LexisNexis® Risk Solutions True Cost Of Fraud™ Study for Ecommerce and Retail

2021 U.S. & Canada Edition

LexisNexis®
RISK SOLUTIONS

Overview

Key Findings

#1 Attacks & Costs

#2 Trends

#3 Challenges

#4 Best Practices

#5 Best Practices in Use

Recommendations

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

The research provides a snapshot of:

- Current fraud trends in the U.S. and Canadian ecommerce and retail markets
- Key pain points related to adding new payment mechanisms, transacting through online and mobile channels, and expanding internationally

COVID-19 impact:

- Data collection occurred during March – April 2021; many of the survey questions reference the past 12 months; therefore, findings reflect activity, fraud risks, challenges and costs that have been impacted by COVID-19 fears, changing behaviors and forced lockdowns

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
- Fraudulent applications (e.g., purposely providing incorrect information about oneself, such as income, employment, etc.)
- Account takeover by unauthorized persons
- Use of accounts for money laundering

This research covers consumer-facing fraud methods:

- Does **not** include insider fraud or employee fraud

The LexisNexis Fraud Multiplier™ cost:

- 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 survey of 1,118 risk and fraud executives in retail and ecommerce companies in the U.S. (973) and Canada (145).

Retailers and Ecommerce Merchants Include a Variety of Categories

# of Survey Completions
1,118

Segments

Segment definitions:	**Small** Earns less than $10 million in annual revenues	**Mid/Large** Earns $10 million+ in annual revenues
# of Survey Completions:	**517**	**601**

Overview

Key Findings

#1 Attacks & Costs

#2 Trends

#3 Challenges

#4 Best Practices

#5 Best Practices in Use

Recommendations

01 **The cost and volume of fraud has risen significantly compared to pre-COVID periods.** Every $1 of fraud costs U.S. retail and ecommerce merchants $3.60 compared to $3.13 prior to the pandemic. The cost of fraud is 3.02 times the lost transaction value for Canadian merchants. The mobile channel is playing a role in this, as more consumers turned to their devices to shop during the pandemic.

02 **COVID-19 has changed consumer behaviors, including more use of mobile channel shopping and payment methods. And fraudsters have followed, taking advantage of merchants who have accelerated their mobile channel approaches.** There is increased use of mobile apps and contactless payment methods, at the expense of mobile browsers. With this shift in behavior has come a shift of fraud costs from mobile browsers to these other methods.

03 **Identity verification remains a top challenge for merchants and represents a larger share of fraud losses compared to previous years. Breached digital identity data (e-mail addresses, phone numbers) are being linked to synthetic identities and more account related fraud.** Merchants struggle with verifying digital identity data and concerns with balancing fraud detection and customer friction. At the same time, however, there is limited use of solutions designed to support both of these issues. Changes in new payment methods through the mobile channel have increased difficulties with fraud detection of transactions involving third-party payment providers.

04 **As fraud becomes more complex, a best-practice approach for retail and ecommerce merchants is to use a multi-layered approach involving digital/transaction risk mitigation solutions that are integrated with cybersecurity and digital customer experience operations.** There has been an increase in merchants who have completed this integration compared to before COVID-19.

05 **Merchants that use the best-practice approach may be able to more effectively prevent fraud, optimize the risk-to-friction level with customers and lower their cost of fraud.** Those who are serious about optimizing fraud detection-to-customer friction levels use this approach across the customer journey and tend to experience fewer challenges with identity verification and distinguishing between legitimate customers versus malicious bots.

KEY FINDING 01

The cost and volume of fraud has risen significantly compared to pre-COVID periods. Every $1 of fraud costs U.S. retail and ecommerce merchants $3.60 compared to $3.13 prior to the pandemic.

The cost of fraud is 3.02 times the lost transaction value for Canadian merchants, up 5.2% since early 2020.

Ecommerce merchants have experienced higher costs during the pandemic compared to retailers.

As the average monthly volume of fraud attacks increase, retail and ecommerce merchants may be losing pace as more attacks move from being prevented to successful.

More fraud costs are being attributed to the mobile channel than in prior years, as more consumers turned to digital transactions—and mobile ones in particular.

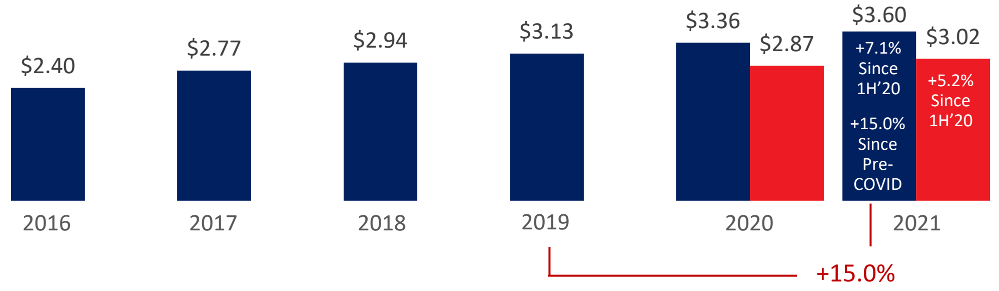
Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

The LexisNexis Fraud Multiplier^{TM} has increased significantly since just before COVID-19. Every $1 of fraud costs U.S. merchants $3.60 compared to $3.13 in the Pre-COVID time period (+15.0%).

This continues a trend based on fraud involving more mobile transactions, increased bot/cyber attacks and synthetic identities which have been significantly heightened during the COVID-19 pandemic. Ecommerce merchants have experienced higher cost of fraud during the pandemic, particularly involving a large portion related to replacing/redistributing lost goods. This aligns with increased fraud volume and new payment methods through online and mobile transactions as physical/in-person shopping declined.

Cost of Fraud: LexisNexis Fraud Multiplier^{TM}

■ U.S. ■ Canada



Continued growth of mcommerce (= fraud), increasing bot attacks/click flooding testing and using breach consumer data; increased use of synthetic identities and an expanded scope of fraud targets beyond the big box retailers.

COVID-19 pandemic heightened, accelerate the above.

SEGMENT HIGHLIGHTS

Ecommerce merchants have higher fraud costs.

- Every $1 of fraud costs Canadian ecommerce merchants $3.23 (up 10% from last year at $2.93)
- U.S. ecommerce merchants have been hit with the highest fraud costs, with nearly half (47%) related to replacing/redistributing lost goods; every $1 of fraud costs these merchants $3.90

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.

▼▲ = significantly or directionally higher/lower than previous period

LexisNexis®
RISK SOLUTIONS

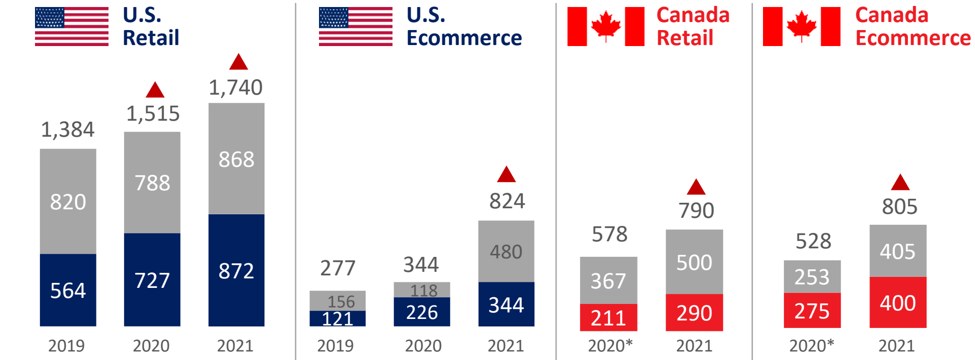
Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

The overall volume of fraud attacks has grown beyond pre- and early-pandemic periods, with businesses allowing online/mobile transactions experiencing the largest year-over-year increase.

In addition to ecommerce merchants, this includes brick and mortar retailers that have a sizeable volume of transactions through their online/mobile channels. While U.S. retailers experience more successful fraud attacks, U.S. and Canadian ecommerce merchants have a reportedly higher percentage increase overall and for successful attacks since the early-pandemic period. This aligns with the period when transactions shifted to remote channels.

Average Monthly Fraud Attacks | Retail & Ecommerce Merchants

▨ Avg. Number Prevented Monthly Fraud Attacks
■ Avg. Number Successful Monthly Fraud Attacks (U.S.)
🟥 Avg. Number Successful Monthly Fraud Attacks (Canada)



Change from Previous Period

Overall	+9%	+15%	+140%	+37%	+52%
Successful Attacks	+28%	+20%	+52%	+37%	+45%

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?

▼▲ = significantly or directionally higher/lower than previous period

SEGMENT HIGHLIGHTS

Mid/Large average successful attacks/month:

- ML Retail (U.S.) (1,130)
- ML Ecommerce (U.S.) (945)
- ML Ecommerce (Canada) (506)

Brick and mortar retailers with sizeable online channel volume (30%+) have more attacks per month (1,916) compared to retailers with less online channel presence (890)

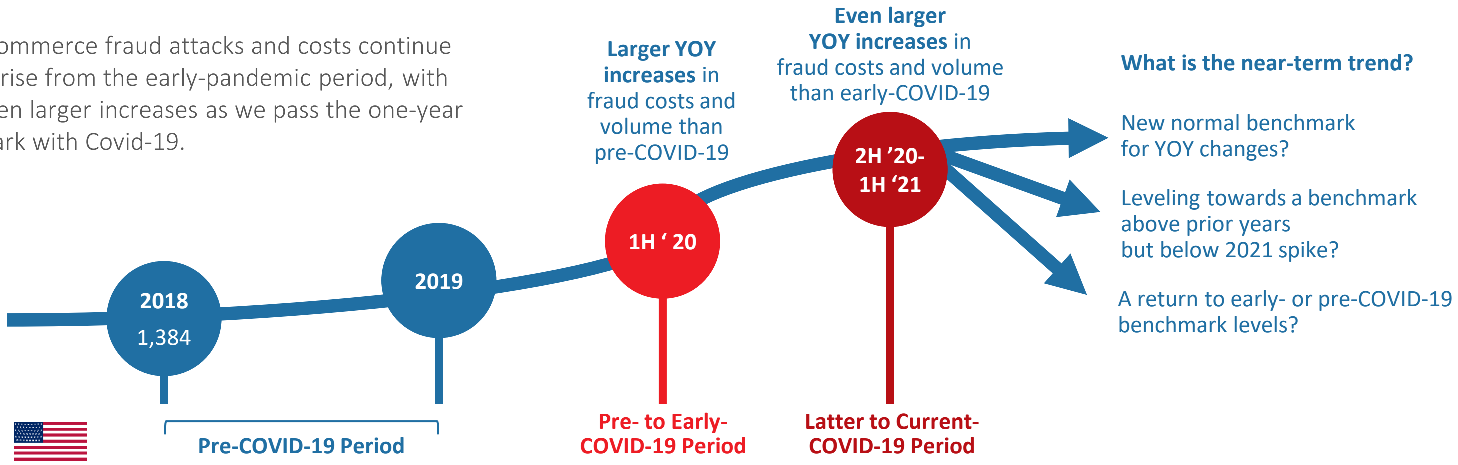
*First wave of True Cost of Fraud TM Study for Canada

Key Finding 01
INCREASED FRAUD ATTACKS

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

The spike in fraud attacks and cost for ecommerce merchants since early 2020 was not a temporary event; Ecommerce saw a 34.4% increase in the cost of fraud and a 140% increase in volume fraud attacks since the pre- to early- COVID-19 period.

Ecommerce fraud attacks and costs continue to rise from the early-pandemic period, with even larger increases as we pass the one-year mark with Covid-19.



Larger YOY increases in fraud costs and volume than pre-COVID-19

Even larger YOY increases in fraud costs and volume than early-COVID-19

What is the near-term trend?

New normal benchmark for YOY changes?

Leveling towards a benchmark above prior years but below 2021 spike?

A return to early- or pre-COVID-19 benchmark levels?

Pre-COVID-19 Period

Pre- to Early-COVID-19 Period

Latter to Current-COVID-19 Period

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. 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?

U.S.* Cost of Fraud: LexisNexis Fraud Multiplier™

Overall	$2.94	$3.13 (+6.5%)	$3.36 (+7.3%)	$3.60 (+7.1%)
E-commerce	$2.51	$2.63 (+4.7%)	$2.90 (+10.2%)	$3.90 (+34.4%)

U.S.* Volume of Fraud: Average Monthly Fraud Attacks

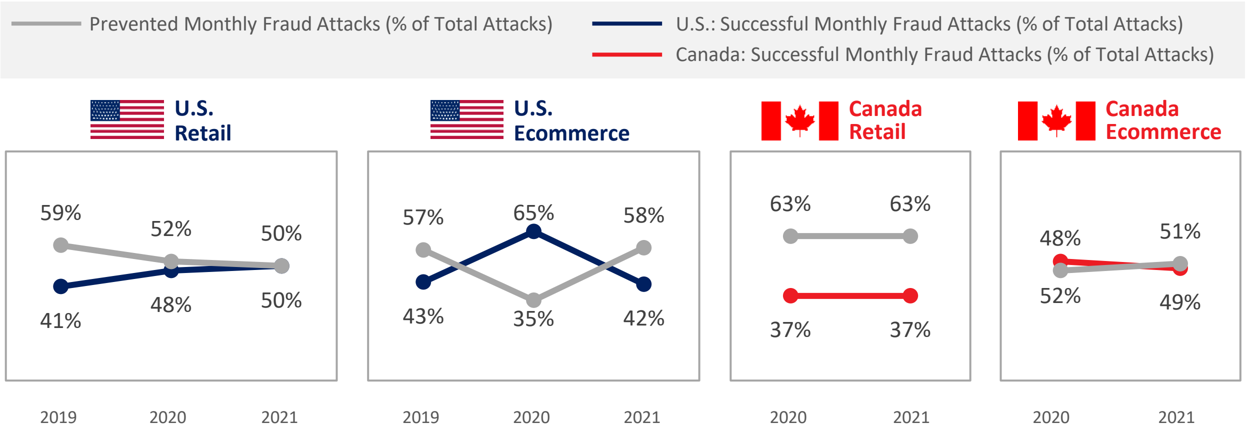
E-commerce	260	277 (+6.5%)	344 (+24.2%)	824 (+140.0%)

* Reflects U.S. only since there is a longer period for trending this market in the LexisNexis® Risk Solutions True Cost of Fraud™ study; Canada was only added as a market in 2020

U.S. retailers may be losing pace with increased fraud attacks, as the percent of successful average monthly attacks rises to the same level as prevented attacks.

A similar ratio is found with Canadian ecommerce merchants. There was a dramatic increase in successful fraud attacks against U.S. ecommerce merchants near the start of the COVID-19 pandemic, though the successful-to-prevented ratio seems to have course-corrected during the pandemic. However, this segment has nonetheless experienced the highest percentage increase in year-over-year attacks.

% Prevented/Successful Monthly Fraud Attacks | Retail & Ecommerce Merchants



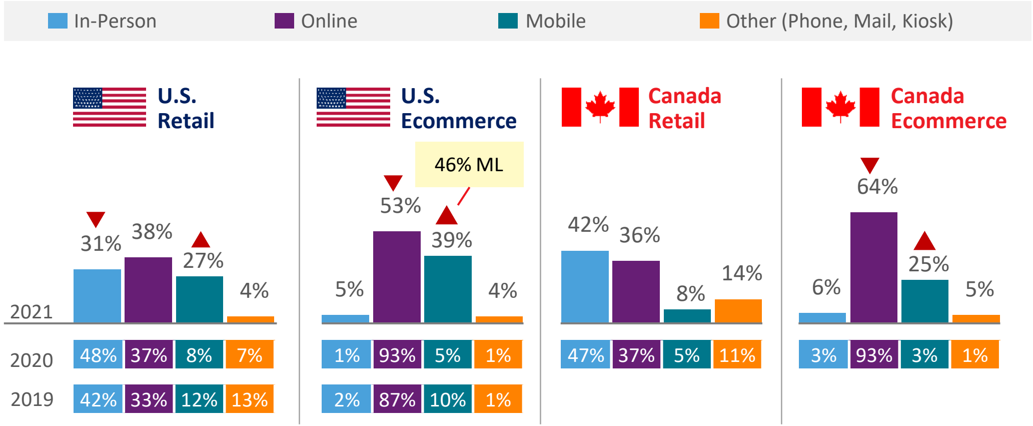
Survey Questions:
Q22: In a typical month, approximately how many fraudulent transactions are prevented by your company? Q24: In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

Increased fraud is being generated from across more channels, not just primarily in-person and online as before. Since the pandemic, there is also sizeable fraud being generated from the mobile channel.

For U.S. retailers, the shift to mobile has been from less in-person based fraud (and transactions), to a point that comes close to the percent driven from the online channel. Ecommerce merchant fraud costs have also involved more mobile channel transactions, particularly U.S. ecommerce.

% Fraud Costs by Channel | Retail & Ecommerce Merchants



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

▼▲ = significantly or directionally higher/lower than previous period

DID YOU KNOW?

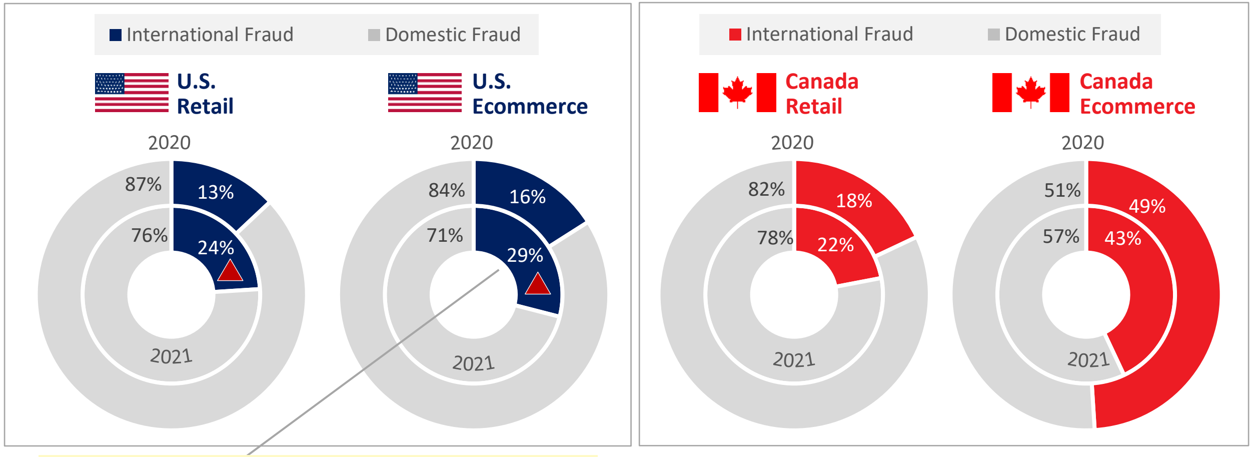
A recent report from LexisNexis® Risk Solutions, *In Uncertain Times: An analysis of the Impact of COVID-19 on Consumer Behavior and Fraud Trends*, there has been an increase in new devices with more consumers turning to digital for the first time (increase in new-to-digital identities). At the same time, there is increased fraud linked to e-mail and IP addresses having multiple billing addresses. And, there has been increased risk of large distances between recorded IP addresses and reported billing addresses, which is the "smoking gun" with regard to digital fraud.

Fraud increases are also coming from more international attacks against U.S. retail and ecommerce merchants, nearly doubling since 2020.

Canadian ecommerce merchants continue to experience significantly more international-based fraud than others.

International transactions carry additional, unique risks including difficulty determining the origination source and authenticating identities based on data privacy restrictions, different consumer behaviors and other payment methods.

% Fraud from Domestic & International Transactions | Retail & Ecommerce Merchants



Mid/large with sizeable % of fraud costs from international (40%+) are more likely to have difficulty distinguishing bots from legitimate customers (40%) and balancing fraud detection/friction (36%) with mobile transactions.

Survey Questions:
Q13: Please indicate the percent of annual fraud costs generated through domestic compared to international transactions in the last 12 months

▼▲ = significantly or directionally higher/lower than previous period

LexisNexis RISK SOLUTIONS

KEY FINDING 02

COVID-19 has changed consumer behaviors, including more use of mobile channel shopping and payment methods. And fraudsters have followed, taking advantage of merchants who have accelerated their mobile channel approaches.

More home/remote time during the pandemic brought more use of mobile devices. Consumers have increased their use of mobile apps as a preferred and more user-friendly format when shopping from their devices.

Consumers have also begun using more contactless payment methods, whether in-store contactless/payment reader or through text-to-pay and bill-to-mobile. There is also some emergence of virtual currency use with mobile transactions.

The distribution of mobile transactions and fraud costs have shifted from mobile browsers to mobile apps and contactless payment methods.

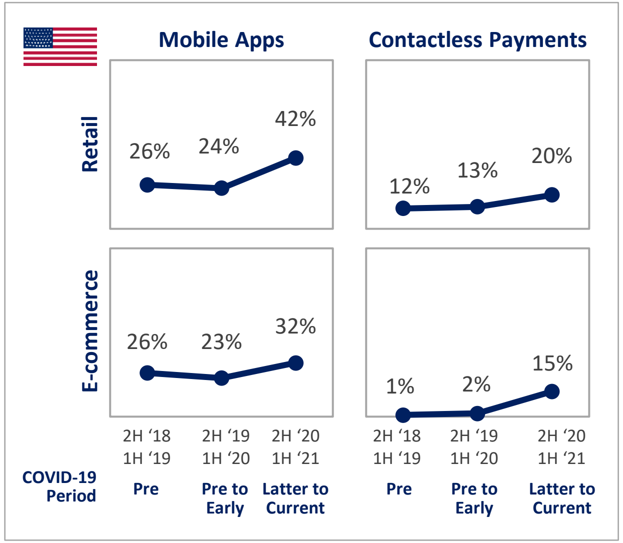
Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

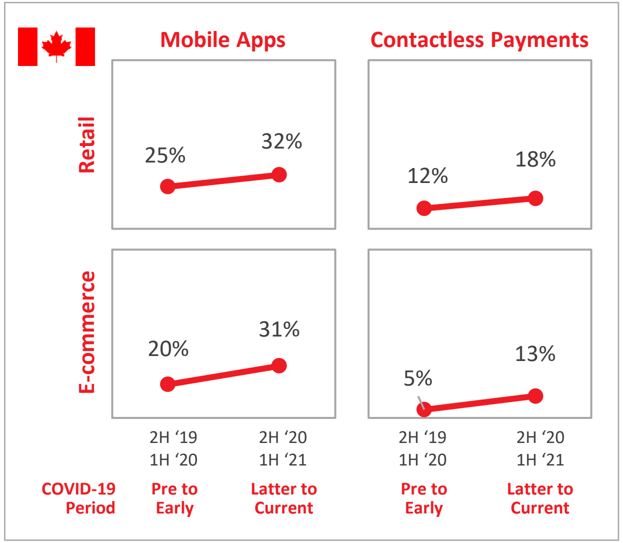
The digital *evolution* of consumers to more remote shopping during the early shutdown period may have become a *digital transformation*.

As expected, early-pandemic period (1H 2020) transitioning from in-person to more online/mobile shopping was a natural result of forced shutdowns and concerns with rising infections. But since then, as merchants began opening up and infection rates leveled off/dropped, the use of mobile channel shopping has risen significantly over the earlier increases.

A digital transformation also involves more than increased digital transactions. It also is shaped by a change in transaction and payment methods, as more consumers shift to using contactless payments and mobile apps. While remote shopping activity could drop during a new normal period, it's likely that some portion of increased digital use will continue based on preferences developed during the pandemic— particularly since there has been an increase in *new* digital consumers and *new* device subscriptions.[1]

Average % of Consumer Transactions Through Mobile Transaction & Payment Methods





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.

[1] A recent report from LexisNexis® Risk Solutions, *In Uncertain Times: An analysis of the Impact of COVID-19 on Consumer Behavior and Fraud Trends*

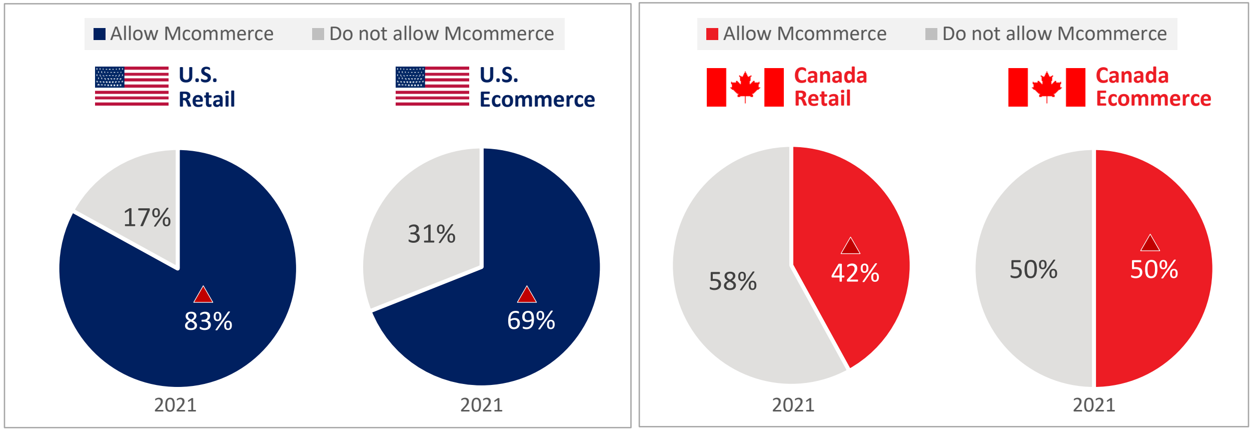
LexisNexis® RISK SOLUTIONS

Overview
Key Findings
#1 Attacks & Costs
#2 **Trends**
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

There has been significant growth among the number of merchants offering mcommerce since 2019.

The increased adoption by businesses is less likely to be a quick response to the pandemic; there were a considerable number of merchants indicating consideration for implementing mcommerce when asked in late 2019/early 2020, which is similar to the percentage uptake. Furthermore, it takes time to implement and optimize a mobile channel process. However, COVID-19 likely accelerated plans that were already underway.

Businesses Offering Mcommerce | Retail & Ecommerce Merchants



		(% Considering)		(% Considering)		(% Considering)		(% Considering)
% Allowing Mcommerce 2020	43%	(35%)	34%	(47%)	23%	(24%)	25%	24%
% Allowing Mcommerce 2019	48%		23%		NA		NA	

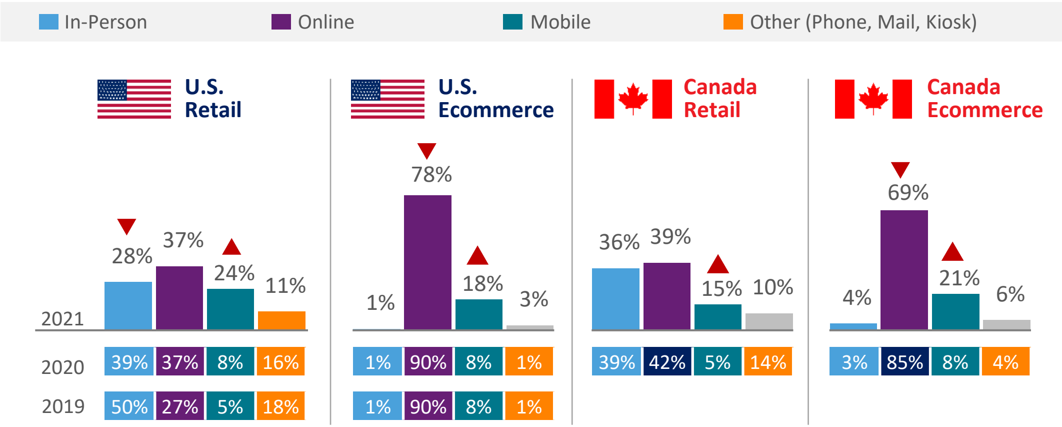
Survey Questions:
Q4: Please indicate the % of transactions completed (over the past 12 months) for mobile payments by your company.

▼▲ = significantly or directionally higher/lower than previous period

Online became the dominant channel for U.S. retailers during the pandemic, but mobile drove growth of remote transactions. While in-person transactions dropped, they are still a sizeable percentage.

Some of the mobile channel growth is due to changed consumer environments/behaviors. Working remotely did not necessarily mean more laptop time; blurring home and office did allow for more mobile device time (free from the boss' eyes). Increased mobile app use is one measure, as consumer shopping focused on essentials, home improvement, entertainment and (for some) health.

% Transaction Volume by Channel | Retail & Ecommerce Merchants



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

▼▲ = significantly or directionally higher/lower than previous period

COVID-19 SHOPPING

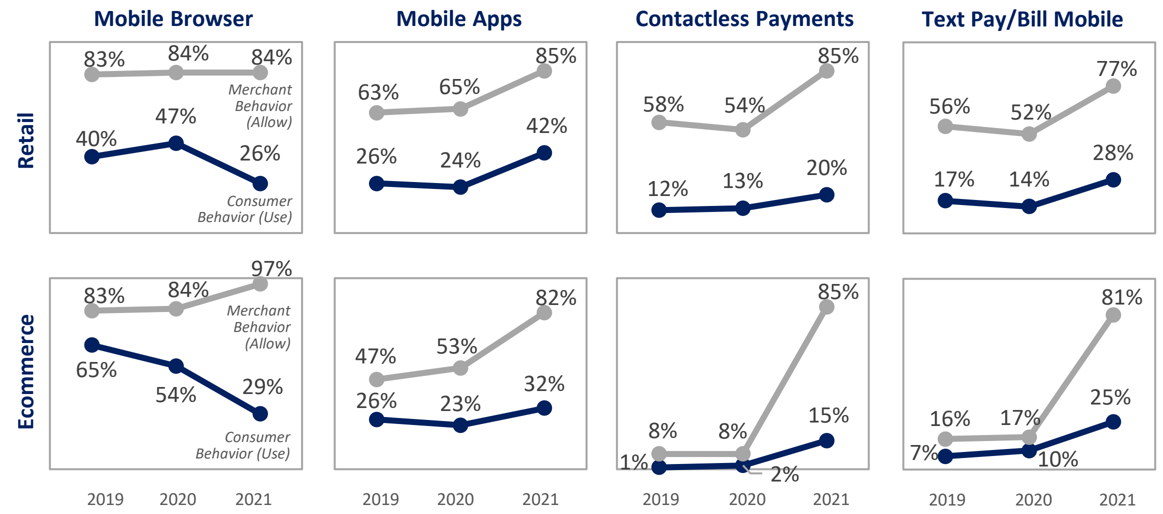
Industries that have been more likely to have higher mobile transactions (20%+) this past year include digital games, drug, health/beauty, flowers/gifts, food and beverage, housewares, general merchandise, gaming, sporting goods and telecommunications.

While Canada has experienced a number of lockdowns, there are certain sectors that kept a restricted in-person channel open, including computers and electronics, grocery, hardware and automotive.

U.S. retailers and ecommerce merchants have expanded ways to purchase through the mobile channel. Consumers have increased in-app purchasing over browsers, as well as some shift to contactless payment methods at both physical point of sale and remotely.

% Merchants Allowing/% Distribution of Transactions Through Mobile Payment Methods | Retail & Ecommerce Merchants

% of Businesses that Accept Transactions through the Channel — Avg. Distribution of All Mobile Transactions through the Channel



MOBILE APP USE

The distribution of consumer transactions using a mobile browser has dropped, as preference and use of mobile apps increased.

Apps for food/delivery, shopping/curbside pickup, and entertainment saw significant increased use during the shutdown.[1]

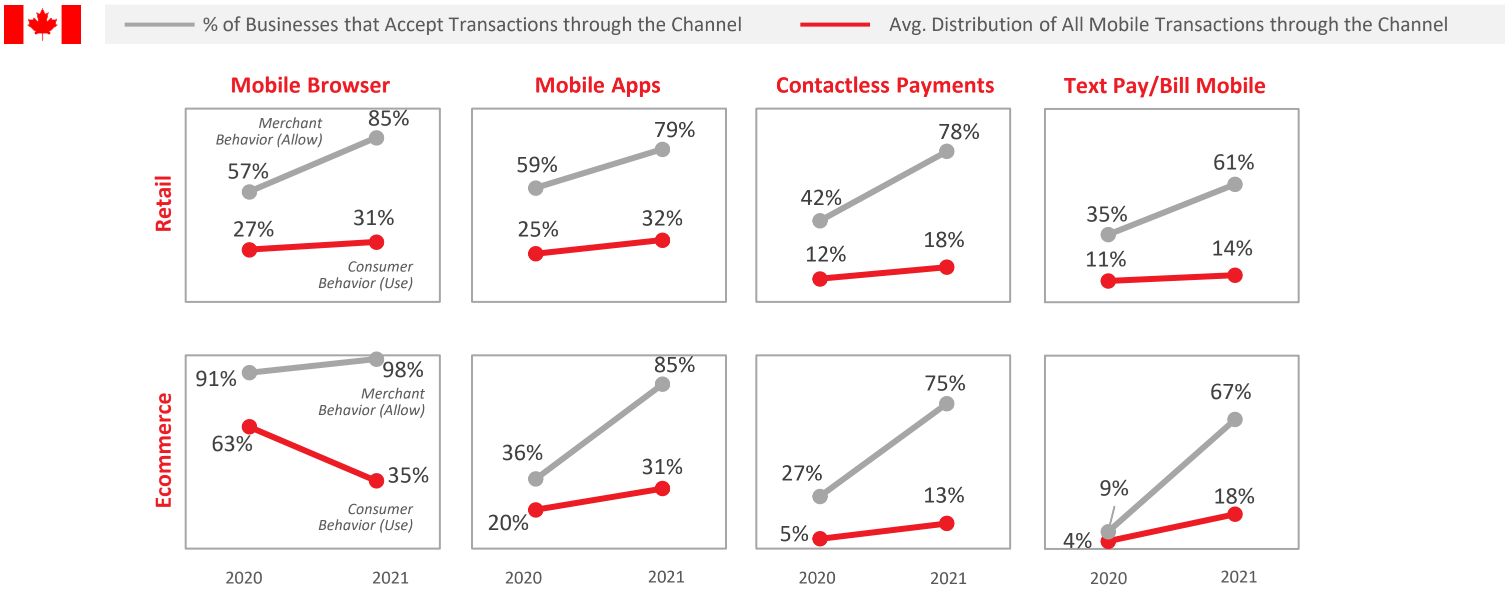
Survey Questions:
Q4: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment channels currently accepted by your company.

▼▲ = significantly or directionally higher/lower than previous period

[1] https://www.gwsolutions.com/the-pandemic-year-in-mobile-apps/

Canadian merchants also expanded mobile payment options. The bigger change in consumer behavior is with ecommerce, as the distribution of mobile payments shifts away from browsers.

% Merchants Allowing/% Distribution of Transactions Through Mobile Payment Methods* | Retail & Ecommerce Merchants



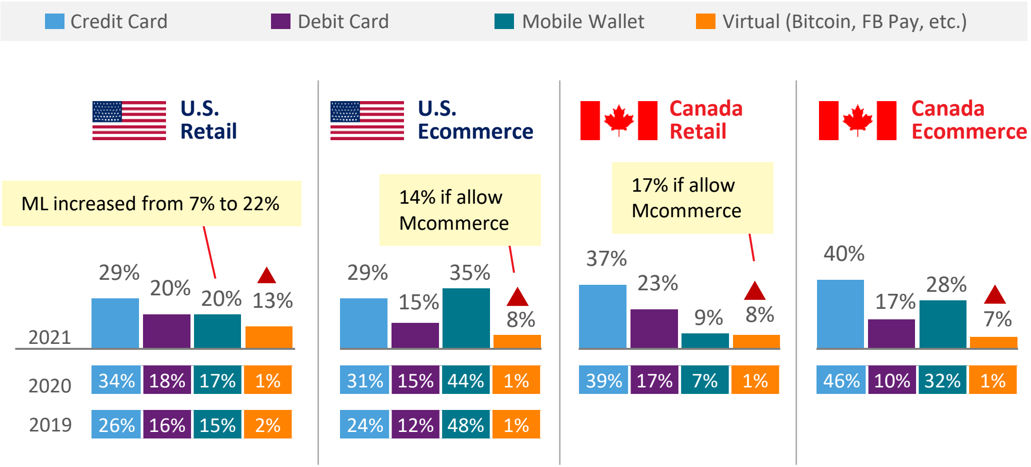
Survey Questions:
Q4: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment channels currently accepted by your company.

▼▲ = significantly or directionally higher/lower than previous period

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

The use of mobile wallets has increased significantly among mid/large U.S. retailers, with some emergence of virtual currency use for mobile transactions.

% Transaction Volume by Payment Method | Retail & Ecommerce Merchants



ML increased from 7% to 22%

14% if allow Mcommerce

17% if allow Mcommerce

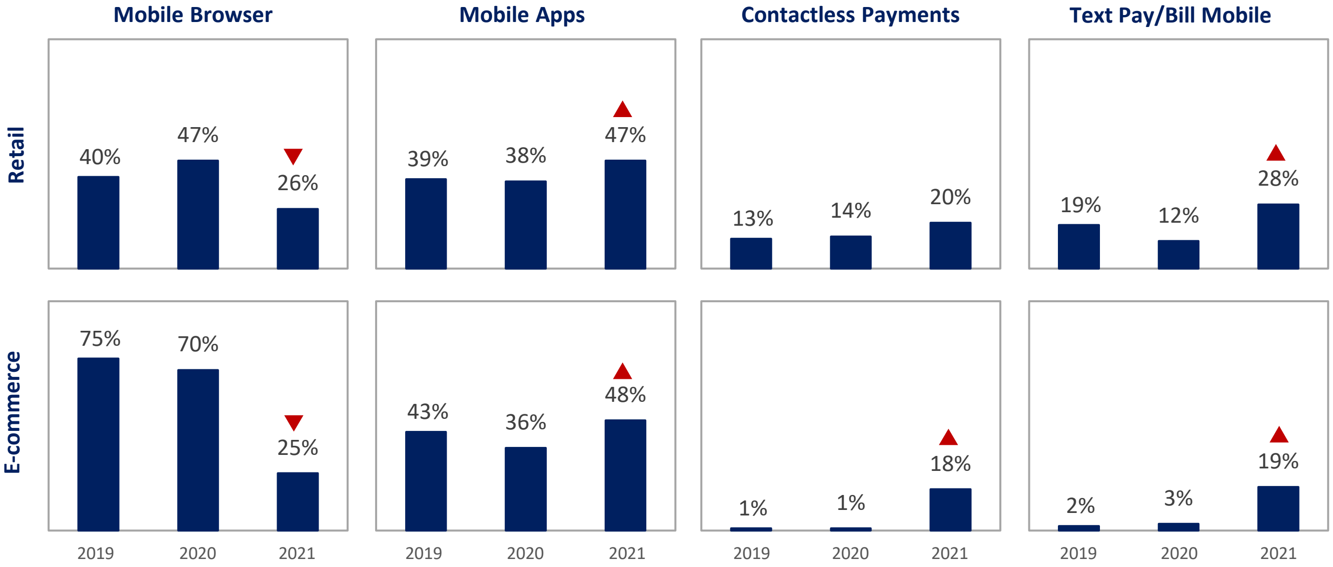
Survey Questions:
Q3: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment methods currently accepted by your company.

▼▲ = significantly or directionally higher/lower than previous period

LexisNexis® RISK SOLUTIONS

The distribution of fraud by mobile payment method among U.S. retail and ecommerce merchants has shifted from browsers to mobile apps and contactless forms, including text-to-pay/bill-to-mobile.

% Distribution of Fraud Losses by Mobile Payment Method | Retail & Ecommerce Merchants



		Mobile Browser	Mobile Apps	Contactless Payments	Text Pay/Bill Mobile
Retail	2019	40%	39%	13%	19%
	2020	47%	38%	14%	12%
	2021	▼ 26%	▲ 47%	20%	▲ 28%
E-commerce	2019	75%	43%	1%	2%
	2020	70%	36%	1%	3%
	2021	▼ 25%	▲ 48%	▲ 18%	▲ 19%

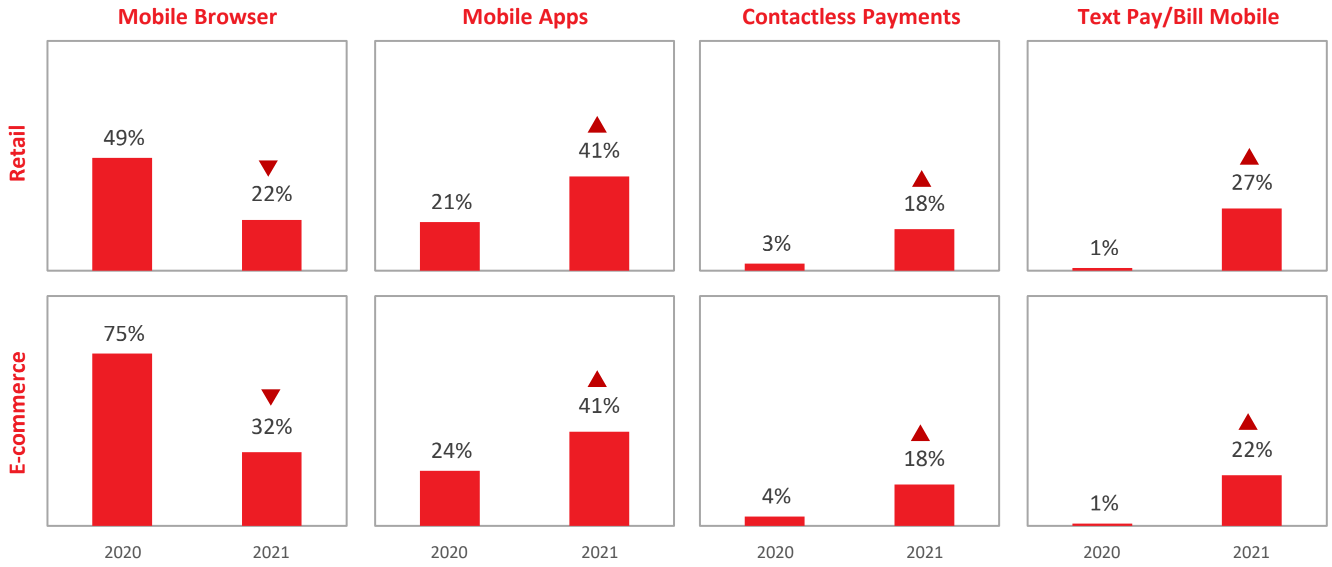
Survey Questions:
Q17: Please indicate the distribution of fraud across the various mobile channels you use/accept.

▼▲ = significantly or directionally higher/lower than previous period

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

The same changing trend with mobile payment method fraud is occurring with Canadian merchants as well.

% Distribution of Fraud Losses by Mobile Payment Method | Retail & Ecommerce Merchants



Survey Questions:
Q17: Please indicate the distribution of fraud across the various mobile channels you use/accept.

▼▲ = significantly or directionally higher/lower than previous period

LexisNexis® RISK SOLUTIONS

KEY FINDING 03

Identity verification remains a top challenge for merchants and represents a larger share of fraud losses compared to previous years. Breached digital-identity data (e-mail addresses, phone numbers) are being linked to synthetic identities and more account related fraud.

These digital-identity attributes are among the top challenges that retail and ecommerce merchants cite for both the online and mobile channels. And, as shown later, there is limited use of fraud detection solutions which can minimize these challenges.

Merchants also struggle with concerns about fraud detection efforts and minimizing customer friction, especially since abandonment is a common risk with remote channel transactions.

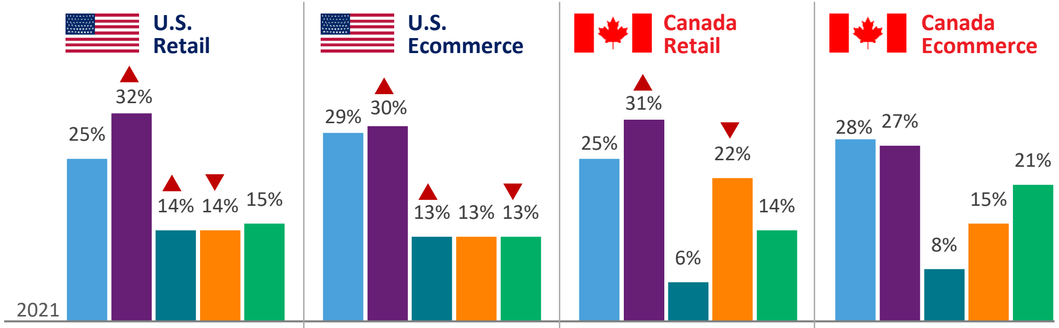
And, as payment methods have changed, merchants are also being challenged with transactions involving non-bank, third-party payment providers significantly more so compared to previous years.

There is need for more real-time transaction data to assess digital identities and determine the origination/source of remote transactions.

Identity fraud has become a larger share of fraud losses, with account takeover also representing a larger share of losses for U.S. merchants compared to previous years.

% Distribution of Fraud Losses by Fraud Type | Retail & Ecommerce Merchants

- 🟦 Friendly Fraud/ 1st Party Fraud
- 🟪 3rd Party/Synthetic Identity Fraud
- ■ 3rd Party Account Takeover
- 🟧 Lost or stolen merchandise
- 🟩 Fraudulent request for return



	U.S. Retail					U.S. Ecommerce					Canada Retail					Canada Ecommerce				
2020	26%	22%	3%	30%	17%	31%	23%	2%	14%	28%	31%	11%	2%	40%	17%	30%	27%	2%	12%	27%
2019	27%	22%	6%	28%	16%	35%	26%	3%	17%	27%										

Survey Questions:
Q12a: Please indicate the percentage distribution of the following fraud methods, as they are attributed to your fraud losses that occurred during the past 12 months.

▼▲ = significantly or directionally higher/lower than previous period

BREACHED DATA

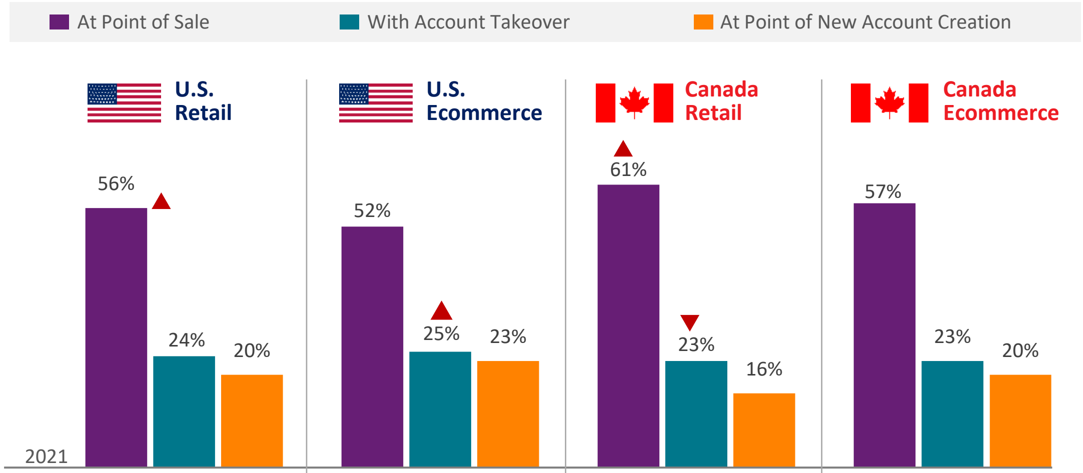
During the past year, the LexisNexis Digital Identity Network indicates a rise in fraudulent events through e-mail addresses and telephone numbers that are likely from data breaches. This data is used by multiple fraudsters to create synthetic identities with a focus on fraudulent account creation or takeover of existing accounts.

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

The significant percent of identity-related fraud continues to be at the point of sale, particularly increasing for Canadian retailers over last year.

The percent of identity-related fraud based on account takeover has increased significantly for U.S. ecommerce merchants.

Identity-Related Fraud: % Distribution by Activity | Retail & Ecommerce Merchants



	U.S. Retail			U.S. Ecommerce			Canada Retail			Canada Ecommerce		
2020	58%	20%	22%	60%	16%	24%	51%	36%	13%	57%	23%	20%
2019	54%	21%	25%	59%	17%	24%						

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

▼▲ = significantly or directionally higher/lower than previous period

LexisNexis RISK SOLUTIONS

Key Finding 03

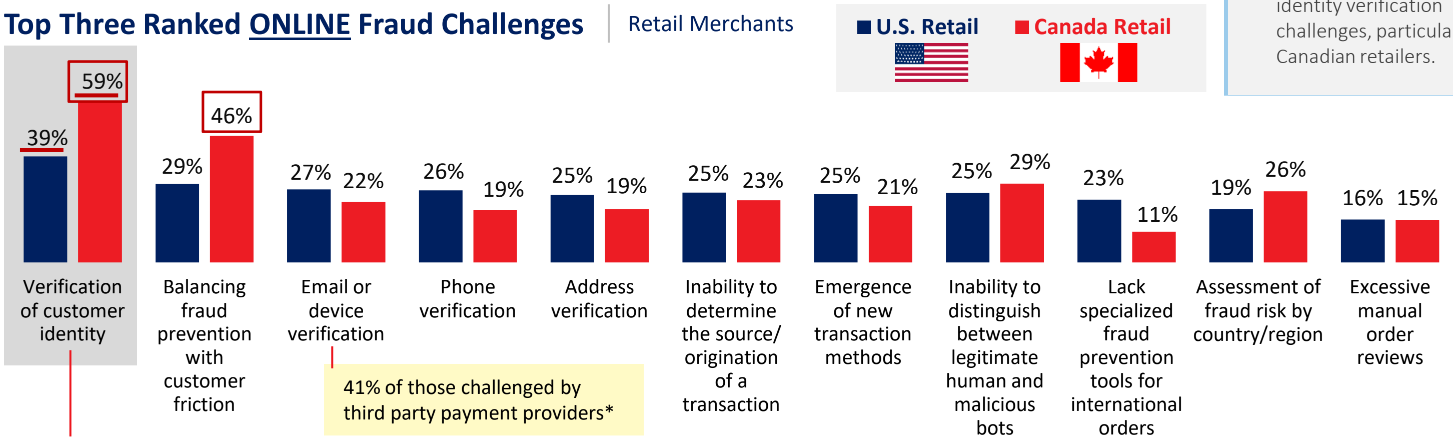
IDENTITY VERIFICATION AS A KEY ONLINE CHANNEL CHALLENGE

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

Identity verification is the top online channel challenge for U.S. and Canadian retailers, followed by balancing fraud prevention with friction and specific types of verification that contribute to the overall identity challenge.

These additional identification challenges involve digital attributes (phone, e-mail addresses), which—as previously mentioned—are types of breached data that fraudsters are using to create synthetic identities.

Top Three Ranked ONLINE Fraud Challenges | Retail Merchants



41% of those challenged by third party payment providers*

Key barriers to identity verification

- Rise of synthetic identities (U.S. 42%, Canada 57%)
- Balancing fraud speed with customer friction (U.S. 47%, Canada 50%)
- Lack of real-time transaction solution (U.S. 47%, Canada 41%)

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

▬ = significantly or directionally higher than other challenges within market

□ = significantly or directionally higher than same challenge in other markets

* 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.

DID YOU KNOW?

Breached data is not entirely about getting access to peoples' PINs and passwords. It is about getting access to people themselves—their physical and digital attributes—where they shop, how they shop, etc. Then, fraudsters use this data to create identities that look and act like valued and legitimate customers. As shown below, this is a leading contributor to identity verification challenges, particularly for Canadian retailers.

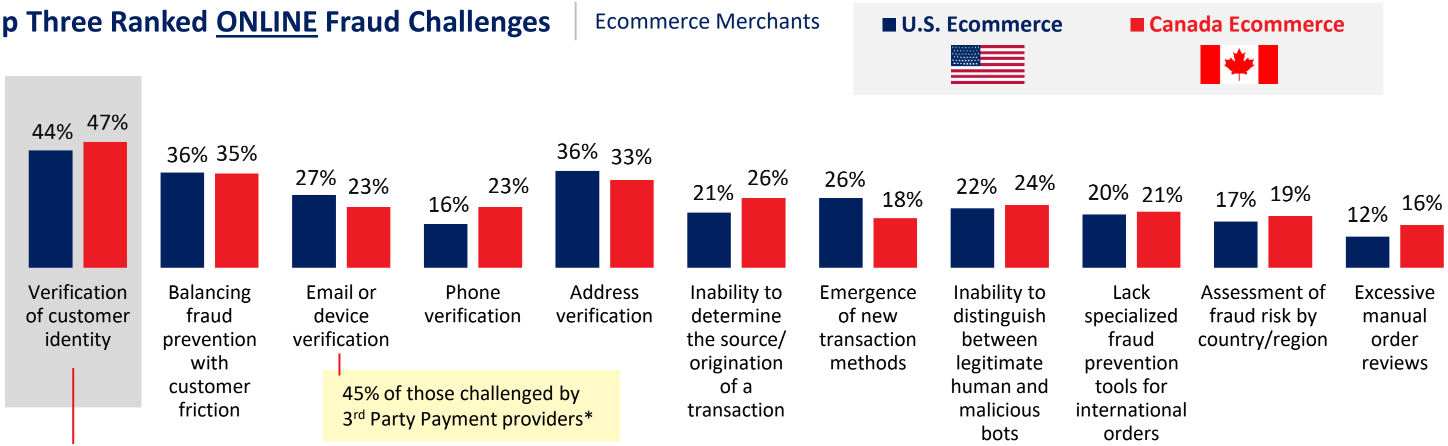
LexisNexis® RISK SOLUTIONS

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

U.S. and Canadian ecommerce merchants have similar top online challenges including identity verification, address verification and balancing fraud prevention with customer friction.

Synthetic identities, balancing speed of fraud detection with customer friction, limited real-time tracking and limited ability to determine order location are key barriers to identity verification.

Top Three Ranked ONLINE Fraud Challenges | Ecommerce Merchants



45% of those challenged by 3rd Party Payment providers*

Key barriers to identity verification

- Rise of synthetic identities (U.S. 37%, Canada 48%)
- Balancing fraud speed with customer friction (U.S. 54%, Canada 54%)
- Lack of real-time transaction solution (U.S. 50%, Canada 38%)
- Limited ability to determine order origination/location (U.S. 55%, Canada 39%)

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

— = significantly or directionally higher than other challenges within market

□ = significantly or directionally higher than same challenge in other markets

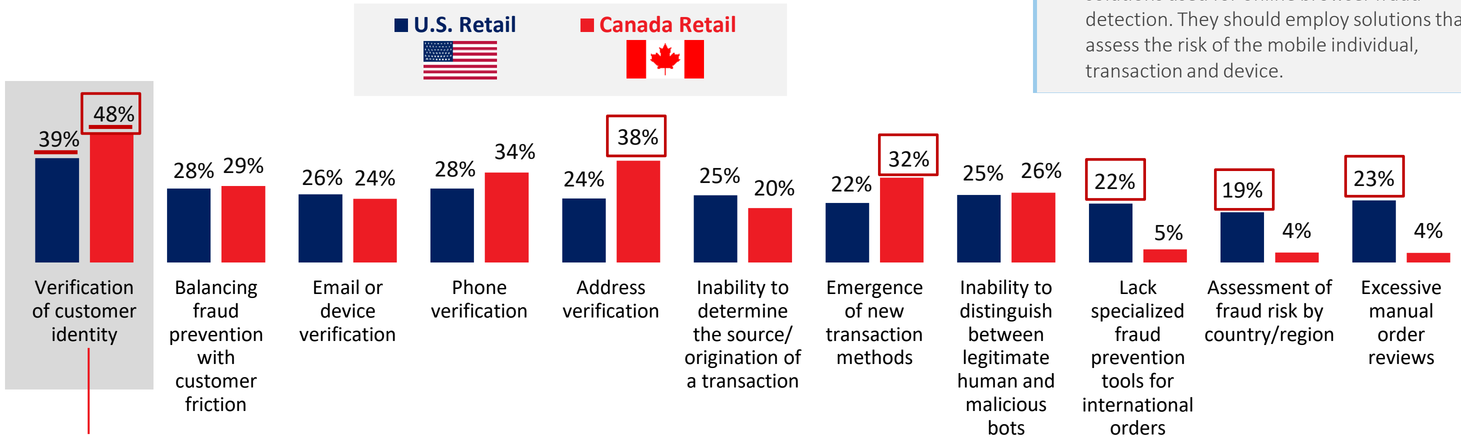
* Non-bank payment can involve a variety of different provider and systems types, such as Mobile and Internet Payment Systems (i.e. mobile wallets, peer-to-peer payments and social media payments), payment services providers (i.e., PayPal, Stripe, Amazon Payments, Authorize.net, etc.) and FinTech companies.

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

Identity verification is also the top mobile channel challenge for U.S. and Canadian retailers.

This is driven by a number of factors including the rise of synthetic identities, concerns about balancing fraud prevention with customer friction, lack of real-time transaction tracking and limited ability to determine order location.

Top Three Ranked MOBILE Fraud Challenges | Retail Merchants



Key barriers to identity verification

- Rise of synthetic identities (U.S. 46%, Canada 36%)
- Balancing fraud speed with customer friction (U.S. 48%, Canada 64%)
- Lack of real-time transaction solution (U.S. 49%, Canada 66%)
- Limited ability to determine order origination/location (U.S. 41%, Canada 44%)

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

▬ = significantly or directionally higher than other challenges within market

□ = significantly or directionally higher than same challenge in other markets

BEST PRACTICE

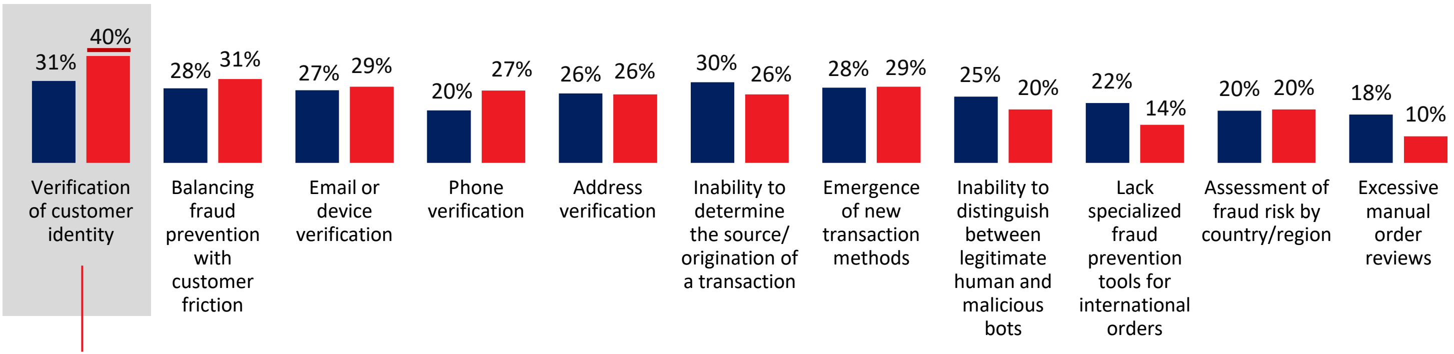
While online (desktop, laptop) and mobile channels are both digital, they are uniquely different regarding technology and fraud-related risks. SIM swaps and mobile malware are specific risks for mobile devices that can interfere with 2-factor authentication. For consumers, mobile = anywhere, anytime. That means challenges determining source origination, use of unsecure open WiFi and being “always logged in”; customers can be even more sensitive to friction with mobile transactions. Businesses that allow mcommerce should not rely on the same solutions used for online browser fraud detection. They should employ solutions that assess the risk of the mobile individual, transaction and device.

U.S. and Canadian ecommerce merchants battle a broader list of mobile channel challenges.

When asked to rank their top three, there was little consensus around the challenges tested.

Top Three Ranked MOBILE Fraud Challenges | Ecommerce Merchants

🟦 U.S. Retail 🟥 Canada Retail



Key barriers to identity verification

- Limited ability to determine order origination/location (U.S. 53%, Canada 54%)
- Rise of synthetic identities (U.S. 45%, Canada 64%)
- Balancing fraud speed with customer friction (U.S. 51%, Canada 36%)

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

▬ = significantly or directionally higher than other challenges within market

□ = significantly or directionally higher than same challenge in other markets

LexisNexis® RISK SOLUTIONS

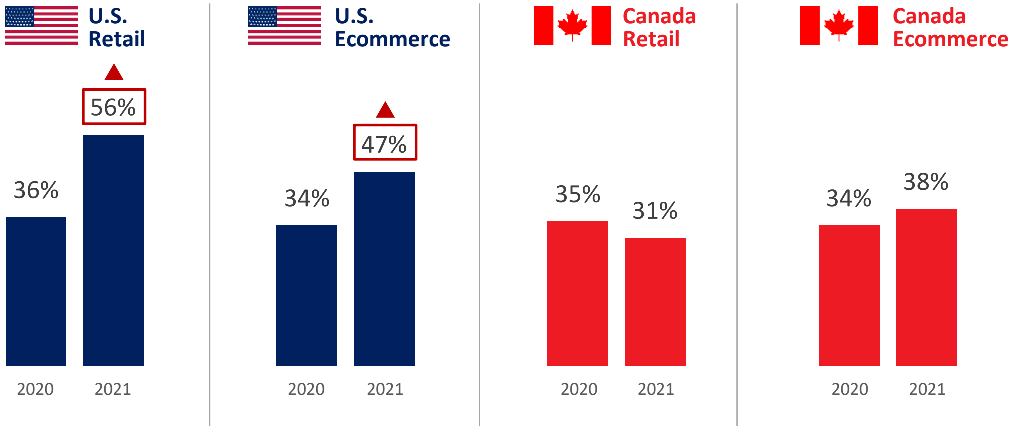
Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 **Challenges**
#4 Best Practices
#5 Best Practices in Use
Recommendations

Significantly more U.S. retail and ecommerce merchants are indicating that third party/non-bank payment providers are creating challenges for their fraud detection and prevention efforts.

Balancing speed, volume and customer friction is difficult, particularly where there is lack of consistency across payment applications, a high rate of false positives and difficulty determining transaction origination.

% Indicating Moderate-to-Significant Challenges with Third Party Payment Transactions*

Retail & Ecommerce Merchants



Survey Questions:
Q42: To what degree have non-bank payment service providers and systems created challenges to your fraud detection and prevention processes within the past year?

▼▲ = significantly or directionally higher/lower than previous period

□ = significantly or directionally higher than in other markets

KEY CHALLENGES

Key challenges for U.S. merchants by third party/ non-bank payment providers include (retail/ecommerce):

- Balancing speed of the transaction with customer friction (71%; 75%)
- Handling high volume of transactions at once (71%; 83%)
- Rate of false positive to review (71%; 73%)
- Lack of consistency across payment applications (75%; 76%)
- Lack of risk profile about the end customer (71%; 78%)
- Determining transaction origination (67%; 76%)

* 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.

LexisNexis RISK SOLUTIONS

KEY FINDING 04

As fraud becomes more complex, a best-practice approach for retail and ecommerce merchants is to use a multi-layered approach involving digital/transaction risk mitigation solutions that are integrated with cybersecurity and digital customer experience operations. This can also support concerns about optimizing risk detection while minimizing fraud.

Tracking fraud on various fronts is essential, including both the payment and transaction channel as well as both successful and prevented fraud attacks. Otherwise, not doing so can weaken fraud prevention efforts.

There has been an increase in the percentage of merchants which integrate their cybersecurity and digital customer experience operations with fraud prevention approaches.

Further, many are using cybersecurity alerts and social media intelligence as supportive capabilities. Just under half of U.S. retailers are also using AI/ML.

Fraud has become more complex; various risks can occur at the same time with no single solution. Fraud tools should 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

Best-practice approaches involve layering different solutions to address unique risks from different channels, payment methods and products. And go farther by integrating capabilities and operations with their fraud prevention efforts.

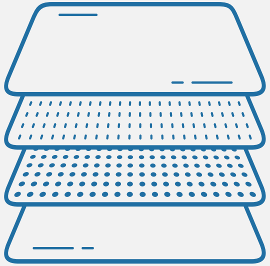
INTEGRATION

Tools & Capabilities with Fraud Prevention Approach

- Cybersecurity Alerts
- Social Media Intelligence
- AI/ML Models
- Crowdsourcing
- Cybersecurity Operations
- Digital/Customer Experience Operations

FRAUD DETECTION AND PREVENTION SOLUTION LAYERING

A multi-layered solution approach is essential to fighting fraud while mitigating customer friction



- Address both identity and transaction fraud risks
- Different challenges and risks for mobile versus online
- Different risks selling digital versus physical goods
- Botnets and malware can compromise mobile devices. Authenticate both the user device

STRATEGY & FOCUS

Minimizing Friction While Maximizing Fraud Protection

- Tracking successful and prevented fraud by both transaction channel and payment method
- Use of digital/passive authentication solutions to lessen customer effort (let solutions do the work behind the scenes)
- Assessing both the individual and transactional risk

Integration of cybersecurity and digital customer experience operations with fraud prevention approach

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 **Best Practices**
#5 Best Practices in Use
Recommendations

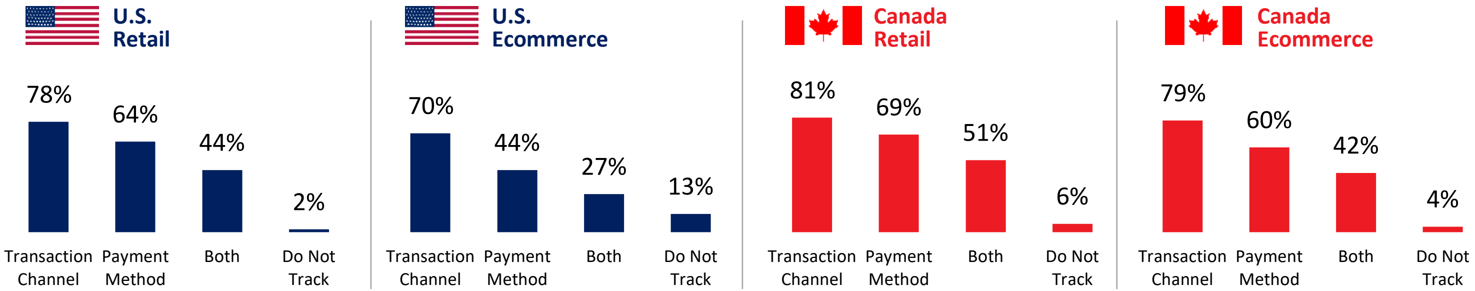
Tracking fraud costs by both transaction channel and payment method is essential to fraud prevention. Many track one or the other, but fewer track both.

Since fraud occurs in different ways depending on selling physical or digital goods and if using the mobile channel, this creates multiple endpoints and ways that fraudsters can attack. These fraudsters will continue to test for the weakest links and where they can operate undetected. Knowing where fraudsters have been successful is important for "plugging the gaps"; but also knowing where they've tried and failed is important in order to maintain vigilance.

U.S. ecommerce merchants are less likely to track fraud costs by payment method than others, at a time when new payment methods are being used by the changing consumer.

Survey Questions:
Q14a: Does your company track the cost of fraudulent transactions by payment channels or methods used?

% Businesses Tracking Fraud Costs by Channel and/or Payment Method | Retail & Ecommerce Merchants

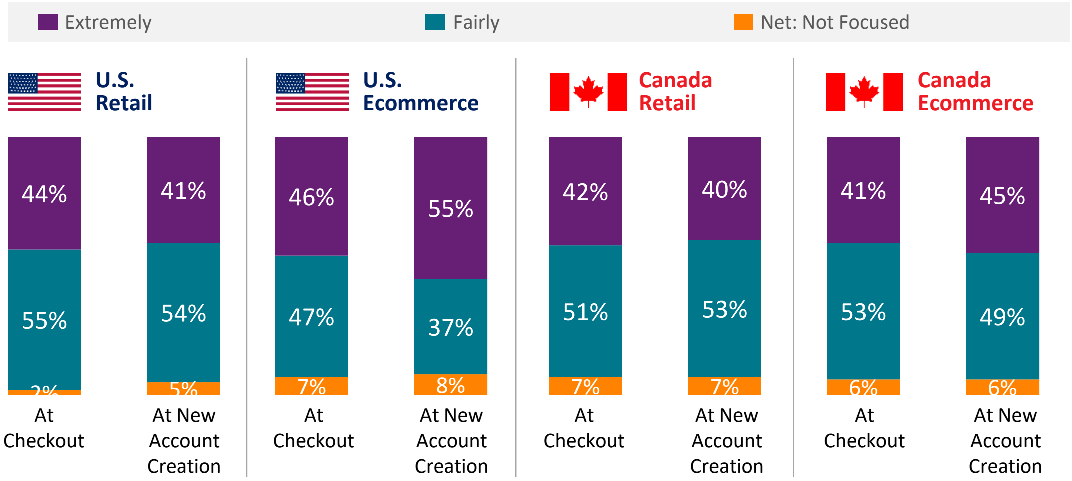


Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 **Best Practices**
#5 Best Practices in Use
Recommendations

For the most part, just under half of U.S. and Canadian merchants report that they are extremely focused on reducing customer friction by optimizing the risk-to-appropriate customer friction level.

Somewhat more U.S. ecommerce merchants are focused on this compared to others.

Degree of Focus on Optimizing Risk Level to Appropriate Customer Friction Level | Retail & Ecommerce Merchants



BEST PRACTICE

Friction is a concern. Reducing friction through layered approaches allow you to apply more or less identity authentication efforts based on the risk of the transaction. Not all transactions carry the same level of risk.

Survey Questions:
Q30. To what degree is your company focused on minimizing customer friction during an online or mobile channel transaction checkout? Q30a. To what degree is your company focused on minimizing customer friction when someone opens a new account online or through a mobile device?

* Asked of those with online and/or mobile channel translations; first asked in 2021

Key Finding 04

FRAUD DETECTION & PREVENTION APPROACHES

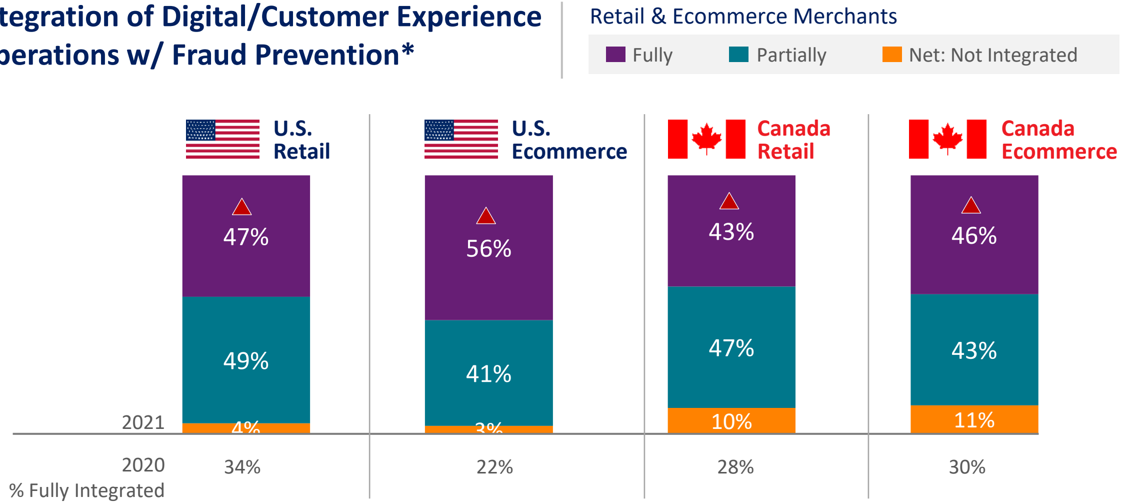
Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

There has been a significant increase in the percentage of merchants that integrate their digital/customer experience operations with fraud prevention. This is likely related to more remote transactions and driven by those seeking to optimize risk-to-customer friction levels.

U.S. ecommerce merchants have been most focused on this.

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

Retail & Ecommerce Merchants



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

▼▲ = significantly or directionally higher/lower than previous period

BEST PRACTICE

Merchants that are focusing on optimizing the risk level of the transaction to the appropriate customer friction level are more likely to integrate digital/ customer experience operations with fraud prevention.

% fully integrated which are also focused on optimizing risk-to-friction levels

- U.S. Retail (68%)
- U.S. Ecommerce (71%)
- Canada Retail (66%)
- Canada Ecommerce (63%)

LexisNexis® RISK SOLUTIONS

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

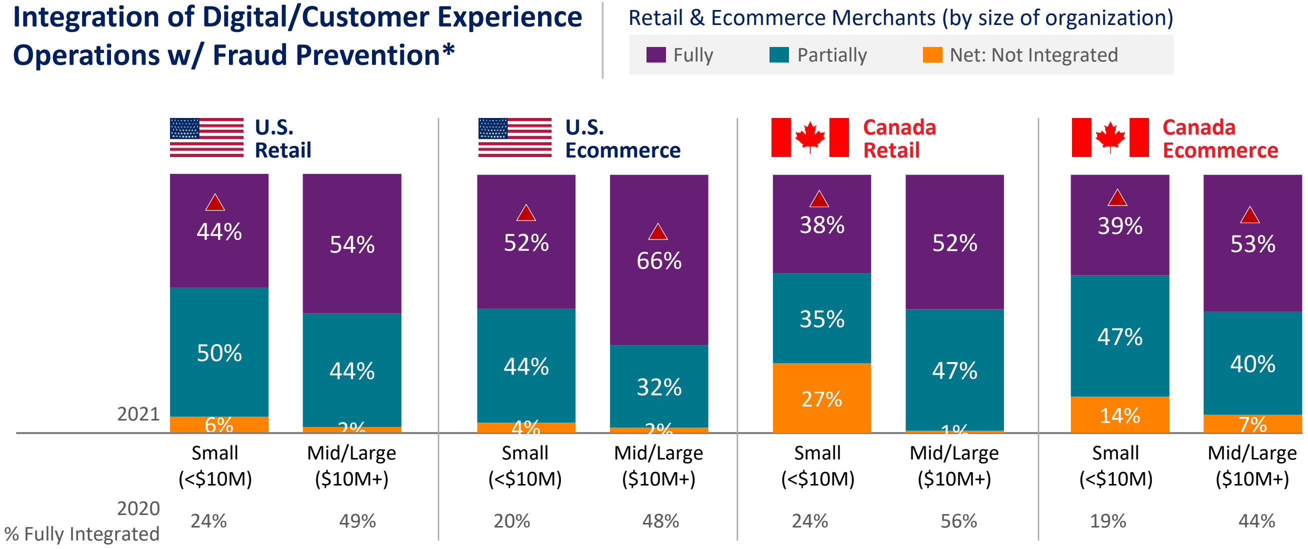
Much of the year-over-year growth in digital/customer experience and fraud prevention integration has come from smaller retailers and ecommerce merchants.

Smaller businesses also took a harder hit from the pandemic, especially when having to pivot to significantly more online/mobile traffic and make every customer transaction count in order to stay in-business.

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

▼▲ = significantly or directionally higher/lower than previous period

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



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

LexisNexis® RISK SOLUTIONS

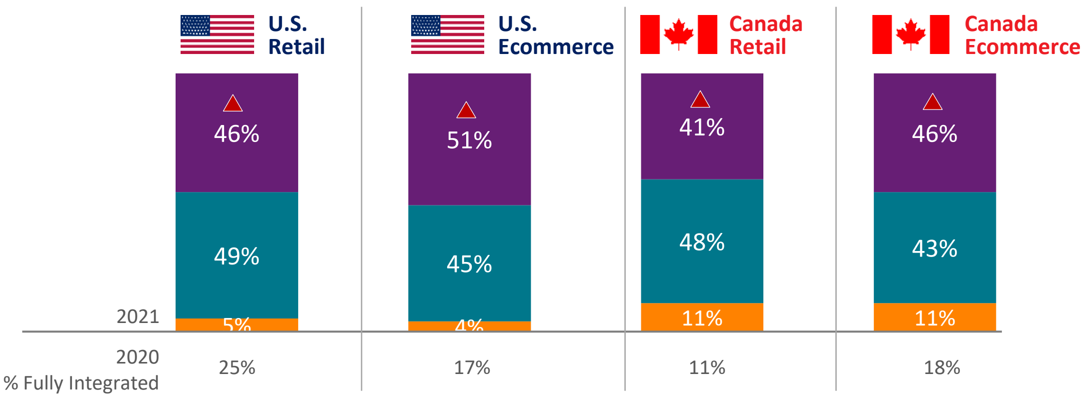
There has also been a significant increase in the percentage of U.S. and Canadian merchants that integrate their cybersecurity operations with fraud prevention.

Again, this is likely related to more remote transactions and driven by those seeking to optimize risk-to-customer friction levels.

Integration of Cybersecurity Operations w/ Fraud Prevention*

Retail & Ecommerce Merchants

🟪 Fully 🟦 Partially 🟧 Net: Not Integrated



Survey Questions:
Q29. To what degree has your company integrated its cybersecurity operations with its fraud prevention efforts?

▼▲ = significantly or directionally higher/lower than previous period

BEST PRACTICE

Merchants that are focusing on optimizing the risk level of the transaction to the appropriate customer friction level that risk are more likely to integrate cybersecurity operations with fraud prevention.

% fully integrated which are also focused on optimizing risk-to-friction levels

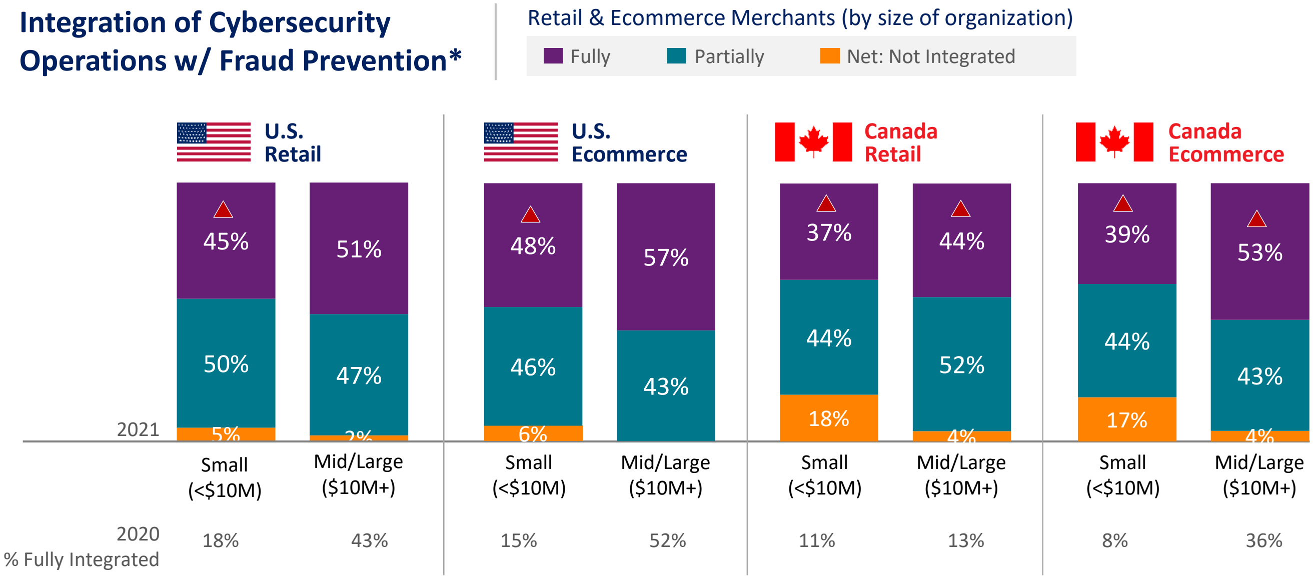
- U.S. Retail (67%)
- U.S. Ecommerce (64%)
- Canada Retail (70%)
- Canada Ecommerce (52%)

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

The increase of U.S. merchant cybersecurity operations and fraud prevention integration has also largely come from smaller businesses. It is occurring across business sizes for Canadian merchants.

For at least smaller merchants, this is a segment that has traditionally lagged with investment in fraud solutions and were likely harder hit from the pandemic.

Integration of Cybersecurity Operations w/ Fraud Prevention*



Survey Questions:
Q29. To what degree has your company integrated its cybersecurity operations with its fraud prevention efforts?

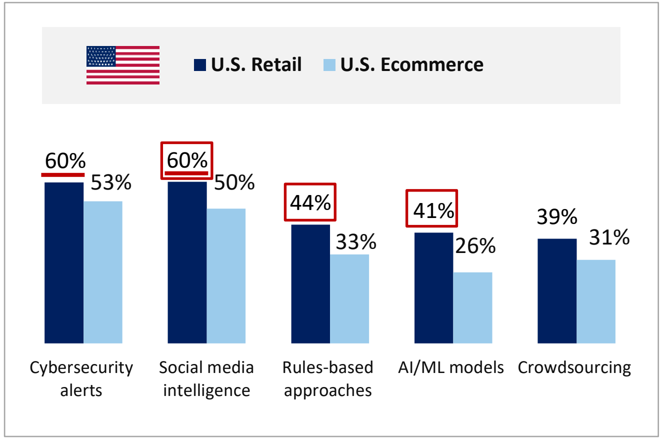
▼▲ = significantly or directionally higher/lower than previous period

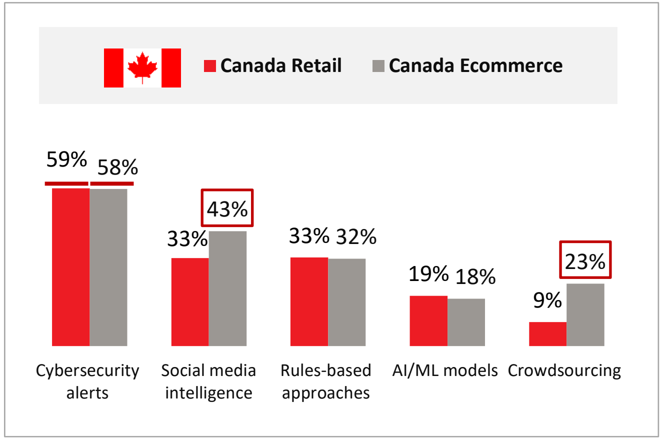
* Asked of those with online and/or mobile channel translations

Just over half of U.S. and Canadian merchants are using cybersecurity alerts to support fraud prevention, with more U.S. retailers also using additional fraud support capabilities.

In the U.S. market, there is broader use of these capabilities among retailers than ecommerce merchants.

% Using Supportive Capabilities to Fight Fraud | Retail & Ecommerce Merchants





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

— = significantly or directionally higher than other responses within market

□ = significantly or directionally higher than same response in other markets

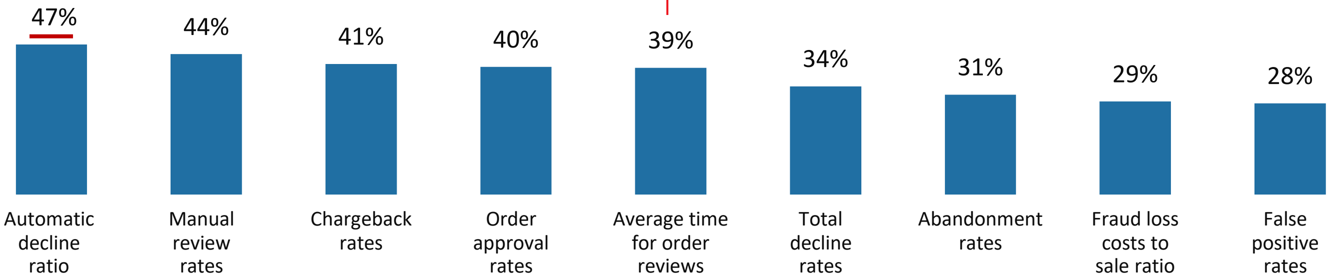
Fraud prevention performance metrics vary, but just under half of merchants are attentive to automatic decline ratios and manual review rates.

Merchants that say they are extremely focused on optimizing the risk-to-customer friction level are also monitoring the average time of transaction reviews.

Measuring Fraud Prevention Performance

Retail & Ecommerce Merchants

Those focused on optimizing risk-to-customer friction levels are more likely to also measure the average time for transaction review (44%) compared to others (34%)



Survey Questions:
Q12c: Which of the following metrics does your organization use to measure its performance with preventing fraud?

▬ = significantly or directionally higher than other responses

KEY FINDING 05

Retail and ecommerce merchants that use the best-practice approach can more effectively prevent fraud, optimize the risk-to-friction level with customers and lower their cost of fraud.

Merchants that are serious about optimizing fraud detection while minimizing customer friction are significantly more likely to be using a multi-layered solutions approach across different customer journey points.

This includes solutions that verify physical identity attributes, digital identity attributes and transaction risk in a seamless manner for customers.

While this tends to include the use of more solutions compared to those not following this best-practice approach, it is not necessarily the number which counts. Rather, it is the type of layering to unique risks presented by different transaction channels and payment methods.

As a result, findings show that these merchants have a lower cost of fraud and volume of successful attacks and fewer challenges associated with identity verification and minimizing customer friction.

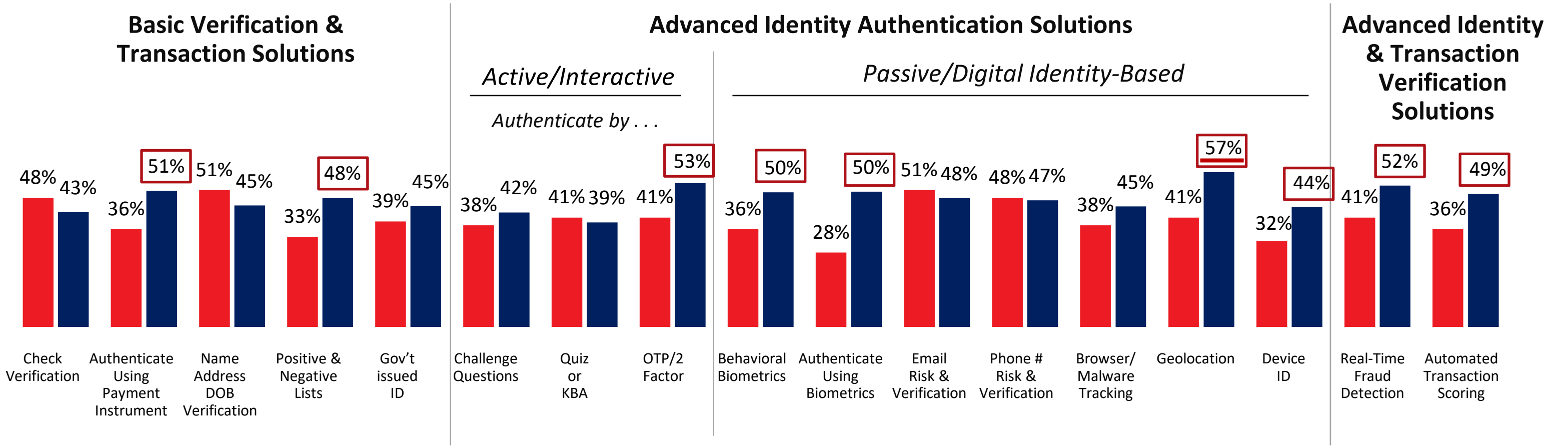
Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

U.S. retailers tend to use somewhat more solutions than Canadian retailers, including passive/digital identity-based solutions that are effective at detecting sophisticated fraud while minimizing customer friction.

These include those designed to assess both individual and device risks (e-mail risk verification, geolocation, device ID, biometrics and behavioral biometrics) and risk of the transaction (real-time fraud detection, automated transaction scoring), which provide fast, seamless and “behind the scenes” fraud detection that reduces customer efforts and delays while more effectively distinguishing synthetic identities and malicious bots.

Fraud Mitigation Solutions Use | Retail Merchants

🟥 Canada Retail ■ U.S. Retail



Avg. # Solutions (U.S. = 8; Canada = 5)

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

— = significantly or directionally higher than other responses within segment

□ = significantly or directionally higher than same response in other segment

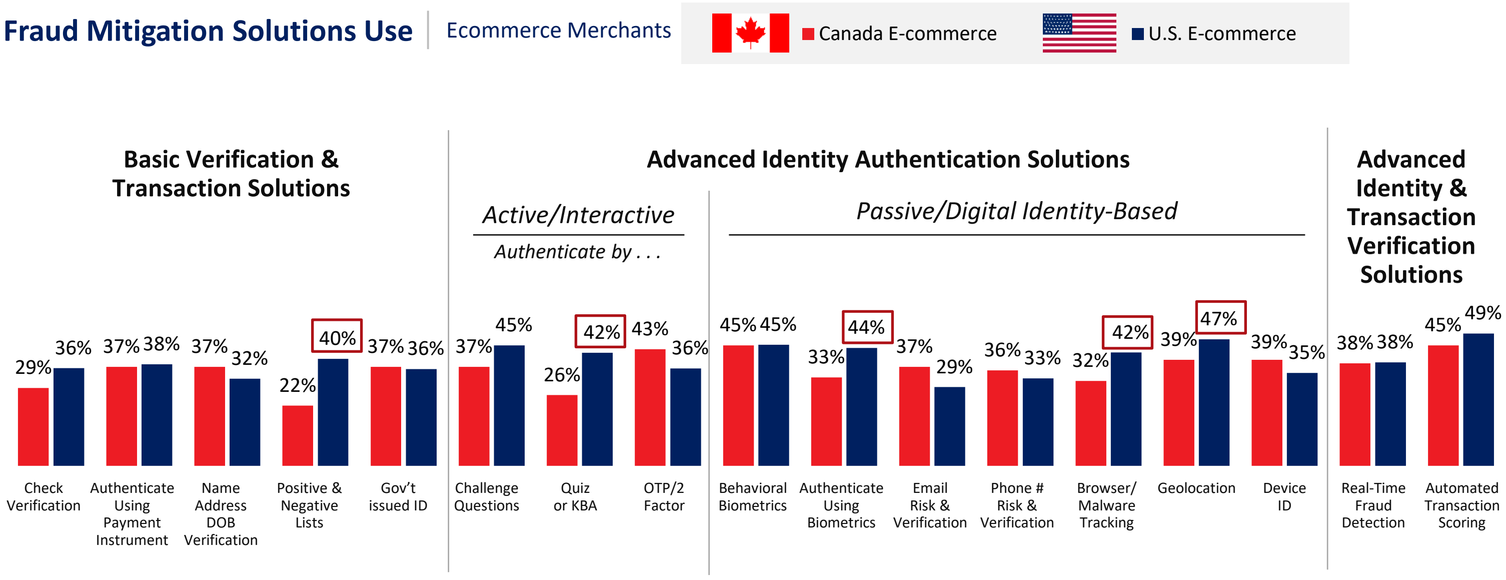
Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 **Best Practices in Use**
Recommendations

U.S and Canadian ecommerce solutions use is more limited compared to retailers. Use of passive/digital identity-based solutions is particularly low.

This may weaken their fraud detection and prevention efforts.

That said, there is investment in behavioral biometrics and automated transaction scoring among roughly half in each market.

Fraud Mitigation Solutions Use | Ecommerce Merchants



Avg. # Solutions (US = 6; Canada = 5)

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

— = significantly or directionally higher than other responses within segment

□ = significantly or directionally higher than same response in other segment

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

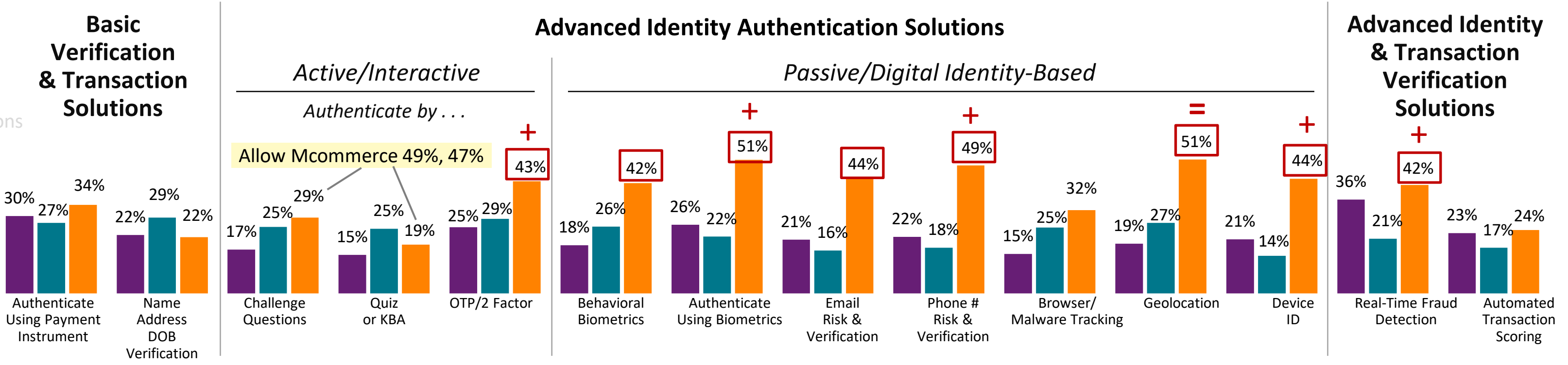
Merchants that are serious about balancing fraud risk assessment-to-customer friction at the point of sale use a multi-solution layered approach that integrates cybersecurity and digital customer experience operations.

This includes real-time fraud detection of the transaction and authenticating the physical attributes through interaction with the individual (challenge questions, 2 factor), along with digital identity-based solutions that work behind the scenes based on the assessed risk level.

Those that indicate being extremely focused on minimizing customer friction but don't follow this integration approach are not optimizing risk-to-friction levels balance; solutions use is limited and fragmented, similar to businesses which say they are not focused on balancing fraud detection and minimizing customer friction.

Fraud Mitigation Solutions Use | North America Retail & Ecommerce Merchants (U.S. & Canada Combined)

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



🟪 Not Focused on Optimal Risk-Friction Level (Not Cyber or DX Integrated) (Avg. 3 Solutions)
🟦 Extremely Focused on Optimal Risk-Friction Level (Not Cyber or Dx Integrated) (Avg 4 Solutions)
🟧 Extremely Focused on Optimal Risk-Friction Level + Cyber & DX Integrated (Avg 6 Solutions)

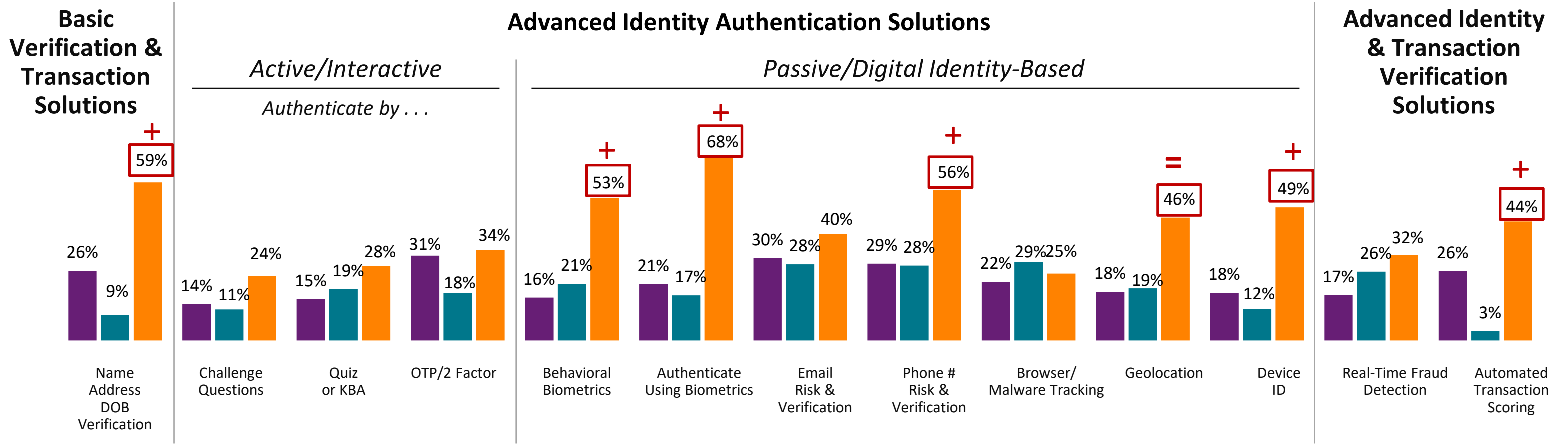
□ significantly or directionally higher than same response in other segment
+ used by many at this phase more than one or both other phases
= used by many across all journey phases

LexisNexis® RISK SOLUTIONS

A combination of physical attribute verification (name, address, DOB), automated transaction scoring, biometrics and digital device risk/verification solutions are best-practice solutions for optimizing risk-to-customer friction at new account creation.

Fraud Mitigation Solutions Use

North America Retail & Ecommerce Merchants (U.S. & Canada Combined)



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

- 🟪 Not Focused on Optimal Risk-Friction Level (Not Cyber or DX Integrated) (Avg. 3 Solutions)
- 🟦 Extremely Focused on Optimal Risk-Friction Level (Not Cyber or Dx Integrated) (Avg 4 Solutions)
- 🟧 Extremely Focused on Optimal Risk-Friction Level + Cyber & DX Integrated (Avg 7 Solutions)

□ significantly or directionally higher than same response in other segment
+ used by many at this phase more than one or both other phases
= used by many across all journey phases

LexisNexis® RISK SOLUTIONS

Customer Journey
Point of Sale
Account Creation
Account Login

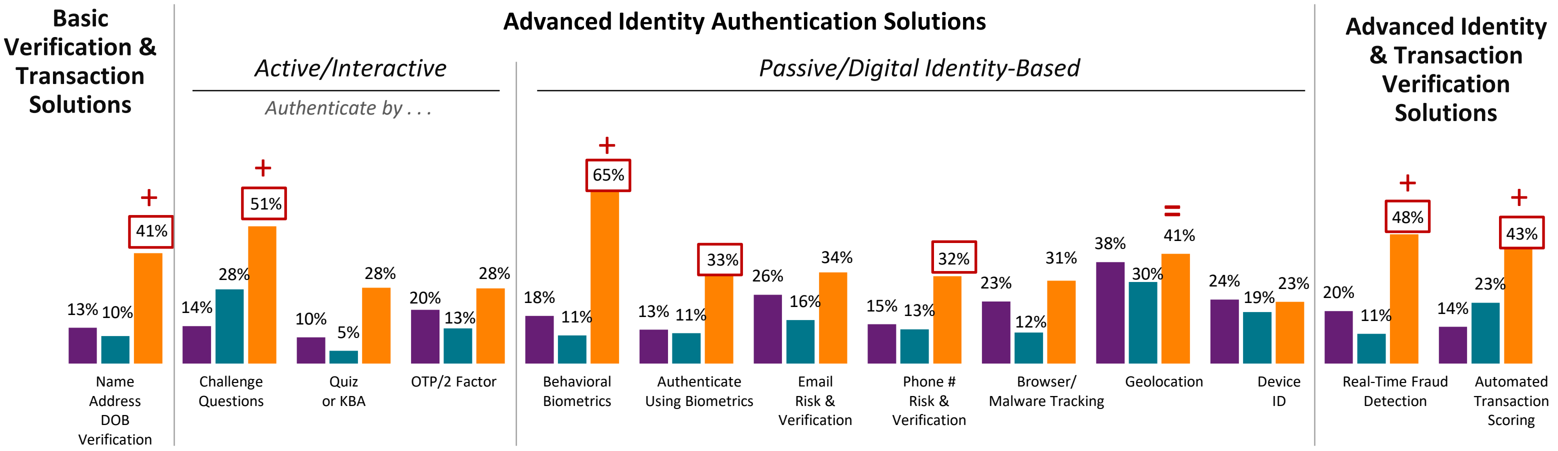
Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

Along with verifying physical attributes and transaction risk, behavioral biometrics is a best-practice solution at the account login phase of the customer journey.

This provides fraud detection/prevention teams with insights about the behavioral patterns, such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognizing normal user and fraudster behavior.

Fraud Mitigation Solutions Use

North America Retail & Ecommerce Merchants (U.S. & Canada Combined)



- ■ Not Focused on Optimal Risk-Friction Level (Not Cyber or DX Integrated) (Avg. 3 Solutions)
- ■ Extremely Focused on Optimal Risk-Friction Level (Not Cyber or Dx Integrated) (Avg 4 Solutions)
- ■ Extremely Focused on Optimal Risk-Friction Level + Cyber & DX Integrated (Avg 7 Solutions)

□ significantly or directionally higher than same response in other segment
+ used by many at this phase more than one or both other phases
= used by many across all journey phases

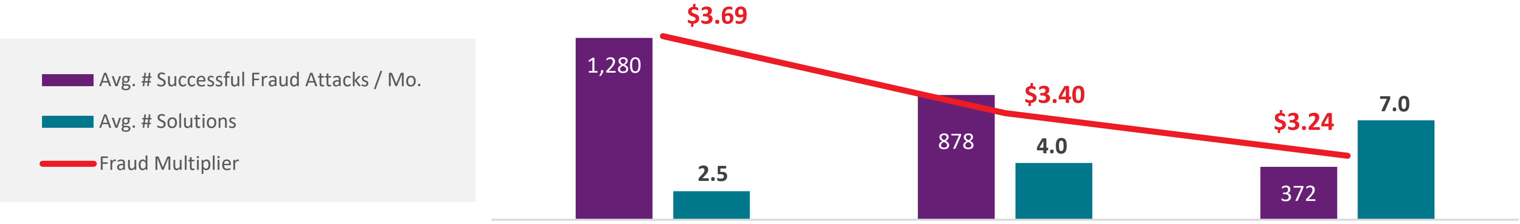
Survey Questions:
Q27: Which of the following fraud solutions does your company currently use?

LexisNexis® RISK SOLUTIONS

Key Finding 05
BEST PRACTICE RESULTS

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 **Best Practices in Use**

Study findings show that the cost of fraud and volume of successful attacks can be mitigated for merchants that invest in the best-practice multi-solutions layered approach which is integrated with cybersecurity and digital experience operations.



	Not Using Best-Practice Approach	Partially Using Best-Practice Approach	Fully Using Best-Practice Approach
Integration of Cybersecurity, Digital Experience with Fraud Ops	No	No	Yes
Focus on Optimizing Fraud Risk-to-Friction Levels	No	Yes	Yes
Solution(s) to verify physical attributes (e.g., name, DOB, address)	✓	✓	✓
Solution(s) to verify digital attributes (e.g., e-mail, phone # risk, biometrics)	Limited or None	Some Limited Use	✓
Solution(s) to assess device risk, location (e.g., device ID, geolocation)	Limited or None		✓
Solution(s) to assess behavior (e.g., behavioral biometrics, transaction risk)	Limited or None		✓

LexisNexis RISK SOLUTIONS

Best-Practice Multi-Layered Solution Approach: Those following a multi-layered solutions approach tend to use some combination of passive/digital identity-based solutions and those which assess physical identity attributes and transaction risk.

Retailers and ecommerce merchants that use the best-practice approach are also less likely to be challenged with digital identity authentication while balancing fraud prevention with customer friction.

This is particularly important as consumers increase their use of mobile transactions and payment methods.

% RANKING AS TOP ONLINE CHALLENGE			
Balancing fraud prevention with friction	**36%**	**41%**	**20%**
Distinguishing legitimate customer from bots	**35%**	**34%**	**9%**
E-mail risk & verification	**32%**	**49%**	**18%**

% RANKING AS TOP MOBILE CHALLENGE			
Identity verification	**39%**	**39%**	**21%**
Phone/e-mail risk & verification	**40% (phone)**	**39% (e-mail)**	**21% (e-mail)**
Balancing fraud prevention with friction	**30%**	**38%**	**10%**

USE OF BEST-PRACTICE APPROACH	NO	PARTIALLY	FULLY
Integration of cybersecurity, digital experience with fraud ops	No	No	Yes
Focus on optimizing fraud risk-to-friction levels	No	Yes	Yes
Solution(s) to verify physical attributes (e.g., name, DOB, address)	✓	✓	✓
Solution(s) to verify digital attributes (e.g., e-mail, phone # risk, biometrics)	Limited or none	Some limited use	✓
Solution(s) to assess device risk, location (e.g., device ID, geolocation)	Limited or none		✓
Solution(s) to assess behavior (e.g., behavioral biometrics, transaction risk)	Limited or none		✓

Best-Practice Multi-Layered Solution Approach: Those following a multi-layered solutions approach tend to use some combination of passive/digital identity-based solutions and those which assess physical identity attributes and transaction risk.

LexisNexis
RISK SOLUTIONS

RECOMMENDATIONS

Remain vigilant and prepared for increased fraud for the foreseeable future; couple this with a focus on minimizing customer friction in a competitive online/mobile channel environment.

Technology is key. Businesses need a robust fraud and security technology platform that helps them adapt to a changing digital environment.

A multi-layered solution approach is recommended. Single-point protection is no longer enough and results in single point of failure. A multi-layered, strong authentication defense approach is suggested.

Cybersecurity and digital customer experience operations should be integrated with fraud processes.

Seek industry alliances to share fraud insights and information. Businesses are likely fighting the same fraudsters.

Recommendation #1

REMAIN VIGILANT AND PREPARED FOR INCREASED FRAUD WHILE MINIMIZING CUSTOMER EFFORT

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

While parts of society are opening up since the start of the pandemic, the foreseeable future is unclear with regard to the new normal. It is reasonable to assume that **accelerated movement to online/mobile transactions and payments caused by the pandemic will remain a preference post-COVID**; therefore, businesses should continue to buildout and enhance the digital customer experience while protecting against fraud.

Fraudsters developed new skills and learnings during the pandemic, including merchants' and financial institutions' weak points with fraud detection. The identity and account-related data stolen during scams and phishing attempts of the past year will be used with synthetic identities and bot attacks on a more successful level where businesses continue to assess only the physical identity attributes and not the digital identity behaviors and transaction risks.

As more transactions move to the online and mobile channels, consumers have more options, including abandoning a transaction that is burdensome. Not every transaction carries the same level of risk; **businesses need intelligence to know when to apply more or less effort with customers.** New customers may appreciate the extra steps taken to verify their identity, such as challenge questions and one-time passcodes. Recurring customers may tire of this at some point based on the expectation that the business should know them.

A successful fraud detection and prevention approach involves an **integration of technology, cybersecurity and digital experience operations,** in a way that addresses the unique risks from different transaction channels and payment methods, as well as by individuals and types of transactions.

Recommendation #2
TECHNOLOGY IS KEY

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

To minimize fraud, reduce challenge rates, manual reviews and costs, organizations should **no longer rely on manual processes** with the assistance of limited technologies.

Businesses need a **robust fraud and security technology platform** that helps them adapt to a changing digital environment, offering strong fraud management and resulting in a risk appropriate friction experience.

Deploying technologies, which can recognize customers, pinpoint fraud and build the fraud knowledge base to streamline on-boarding, can help **prevent account takeovers and detect insider threats.**

Using valuable data attributes like users' login from multiple devices, locations and channels is essential for identifying risks.

Enabling **integrated forensics, case management and business intelligence** can help to improve productivity.

Recommendation #3

A MULTI-LAYERED SOLUTION APPROACH IS REQUIRED

Overview
Key Findings
#1 Attacks & Costs
#2 Trends
#3 Challenges
#4 Best Practices
#5 Best Practices in Use
Recommendations

Single-point protection may no longer be enough and may result in single point of failure.

As consumers transact across locations, devices and geographies, user behaviors, such as transaction patterns, payment amounts and payment beneficiaries, are **becoming more varied and less predictable.**

A multi-layered, strong authentication defense approach is recommended. This includes a single authentication decision platform that incorporates real-time event data, third-party signals and global, cross-channel intelligence.

Also recommended is the ability to **examine malware level threats, bot and remote access Trojan and IP spoofing** detection across web and mobile channels.

At the same time, the ability to **provide behavioral analytics and reduce false positives and customer friction is key.**

Recommendation #4

CYBERSECURITY AND DIGITAL CUSTOMER EXPERIENCE OPERATIONS MUST BE INTEGRATED WITH YOUR FRAUD PROCESSES

Improve decisions and the customer experience with **machine learning and an integration of systems/resources** that manage risk across the business and all endpoints—risk convergence.

Enhanced data and analytic capabilities from tools such as **AI/ML, cyber alerts, social media intelligence and crowdsourcing** lets businesses predict threats rather than react to them.

Integrating these tools with **digital identity-based solutions** provides protection across the customer journey, not just at the point of transaction; most fraudsters prefer account-related takeovers/creation because this provides an ongoing source of assets instead of a one-time transaction.

Combined, the above can provide efficiencies and cost savings, as well as ensuring an optimized customer experience, particularly where fraud risks can be segmented so that security controls can be adjusted upwards or downwards based on the transaction.

LexisNexis RISK SOLUTIONS

Recommendation #5

SEEK INDUSTRY ALLIANCES FOR INFORMATION SHARING

Organizations are likely fighting against the same group of fraudsters. In fact, **fraud patterns and risks share many similarities across industries and geographies.**

Building an **industry-specific alliance that exchanges important** information can keep members up-to-speed on industry fraud patterns and tactics, complementing their own intelligence and allowing them to more accurately identify and track at-risk individuals and devices. Such information can include:

- Historic blacklisted devices
- Mule accounts and associated fraud strategies
- Specific risks pertaining to industry/use case/geography

LexisNexis® Risk Solutions can help

For more information

💻 risk.lexisnexis.com/tcof

📱 800.953.2877
408.200.5755

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products identified. LexisNexis does not warrant this document is complete or error free. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. LexisNexis Fraud Multiplier is a trade mark of RELX Inc. True Cost of Fraud is a trademark of LexisNexis Risk Solutions Inc.