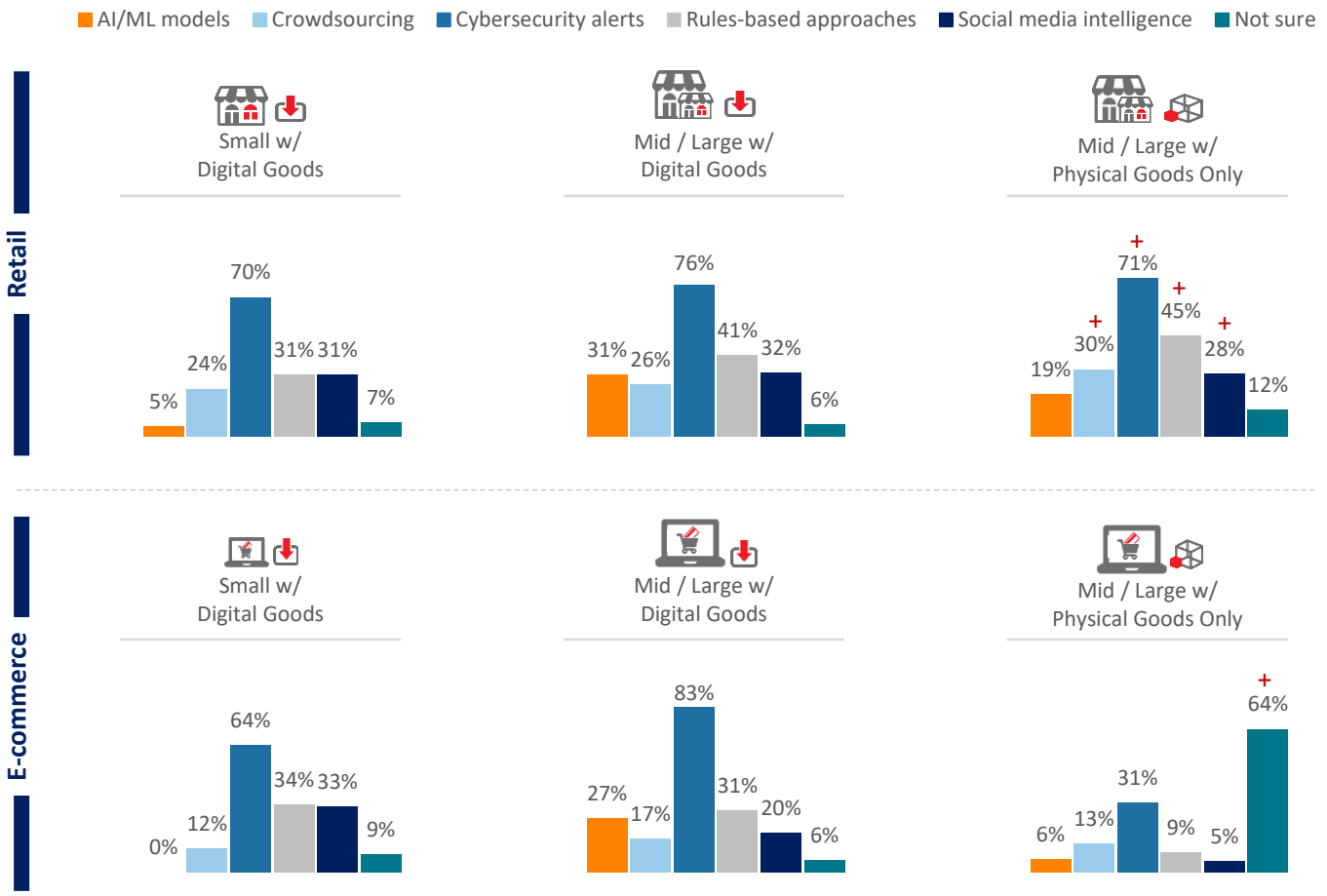
Survey Questions:
Q28b: In addition to solutions, what supportive capabilities is your company using to help fight fraud?

In addition to risk mitigation solutions, a significant majority of US retailers and digital goods E-commerce merchants also rely on cybersecurity alerts.

Crowdsourcing and AI/Machine learning supportive capabilities are being used in some Mid / Large organizations as well.

Supportive Capabilities Usage

US Retail & E-commerce Merchants



+ = significantly higher than the segment counterpart

 |

LexisNexis® RISK SOLUTIONS

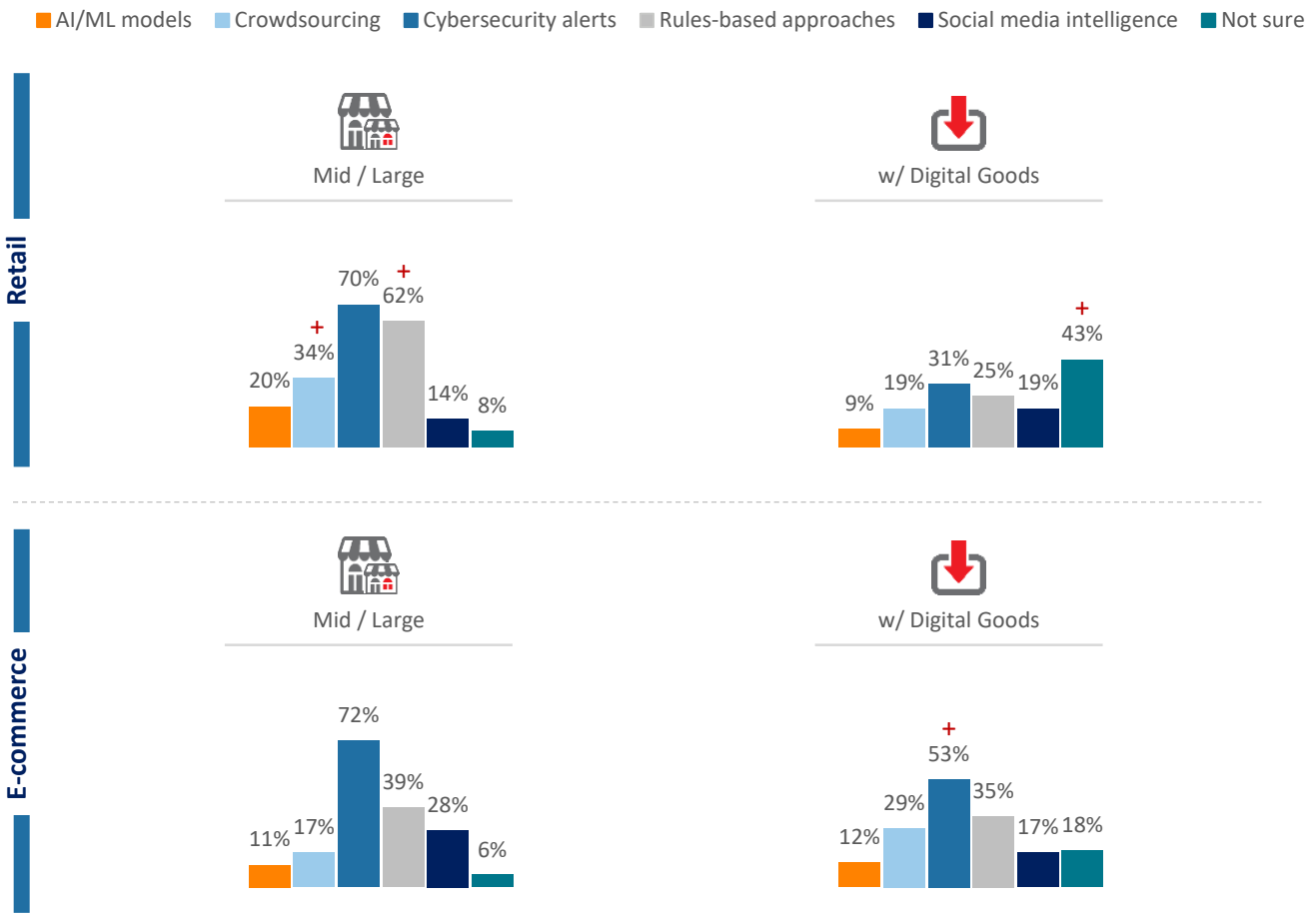
Survey Questions:
Q28b: In addition to solutions, what supportive capabilities is your company using to help fight fraud?

Cybersecurity alerts are prevalent among Mid / Large Canadian retailers and E-commerce merchants, with many Mid / Larger retailers still using rules-based approaches.

Use of AI/Machine learning is still limited in this market.

Supportive Capabilities Usage

Canada Retail & E-commerce Merchants



+ = significantly higher than the segment counterpart

LexisNexis® RISK SOLUTIONS

Key Finding #6: Study findings show that those who use a layered solutions approach, as well as one that integrates cybersecurity, the digital customer experience, and fraud prevention efforts, experience fewer comparable fraud attacks, are better able to detect botnets and minimize customer friction, and realize a lower cost of fraud.

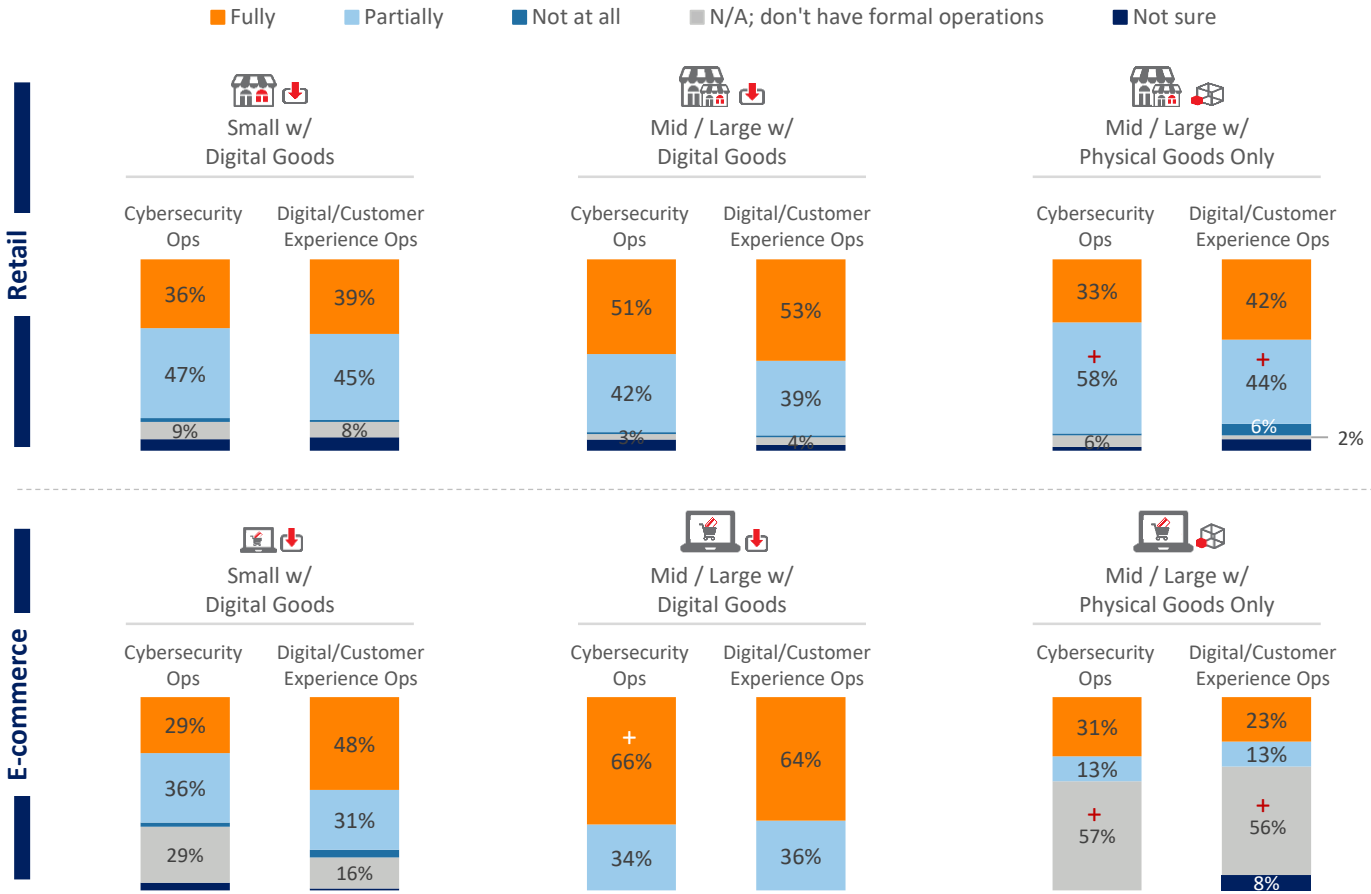
- There is movement among a number of retail and e-commerce merchants toward such integration. Those who are fully integrated experience the above benefits compared to those who are only partially integrated.
- US retailers and e-commerce merchants are somewhat further ahead with integrating both cybersecurity and the digital customer experience with fraud prevention compared to Canadian merchants.
- That said, many Canadian retailers and e-commerce merchants recognize the benefit of achieving full integration.

There is movement among US retailers and E-commerce merchants toward integrating fraud prevention efforts with cybersecurity operations and the digital / customer experience.

Mid / Large merchants that sell digital goods are further along, with over half of organizations saying that they have fully integrated these efforts. Mid / Large e-commerce selling only physical goods lag behind.

Integration of Cybersecurity & Digital/Customer Experience* Operations w/ Fraud Prevention

US Retail & E-commerce Merchants



Survey Questions:
Q29: To what degree has your company integrated its cybersecurity operations with its fraud prevention efforts? Q30b: To what degree has your company integrated its digital/customer experience operations with its fraud prevention efforts?

*asked of those with online and/ or mobile channel translations

+ = significantly higher than the segment counterpart

 |

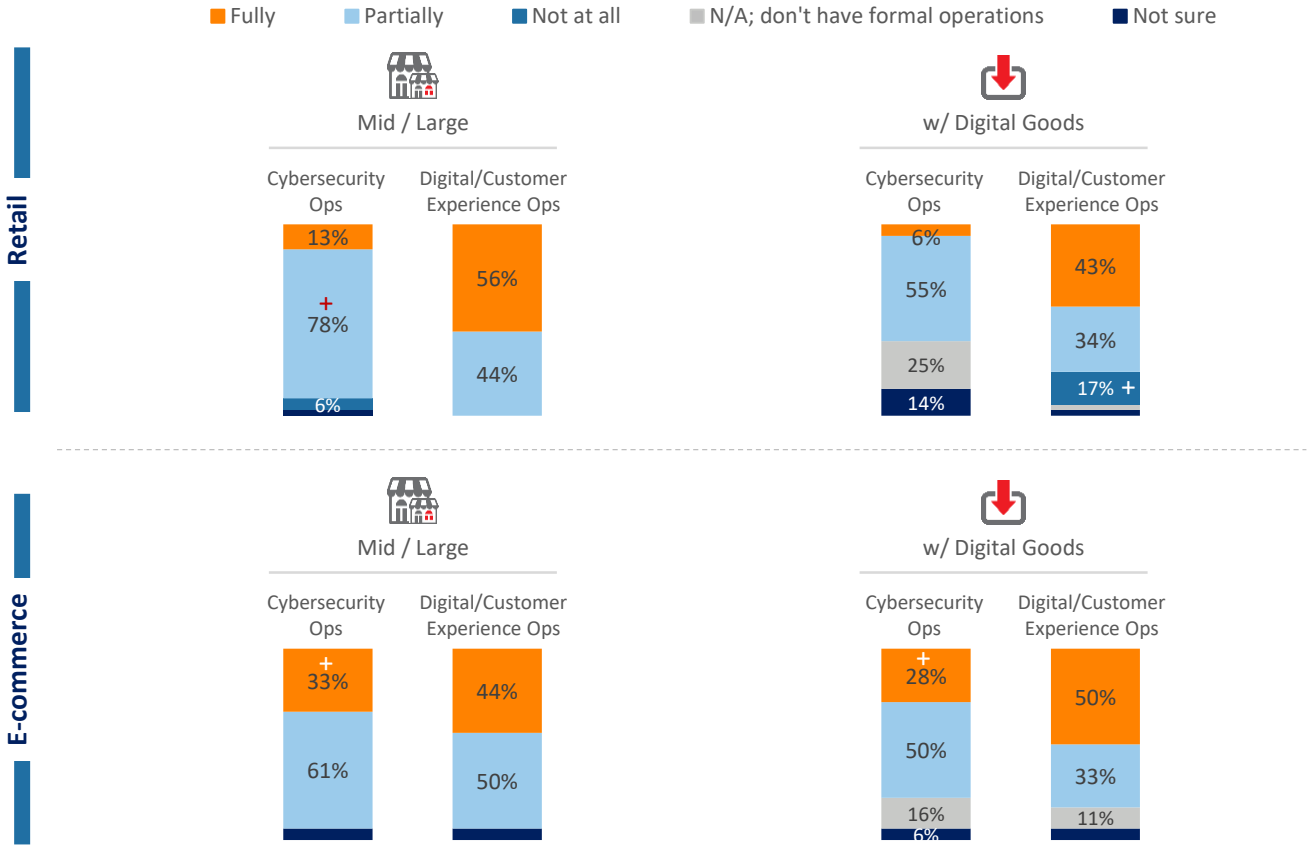
LexisNexis® RISK SOLUTIONS

Larger Canadian retailers that sell digital goods are further along with the integration of fraud prevention and the digital / customer experience than they are with cybersecurity.

Even a majority of Canadian e-commerce merchants are still only partially integrated with fraud and cybersecurity efforts.

Integration of Cybersecurity & Digital/Customer Experience* Operations w/ Fraud Prevention

Canada Retail & E-commerce Merchants



Survey Questions:
Q29: To what degree has your company integrated its cybersecurity operations with its fraud prevention efforts? Q30b: To what degree has your company integrated its digital/customer experience operations with its fraud prevention efforts?

*asked of those with online and/ or mobile channel translations

+ = significantly higher than the segment counterpart

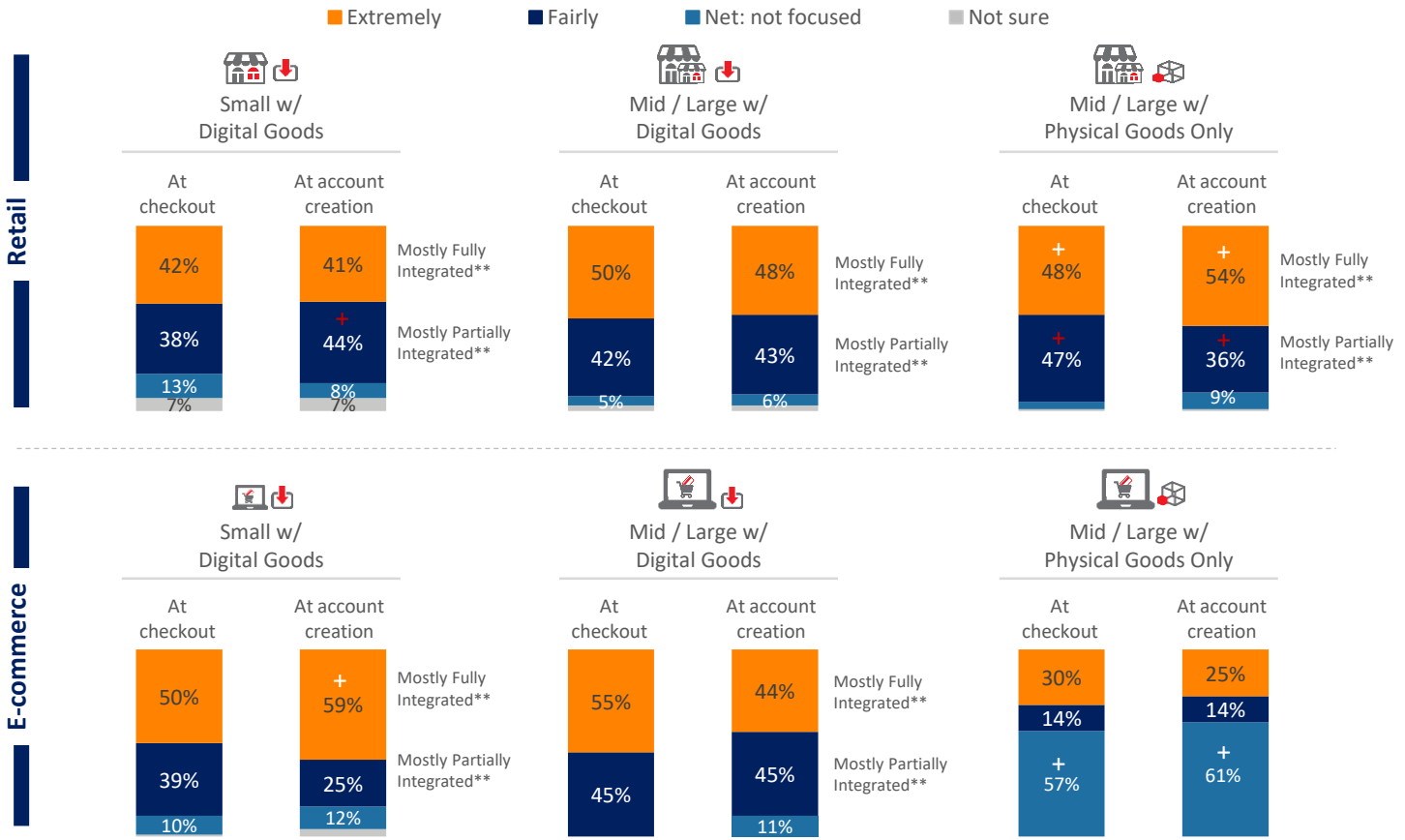
LexisNexis® RISK SOLUTIONS

Not surprisingly, there is a relationship between the degree of current integration efforts and strategic focus, with similar levels of attention given to both the checkout and account creation parts of the customer journey.

Those who are extremely focused on minimizing customer friction in remote channels tend to have fully integrated fraud prevention and digital CX efforts. Those who are fairly, but not fully-focused, are partially integrated.

Degree Company is Focused on Minimizing Customer Friction Through Online/Mobile Channels*

US Retail & E-commerce Merchants



Survey Questions:
Q30: To what degree is your company focused on minimizing customer friction during an online/mobile transaction checkout? Q30a: To what degree is your company focused on minimizing customer friction during online/mobile account opening?

*asked of those with online and/ or mobile channel translations

** Integration of digital / customer experience with fraud prevention

+ = significantly higher than the segment counterpart

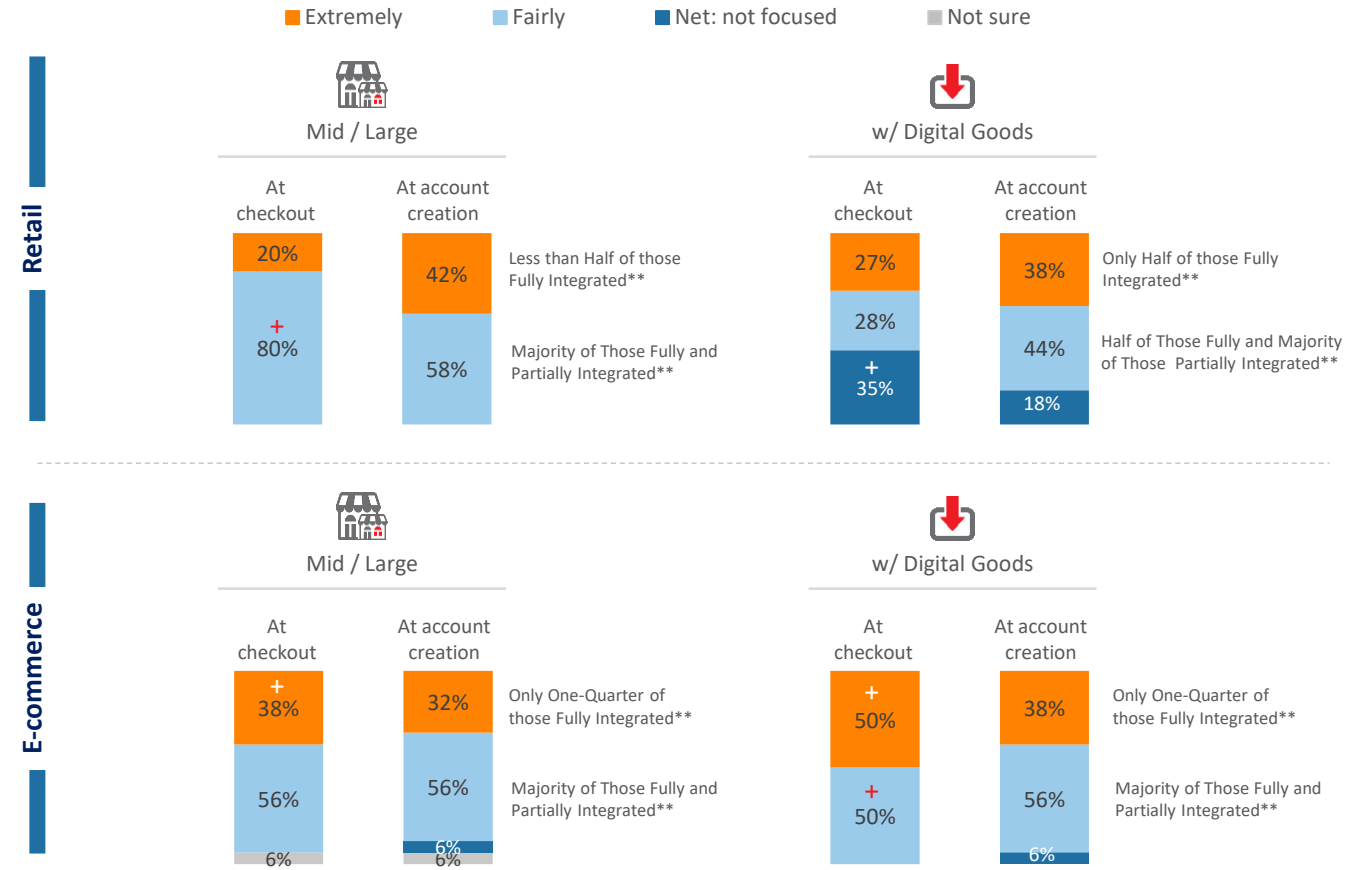
LexisNexis® RISK SOLUTIONS

Canadian retailers and E-commerce merchants more often indicate being fairly focused on minimizing the customer experience in relation to integrating fraud prevention with the digital / customer experience.

Even those indicating full integration more often report being less than fully-focused on minimizing friction. This suggests that they are juggling multiple priorities, rather than less importance being attached to customer friction.

Degree Company is Focused on Minimizing Customer Friction Through Online/Mobile Channels*

Canada Retail & E-commerce Merchants



Survey Questions:
Q30: To what degree is your company focused on minimizing customer friction during an online/mobile transaction checkout? Q30a: To what degree is your company focused on minimizing customer friction during online/mobile account opening?

*asked of those with online and/ or mobile channel translations

** Integration of Digital / Customer Experience with fraud prevention

+ = significantly higher than the segment counterpart

LexisNexis® RISK SOLUTIONS

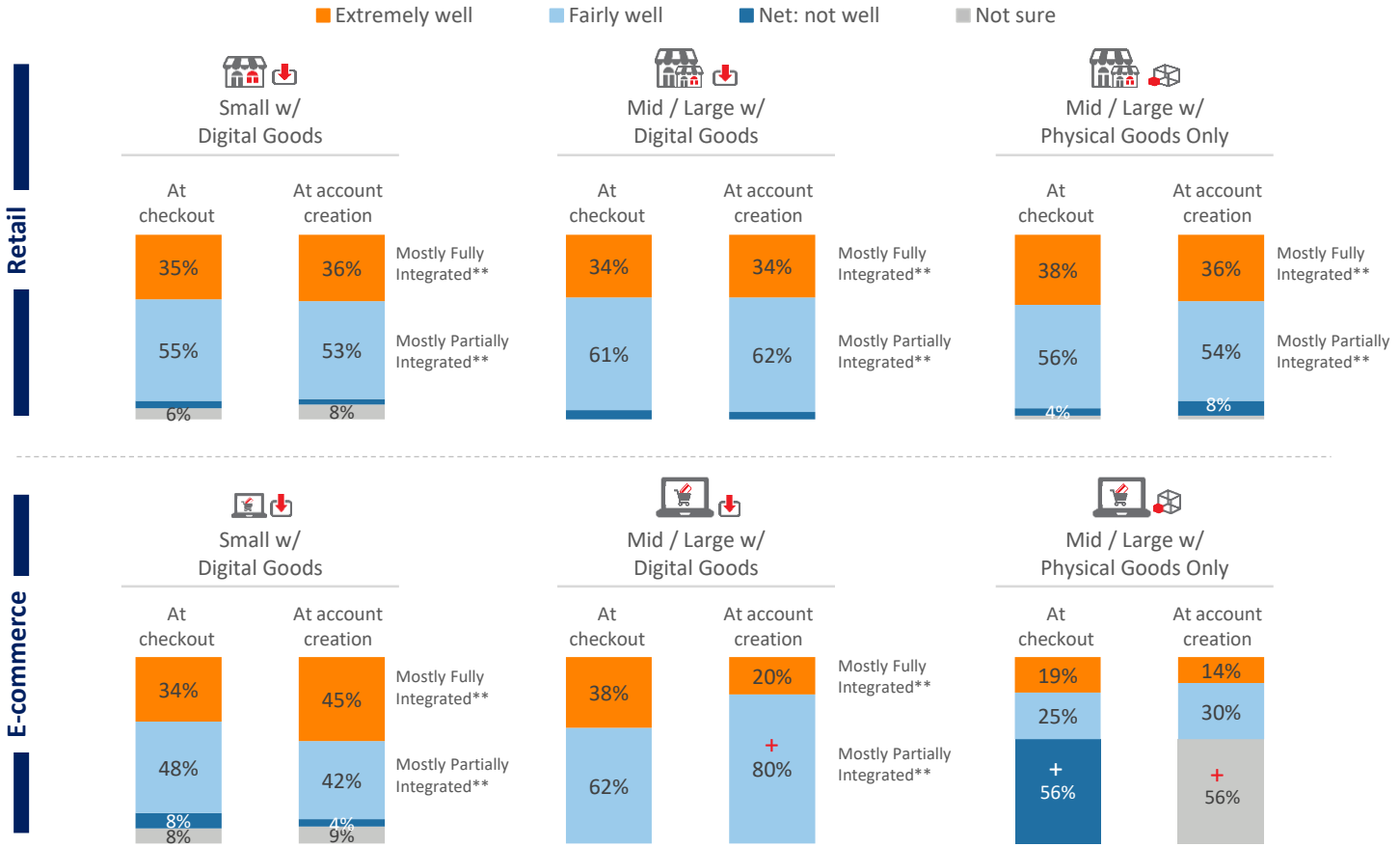
Survey Questions:
Q30c: How well would you say your company balances good customer experience/low friction against minimizing fraud risk during an online or mobile channel transaction checkout? Q30d: And wow well does it balance good customer experience/low friction against minimizing fraud risk during account opening?

There is recognition that fuller integration strengthens the ability to minimize both customer friction and fraud risk. Those who are fully integrated feel that they have done extremely well with this effort.

Mid / Large e-commerce that sell physical goods lag behind on digital / customer experience and fraud prevention integration efforts, but recognize that this can increase friction at checkout.

How Well Does Company Balance Good Customer Experience/Low Friction Against Minimizing Fraud Risk?*

US Retail & E-commerce Merchants



*asked of those with online and/or mobile channel translations
** Integration of digital / customer experience with fraud prevention
+ = significantly higher than the segment counterpart

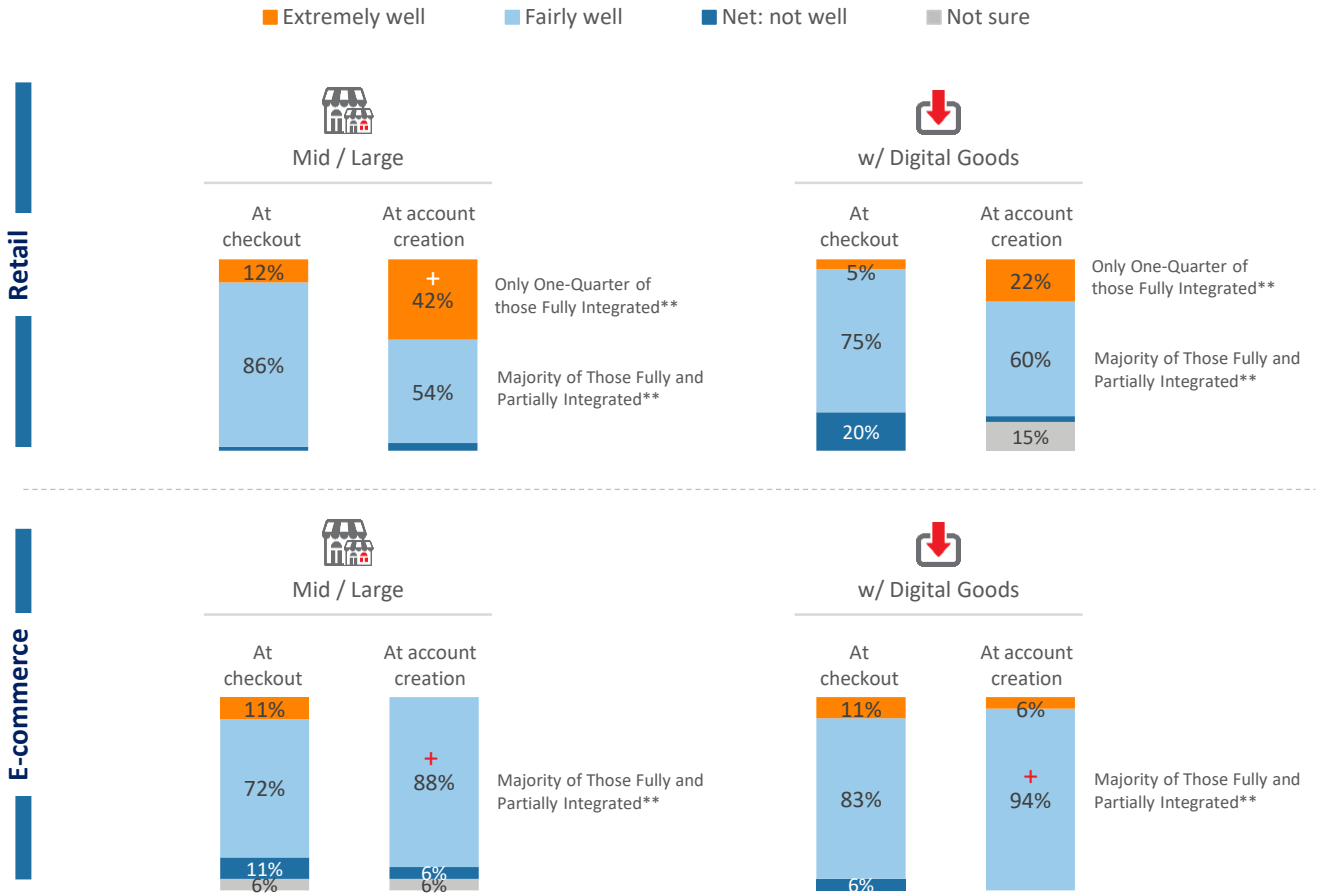
LexisNexis® RISK SOLUTIONS

The majority of Mid / Large Canadian retailers and E-commerce merchants tend to have more work to do with balancing fraud assessment and customer friction.

Even a majority of those who have fully integrated their digital / customer experience and fraud prevention efforts rate themselves as less than extremely good at balancing the customer experience against fraud risk.

How Well Does Company Balance Good Customer Experience/Low Friction Against Minimizing Fraud Risk?*

Canada Retail & E-commerce Merchants



Survey Questions:
Q30c: How well would you say your company balances good customer experience/low friction against minimizing fraud risk during an online or mobile channel transaction checkout? Q30d: And wow well does it balance good customer experience/low friction against minimizing fraud risk during account opening?

*asked of those with online and/or mobile channel translations
** Integration of digital / customer experience with fraud prevention
+ = significantly higher than the segment counterpart

LexisNexis® RISK SOLUTIONS

The degree of integration between cybersecurity, digital / customer experiences, and fraud prevention results in a measurable difference on organizations' ability to effectively fight fraud and reduce associated costs.

Study findings show that Mid / Large US retailers with digital goods (high risk for fraud), that have fully integrated these efforts, are more effective at fraud mitigation than even those who have partially integrated.

Mid / Large Retailers w/ Digital Goods

Fully Integrated	Risk Mitigation Solutions (% Indicating Use)	Partially Integrated
More Targeted & Layered Solutions (Avg. 8) Targeting high risk channels and transactions		**Fewer, Less Targeted & Layered Solutions** (Avg. 4)
E-mail Risk & Verification 58%		E-mail Risk & Verification 43%
Phone Risk & Verification 58%		Phone Risk & Verification 39%
Device ID 53%		
Geolocation 65%	***Passive / Digital Identity-based*** holistic view of individual; quick, behind-the-scenes fraud assessment that reduces customer effort and friction	Geolocation 53%
Biometrics 28%		
Behavioral Biometrics 30%		
Automated Transaction Tracking 48%	***Advanced ID & Transaction Verification*** assess risk of both the transaction and individual	Real-Time Transaction Tracking 66%
Real-Time Transaction Tracking 50%		
Authenticate by Challenge Question 55%	***Interactive Identity Authentication***	
Two-Factor Authentication 55%		
Better Able to Detect Botnets & Balance Fraud Assessment with Friction	**Mobile Channel Challenges** (% Ranking as a Top Challenge)	**Challenged with Detecting Botnets & Balancing Fraud Assessment with Friction**
16%	Inability to distinguish legitimate humans from malicious botnet attacks	36%
20%	Balancing fraud assessment with customer friction	38%
Less Than Average # Successful Monthly Fraud Attempts	**Average Monthly Fraud Attacks**	**Higher Average # Successful Monthly Fraud Attempts**
Slightly less than 2019 average	Average # Successful Attacks / Mo. 2019 = 1,135	More than 2019 average
1,032	Average # Successful Attacks / Mo. (2020)	1,403 (More than 16k per year)
Lower Cost of Fraud	**LexisNexis Fraud Multiplier™**	**Higher Cost of Fraud**
$2.92	Every $1 of fraud actually costs these retailers	$3.22
	2019 = $3.38	

LexisNexis® RISK SOLUTIONS

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 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 a 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 transaction patterns of an individual against their current transactions to detect if volume by the cardholder matches 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 a 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; email/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

Recommendations

- The combination of physical and digital identity analysis is essential.
- A multi-layered solution approach is most effective for fighting fraud across various channels and transaction types.
- Retailers and e-commerce merchants need to be extra prepared for increased fraud attacks for the foreseeable future.
- Protecting the customer relationship and brand is an important part of fraud prevention; it isn't just about the cost of fraud.
- More sophisticated global crime networks require more real-time third-party data and analysis in order to detect and prevent fraud and its collateral damage.

Recommendations

1) 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".

- These sophisticated threats are increasing, which negatively impacts e-commerce merchants and retailers with high fraud costs and potentially lost customers.
- 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".

2) A multi-layered solution approach is essential to protect retailers and E-commerce merchants throughout a single buyer experience. Each transaction channel and type carries unique risks.

- 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.)

3) Retailers and E-commerce merchants need to be extra prepared for increased fraud attacks and costs for the foreseeable future.

- It is unclear what the purchasing landscape will look like over the next 1 -2 years as shaped by the COVID-19 pandemic.
- Will we see a return to pre-COVID-19 shopping behaviors, or will there be a new normal that involves a higher level of online and mobile channel transactions than would have otherwise trended without the pandemic?
- If so, then retailers and e-commerce merchants could be faced with greater fraud spikes for at least for the foreseeable future. And since these will involve remote channels, the fraud techniques are more insidious and complex than those used with in-store transactions.
- Businesses which have invested in digital identity and transaction fraud detection solutions cited earlier will be more prepared to deal with these sudden changes. As the cost of doing business rises in this COVID-19 environment, the *added cost* of fraud may become a negative tipping point for retailers / merchants that haven't yet invested in these solutions.

4) As more transactions move to the online and mobile channels, the ability to compete becomes more challenging. Protecting customer relationships and your brand will become more important than ever.

- Consumers literally have more options at their fingertips, including abandoning a transaction that is burdensome. New customers may appreciate extra steps taken to verify their identity, such as providing passwords, answers to questions and one-time code numbers. Recurring customers may tire of this at some point based on the "you should know me by now" mindset. Not all transactions carry the same level of risk.
- Having risk mitigation solutions that allow you the flexibility of customizing verification efforts according to risk level can lessen friction.
- Customer relationships can be harmed if your customers become victims of fraud that is based on transactions with your business. Social media can further erode brand health where these grievances are shared.
- As a result, the investment in multi-layered solutions that assess both the digital and physical, individual and transactional attributes are important for not only protecting against fraud, but to also minimize the friction points and collateral damage caused by fraud.
- But there should be more to your fraud prevention strategy. It is crucial to have an approach that fully integrates these solutions with your cybersecurity and digital customer experience efforts as well, including the tracking of fraud by channel and transaction type.

LexisNexis® RISK SOLUTIONS

Recommendations (cont.)

5) Without more real-time third-party data and analysis, retailers and E-commerce merchants will continue to struggle with various aspects for fraud.

- More online / mobile purchasing will translate into faster transactions, with the need to quickly identity fraud and minimize friction.
- Those conducting international transactions will experience even further challenges without such real-time third-party data.
  - More complex and interconnected fraud rings using multiple devices and identity attributes can easily confuse the source of transaction origination.
  - Newer privacy regulations, such as GDPR, make it increasingly difficult for businesses to access and store customer data that is essential for effective identity verification and authentication.
- Payment gateways / providers can unknowingly be leveraged by fraudsters in order to hide behind complex transaction linkages, speed and volume of transactions hitting a retailer and lack of transparency about the origination source and end customer.

LexisNexis® Risk Solutions can help.

For more information:

risk.lexisnexis.com/FraudandIdentity

+1 800 953 2877
+408 200 5755

LexisNexis® RISK SOLUTIONS