

# The LexisNexis® Thirteenth Annual True Cost of Fraud™ Study *for Ecommerce and Retail*

*U.S. & Canada Edition*



Overview



Key Findings



#1

Transaction Trends



#2

Fraud Attacks &  
Losses

#3

The Customer  
Journey

#4

Robust Practices



Recommendations

## The LexisNexis® True Cost of Fraud™ Study for Ecommerce and Retail 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.

### Pandemic Impact:

- Data collection occurred during November – December 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 the continued pandemic, 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



Overview



Key Findings



#1

Transaction Trends



#2

Fraud Attacks &  
Losses

#3

The Customer  
Journey

#4

Robust Practices



Recommendations

The study included an extensive survey of 800 risk and fraud executives in retail and ecommerce companies in the U.S. (698) and Canada (102).

### Retailers and Ecommerce Merchants Include a Variety of Categories:

# of Survey  
Completions  
**800**



### Segments

Segment  
definitions:



Small

Earns less than \$10 million in  
annual revenues



Mid/Large

Earns  
\$10 million+ in annual  
revenues

# of Survey  
Completions

450

350



Overview



Key Findings



#1

Transaction Trends



#2

Fraud Attacks &  
Losses

#3

The Customer  
Journey

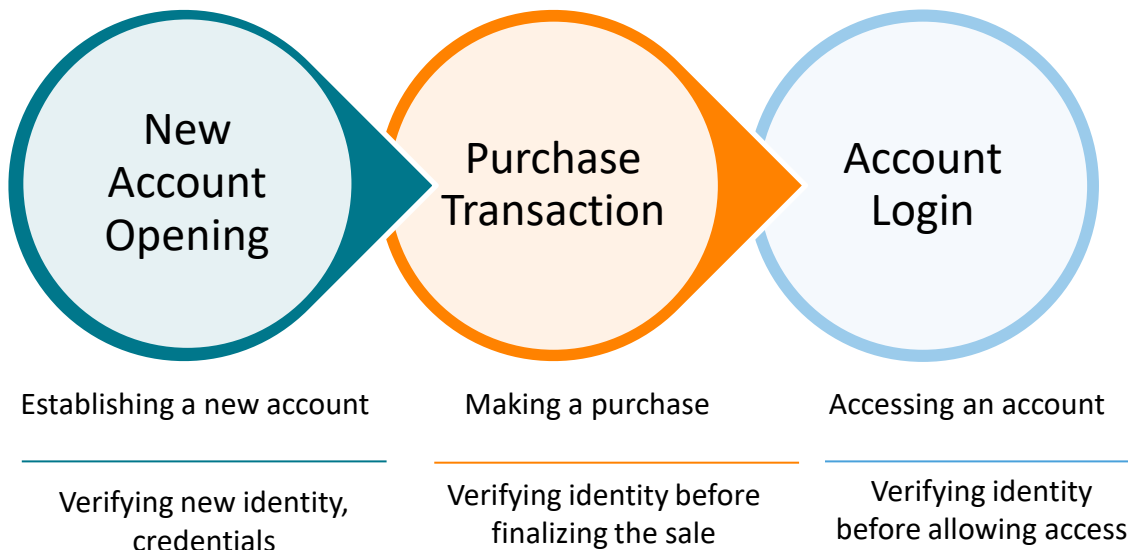
#4

Robust Practices



Recommendations

**For the True Cost of Fraud™ Study, the customer journey is defined as follows:**





## Overview

**01 Mobile channel use continues to grow as a transformation is occurring with mobile commerce.** More retailers and ecommerce merchants have implemented mobile channel transactions since the start of the pandemic in order to meet changing consumer behaviors and preferences. This includes through mobile apps and alternative payment methods that seek to enhance the customer experience.



## Key Findings

**02 The cost and volume of fraud is up and mobile commerce is driving it.** The LexisNexis Fraud Multiplier™ has increased double digits for U.S. and Canadian merchants since before or at the start of the pandemic. The year-over-year increased volume of attacks is experienced by those which adopt mobile commerce, while it is relatively unchanged among those who don't. This aligns to an increase in the percentage of fraud costs attributed to the mobile channel, particularly among ecommerce merchants.



## Transaction Trends

**03 Fraud is occurring across the customer journey, though the account login phase is at-risk for a number of merchants with regard to takeovers and breaches.** Identity-related fraud attributed to the account creation and login journey phases has increased year-over-year. Merchants tend to focus more on account creation and in-person transactions even though fraud costs attributed to account logins/compromises are fairly similar to these other journey points. And fewer solutions designed to increase identity verification effectiveness are being used at the account login phase, even though fraud is on the rise at this stage.



## Fraud Attacks &amp; Losses



## The Customer Journey



## Robust Practices

**04 Robust practice fraud detection and prevention includes a multi-layered solution approach unique to different customer journey phases, which assesses the risks and behaviors within the digital channels and the integration of fraud prevention with cybersecurity operations and the digital customer experience.** Layering in supportive capabilities such as social media intelligence and AI/ML further strengthens fraud prevention. Study findings show that firms which follow this approach are less likely to be challenged with identity verification, botnet attacks and optimizing fraud detection/risk levels with the customer experience. They also experience fewer successful fraud attacks per month and realize a lower cost of fraud.



## Recommendations

# KEY FINDING 01

Mobile channel use continues to grow as a transformation is occurring with mobile commerce.

More retailers and ecommerce merchants have implemented mobile channel transactions since the start of the pandemic in order to meet changing consumer behaviors and preferences.

- Merchants are seeking to meet mobile app and alternative payment preferences.
- Mobile wallets, Buy-Now-Pay-Later (BNPL) and social media payment methods are being offered to enhance the customer experience.
- Many merchants follow a mobile-first strategy of designing the shopping experience around mobile and then adapting that to the web experience.



## More ecommerce merchants, as well as Canadian retailers, are recognizing the need for adopting mobile commerce since the pandemic began.

This continues an upward trend in mobile commerce adoption overall, but particularly among Canadian merchants as demand has grown among more Canadian consumers – particularly Millennials. This has been accompanied by growth in mobile payments through increased mobile apps availability and digital marketing through social media.<sup>1</sup>

Overview

Key Findings

#1 Transaction Trends

#2 Fraud Attacks &amp; Losses

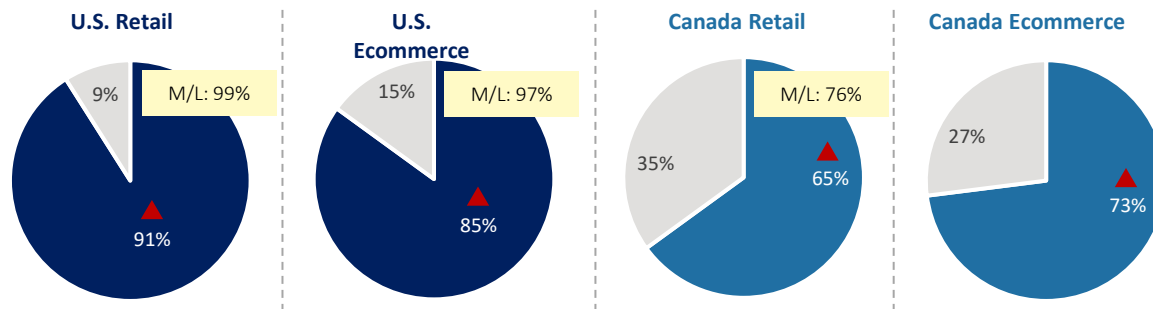
#3 The Customer Journey

#4 Robust Practices

Recommendations

### Businesses Offering Mobile Commerce | Retail & Ecommerce Merchants

■ Adopt mobile commerce  
■ Do not adopt mobile commerce



% Offering  
Mobile Commerce

2021	83%	69%	42%	50%
2020	43%	34%	23%	25%
2019	48%	23%	N.A.	N.A.

<sup>1</sup> <https://www.trade.gov/country-commercial-guides/canada-ecommerce>

#### Survey Questions:

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

Q6: Is your company considering accepting mobile transactions over the next 12 months?

▲ = significantly or directionally higher/lower than previous period

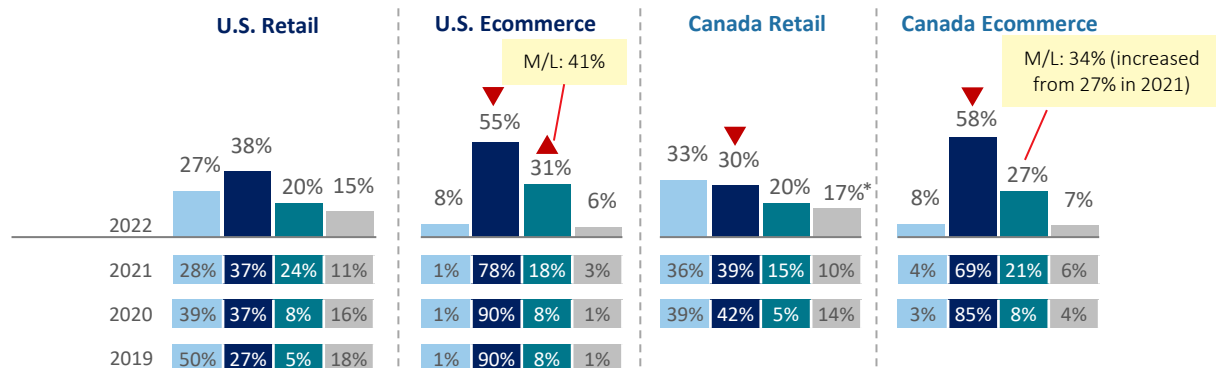
# U.S. and Canadian consumers are continuing to conduct more mobile transactions, with a significant increase among ecommerce shoppers.


There is also some expansion of channels among ecommerce merchants. While representing a small percentage of volume, there is a directional uptick and emergence of in-person transactions reported by ecommerce merchants. As a select few ecommerce giants began opening a limited number of bricks and mortar locations (“clicks to bricks”) as early as 2018<sup>2</sup>, more – across merchant size – have done this during the past year in order to compete through a multi-channel approach, with a focus on the customer experience for those who prefer the touch/feel of an in-store experience and to position their brand everywhere that customers shop.<sup>3</sup>

## % Transaction Volume by Channel

### Retail & Ecommerce Merchants

 In-Person  
 Mobile  
 Online  
 Call Center



 = significantly or directionally higher/lower than previous period

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.

<sup>2</sup> Ecommerce and Physical Stores How Do They Stack Up <https://www.tecsys.com/blog/2018/12/ecommerce-and-physical-stores-how-do-they-stack-up/>

<sup>3</sup> 11 DTC Brands Opening Physical Retail Stores in 2021; <https://www.shopify.com/retail/dtc-to-brick-and-mortar>

\* 6% Other (kiosk, mail)



# A transformation is occurring within mobile commerce, with mobile browsing preference declining in favor of mobile apps and alternative payment options.

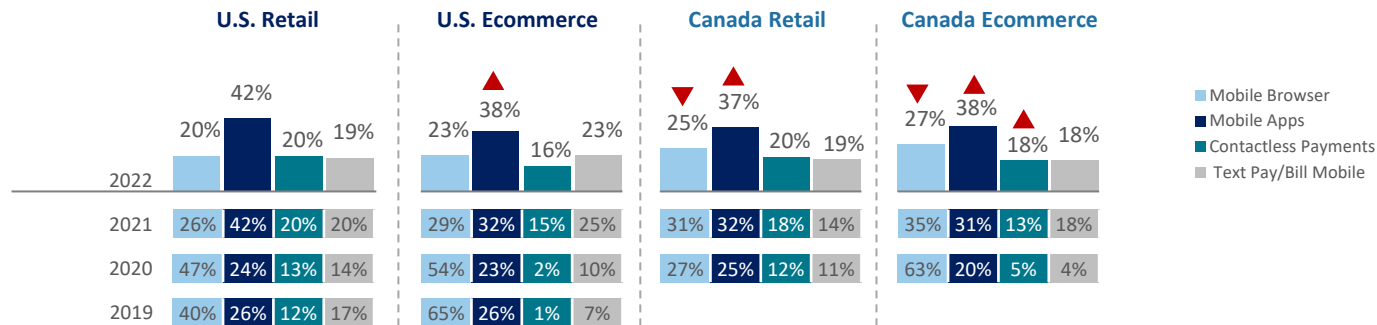
On the face of it, this is a trend since at least the start of the pandemic in 2020, as part of the wider digital transformation. But there are more fundamental shifts driving the mobile commerce transformation.

- Growth is driven in part by consumer experience preference. Mobile apps provide a more enhanced user experience by being scaled to the device, whereas using a browser via a mobile device can result in sites not optimized for this channel (e.g., small font sizes, fewer page options, more crowded space).
- Newer payment methods, such as Buy-Now-Pay-Later (BNPL), support both the consumer shopping and payment experience needs.
- Mobile apps support an omnichannel strategy through access to in-store benefits and loyalty programs.<sup>4</sup>
- And, the strategy of mobile-first is followed by many retail merchants, whereby the remote shopping experience is designed around the mobile transaction first and then adapted to online web browsers.<sup>5</sup>

## % Transaction Volume by Mobile Channel



Retail &amp; Ecommerce Merchants



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

<sup>4</sup> <https://www.alistdaily.com/digital/app-annie-mobile-shopping-to-increase-20-percent-year-over-year/>

<sup>5</sup> *The Mobile-first Enterprise Report*; AppsFlyer, February 2022; <https://www.appsflyer.com/resources/reports/mobile-first-enterprise-retail/>

# Not surprisingly, alternative payment methods continue to grow, with mobile wallets leading among U.S. ecommerce and growing among Canadian retailers. Directionally, there is an upward tick with virtual payments as well.

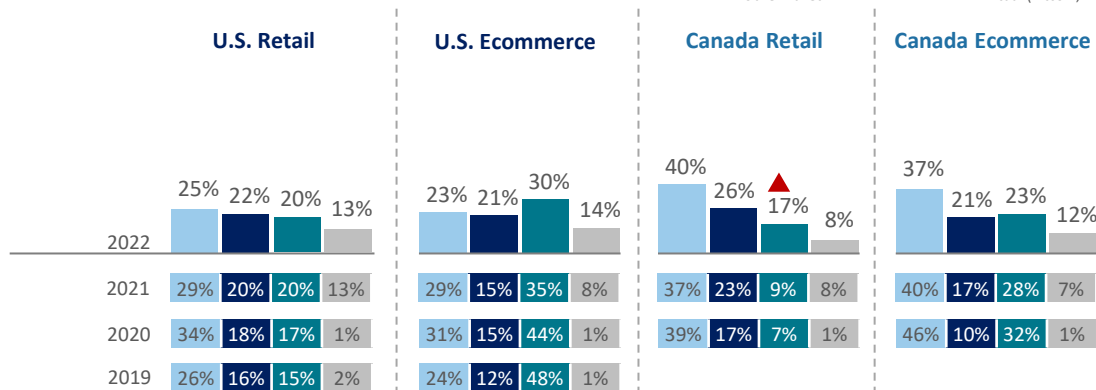
The actual transaction volume of alternative payment methods could be higher than the report level when combining various types of emerging methods, including Buy-Now-Pay-Later (BNPL), social media payments and various mobile/digital wallets. At present, the distinction between these, in terms of specific categories, may not be fully clear to survey respondents. The 2021 holiday season saw a reported 20% YOY increase in BNPL installments alone.<sup>6</sup>

## % Transaction Volume by Payment Method



### Retail & Ecommerce Merchants

Credit Card  
 Debit Card  
 Mobile Wallet  
 Virtual (Bitcoin, FB Pay, etc.)



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

# KEY FINDING 02

The cost and volume of fraud is up and mobile commerce is driving it.

The cost of fraud for U.S. merchants has increased by 19.8% since 2019, from 3.13 to 3.75 times the lost transaction value. And it continues to be above the early 2020 pandemic level as well (3.36). A similar trend follows for Canadian merchants, up 11.1% since early 2020, from 2.87 to 3.19.

Ecommerce merchants have the highest LexisNexis Fraud Multiplier™ of 3.85 and 3.45 for U.S. and Canada, respectively.

The mobile channel is driving the increase in fraud attacks. Year-over-year changes in average monthly attack volume is relatively unchanged for those that don't adopt mobile commerce, while it is significantly up among those which do offer it.

Retailers and ecommerce merchants indicate that fraudsters are targeting the mobile channel. This aligns with an increase in the cost of fraud attributed to mobile transactions, particularly among ecommerce merchants.

## The volume of fraud attacks continues to increase significantly from pre- and early-pandemic periods.

Ecommerce merchants and Canadian retailers have experienced the most significant increases during this period, with successful attacks being higher for mid/large businesses.

These are the segments where mobile commerce has grown quickly.

Overview

Key Findings

Transaction Trends

Fraud Attacks & Losses

The Customer Journey

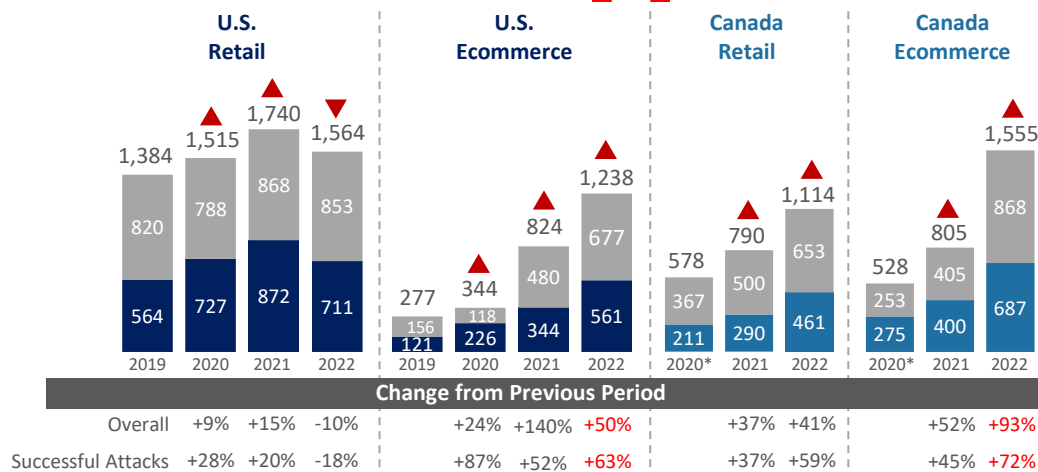
Robust Practices

Recommendations

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?

### Average Monthly Fraud Attacks Retail & Ecommerce Merchants

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



### SEGMENT HIGHLIGHTS

Mid/Large average **successful** attacks per month:

- ML Retail (U.S.) (835)
- ML Ecommerce (U.S.) (933)
- ML Retail (Canada) (675)
- ML Ecommerce (Canada) (1208, from 506 in 2021)

## These increased attacks are being driven by growth of mobile transactions.

The year-over-year change in average attack levels per month is relatively unchanged among those that have few transactions through the mobile channel. The significant increases are coming from merchants that have a sizeable amount (nearly half or more) of transactions through this channel.

And the volume of attacks is significantly higher for merchants with heavy mobile transaction volume.



Overview



Key Findings



Transaction Trends



Fraud Attacks &amp; Losses



The Customer Journey



Robust Practices



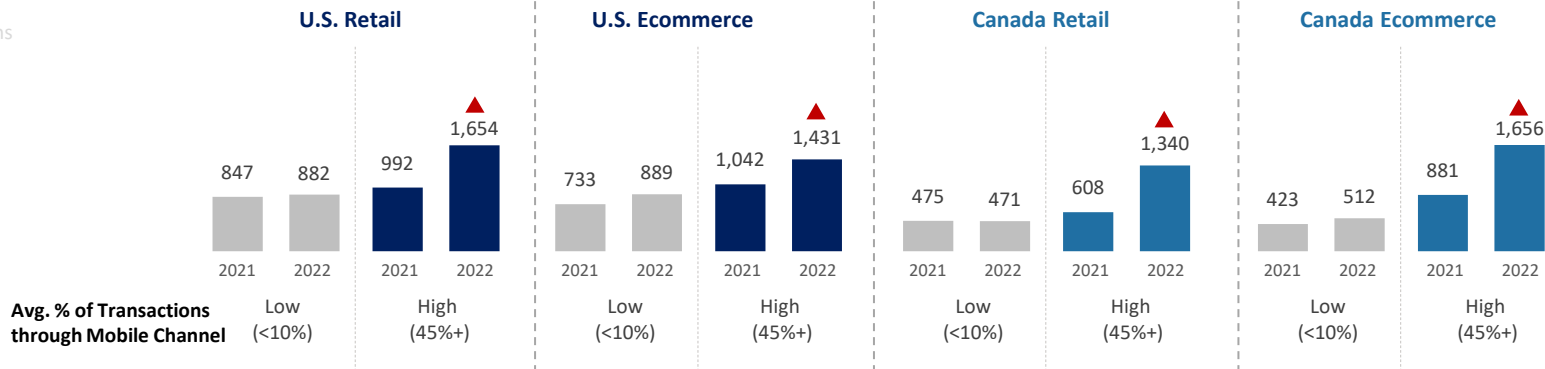
Recommendations

### Average Monthly Fraud Attacks



Retail &amp; Ecommerce Merchants

*Increases Driven by Mobile Transactions*



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



Transaction Trends



Fraud Attacks & Losses



The Customer Journey



Robust Practices



Recommendations

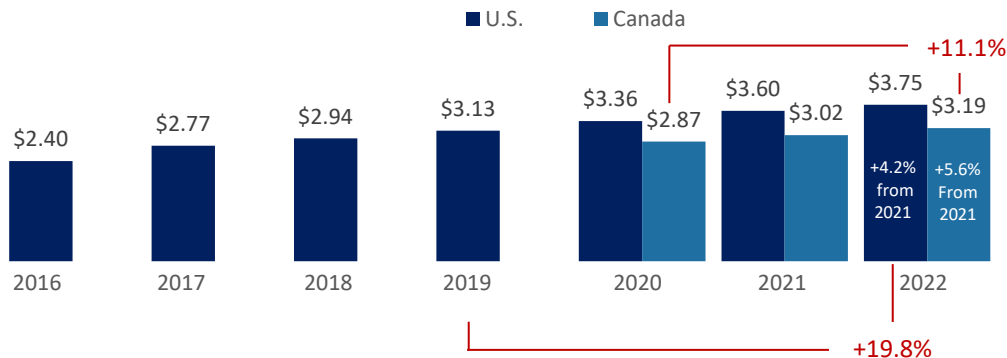
Survey Question:  
Q16a: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.

## As fraud volume increases, so too does the cost of fraud. The LexisNexis Fraud Multiplier™ has risen by double-digits for North America since before the pandemic, particularly for U.S. merchants.

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 pandemic.

Ecommerce merchants continue to experience higher costs of fraud during the pandemic.

### Cost of Fraud: LexisNexis Fraud Multiplier™



### SEGMENT HIGHLIGHTS

Ecommerce merchants have higher fraud costs.

- Every \$1 of fraud costs Canadian ecommerce merchants \$3.45 (up 17.8% from pre-pandemic \$2.93)
- U.S. ecommerce merchants continue to have the highest cost, where every \$1 of fraud costs these merchants \$3.85

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

The pandemic heightened, accelerated the above, along with the digital transformation



## U.S. retailers and ecommerce merchants are getting hit the hardest by malicious bot attacks.

Forty-percent of U.S. retailers say that they've experienced an increase in these attacks over the past 12 months, more so compared to other segments. U.S. ecommerce merchants report a significantly higher percent of their transactions being malicious bot attacks compared to others.

Overview

Key Findings

Transaction Trends

Fraud Attacks &amp; Losses

The Customer Journey

Robust Practices

Recommendations

### Malicious Bot Attacks – Trends



Retail &amp; Ecommerce Merchants

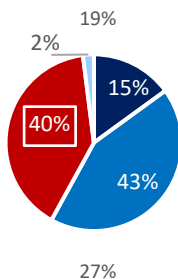
■ Decreased ■ Remained the same ■ Increased ■ Not sure

% of transactions that are malicious bot attacks

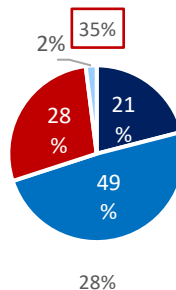
Compared to 12 months ago, monthly malicious bot attacks have...

Average % increase of monthly malicious bot attacks

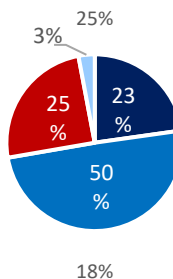
#### U.S. Retail



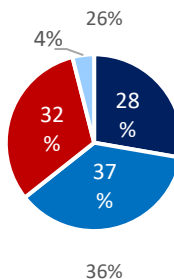
#### U.S. Ecommerce



#### Canada Retail



#### Canada Ecommerce



#### Survey Questions:

B1a: In a typical month, what percent of your transactions are determined to be malicious automated bot attacks? B1b: (ASK IF DID NOT ANSWER "NOT SURE" IN B1A) How does this compare to the same time last year? B1c: (ASK IF "INCREASED" IN B1B) By how much has the percent of monthly automated malicious bot attacks increased over the past year?

## As mobile transaction volume grows, fraudsters are increasingly targeting this channel.

Many Canadian ecommerce merchants have only recently expanded into the mobile channel and are reporting higher percentage of fraud increases targeting these transactions. This demonstrates that fraudsters actively seek out and test new opportunities.

Overview

Key Findings

Transaction Trends

Fraud Attacks &amp; Losses

The Customer Journey

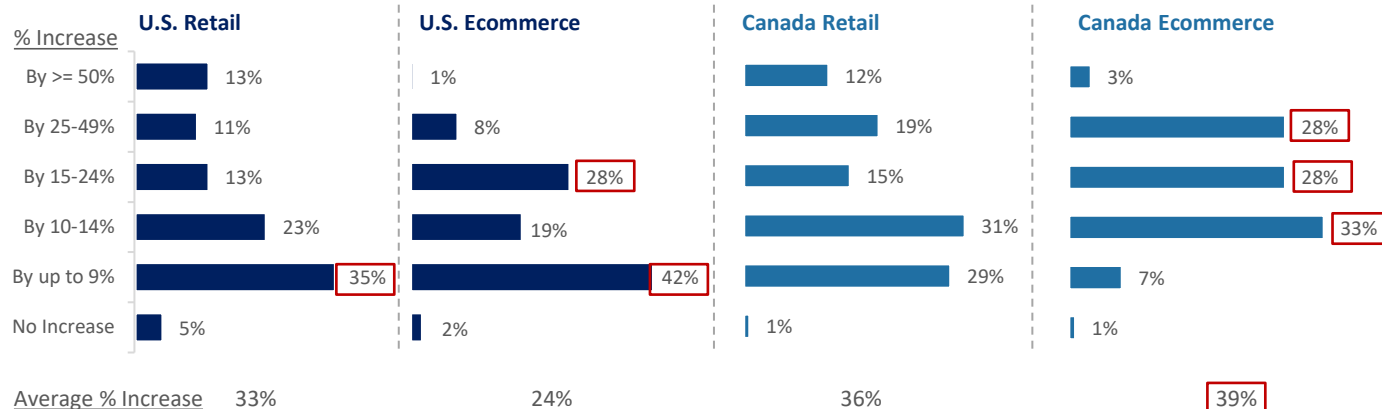
Robust Practices

Recommendations

### % Fraud Increase in Mobile Channel Transactions



Retail &amp; Ecommerce Merchants



Survey Questions:  
Q17b: To what degree has fraud that targets your mobile channel transactions increased during the past 12 months?

   = significantly or directionally higher than other segments

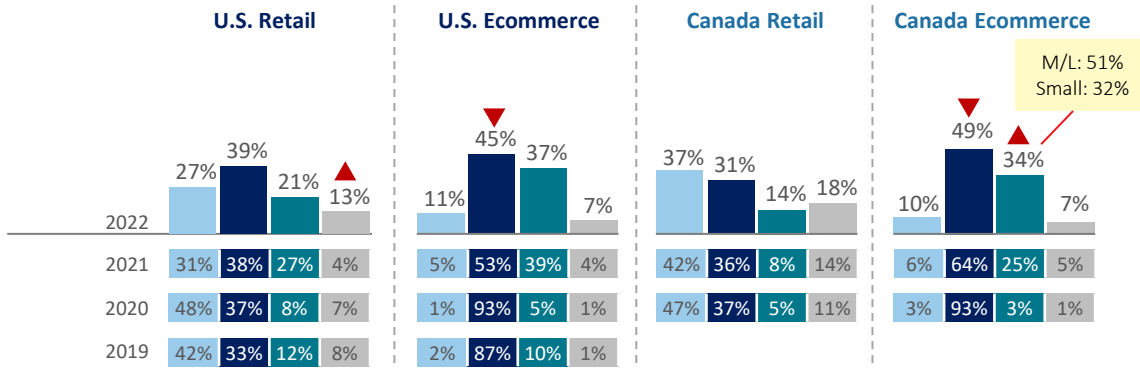
## Not surprisingly, the mobile channel continues to account for a sizeable portion of fraud costs among Ecommerce merchants.

There is also a directional increase in the percent of fraud costs associated with U.S. retail call centers and is a sizeable portion for Canadian retailers. Call center fraud is not new, though more work-at-home since the pandemic has likely put this higher on fraudsters radar. And, for some merchants, this channel may reside outside of fraud prevention efforts focusing on in-person and remote channel transactions.<sup>3</sup>

There has also been a directional increase in fraud costs associated with in-person channels among ecommerce merchants.

### % Fraud Costs by Channel | Retail & Ecommerce Merchants

■ In-Person  
■ Mobile  
■ Online  
■ Call Center



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

## The percent of fraud costs associated with international transactions is growing significantly for U.S. ecommerce merchants and is sizeable for Canadian ecommerce as well.

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.

Overview

Key Findings

Transaction Trends

Fraud Attacks &amp; Losses

The Customer Journey

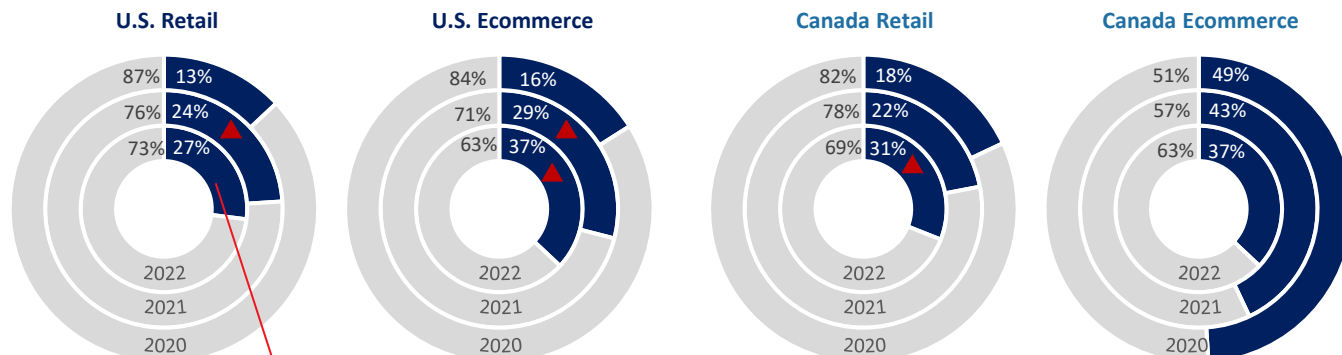
Robust Practices

Recommendations

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

■ International Fraud

■ Domestic Fraud



M/L: 32% (increased from 21% in 2021)

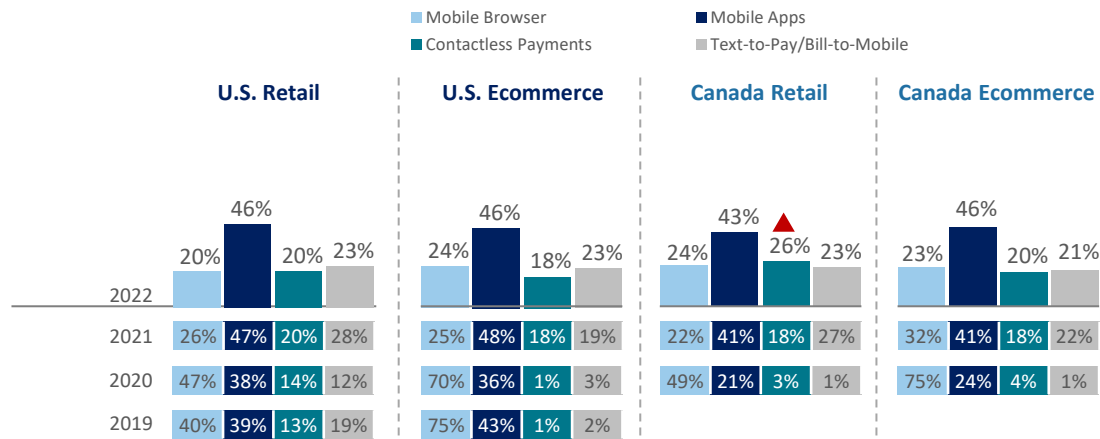
Survey Questions:  
Q13: Please indicate the percent of annual fraud costs generated through domestic compared to international transactions in the last 12 months

▲ = significantly or directionally higher/lower than previous period



# Mobile apps remain the primary source of mobile payment fraud, with other alternative digital payment methods representing a sizeable portion of fraud losses as well.

The trend of mobile payment fraud away from traditional browsers to other mobile transaction and payment options continues since the start of the pandemic, as the rise of digital/mobile wallets use has increased.

## % 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

# KEY FINDING 03

Fraud is occurring across the customer journey, though the account login phase is at-risk for a number of merchants with regard to takeovers and breaches.

Identity fraud is a leading reason for fraud losses across the customer journey. And the percent of identity-related fraud attributed to the account creation and login phases has increased year-over-year.

Many merchants focus on new account creation and/or the point of purchase as being most susceptible to fraud – and findings show these journey points as being fraud targets. However, the percentage of fraud costs attributed to account logins/compromises is fairly similar to the amount attributed to the other journey points.

Digital identity verification is a key challenge across the customer journey, driven by an increase in bot attacks and synthetic identities. Few solutions designed to increase identity verification effectiveness are being used at the account login phase, even though fraud is on the rise at this stage.



## Key Finding 03

### INCREASED LOSSES DUE TO IDENTITY AND ACCOUNT-RELATED FRAUD ACROSS THE CUSTOMER JOURNEY

# Friendly/first-party and third-party/synthetic-identity fraud are driving retail and ecommerce fraud losses across the customer journey.

Canadian ecommerce merchants are particularly seeing losses related to identity fraud at the point of purchase.

Overview

Key Findings

Transaction Trends

Fraud Attacks & Losses

The Customer Journey

Robust Practices

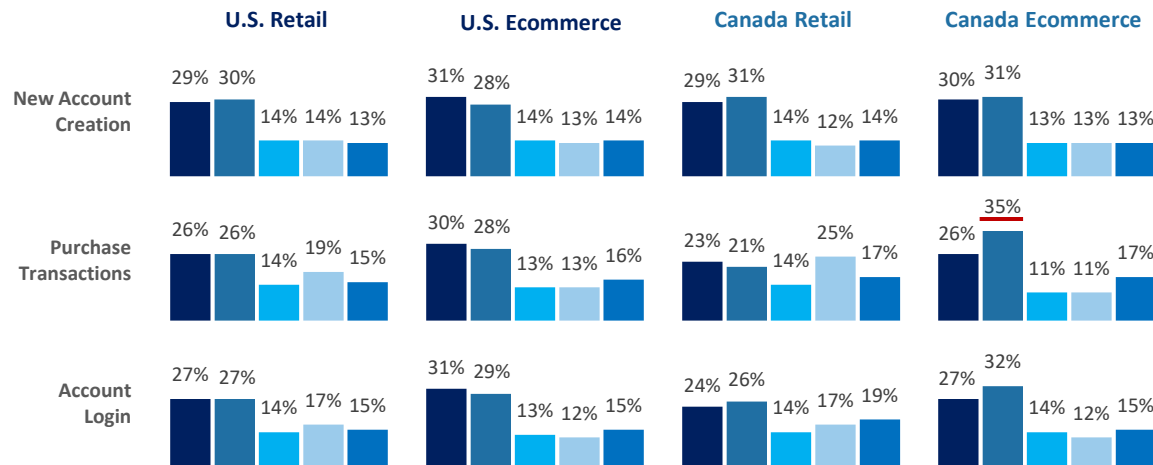
Recommendations

## % Distribution of Fraud Losses by Fraud Type



Retail & Ecommerce Merchants

■ Friendly/  
First-Party Fraud   ■ Third-Party/Synthetic-Identity Fraud   ■ Third-Party  
Account Takeover   ■ Lost/stolen  
merchandise   ■ Fraudulent request  
for return



Survey Questions:  
Q12a: For each specific customer journey stage, please indicate the percentage distribution for your past 12-month's fraud losses across the following fraud methods.

— = significantly or directionally higher than other challenges within customer journey stage

## For most, new account creation and in-person transactions are primary risk stages in the customer journey; they also represent a sizeable portion of fraud costs.

Interestingly, few indicated account login as being most susceptible to fraud even though that customer journey point also accounts for a sizeable portion of fraud costs.

Overview

Key Findings

Transaction Trends

Fraud Attacks &amp; Losses

The Customer Journey

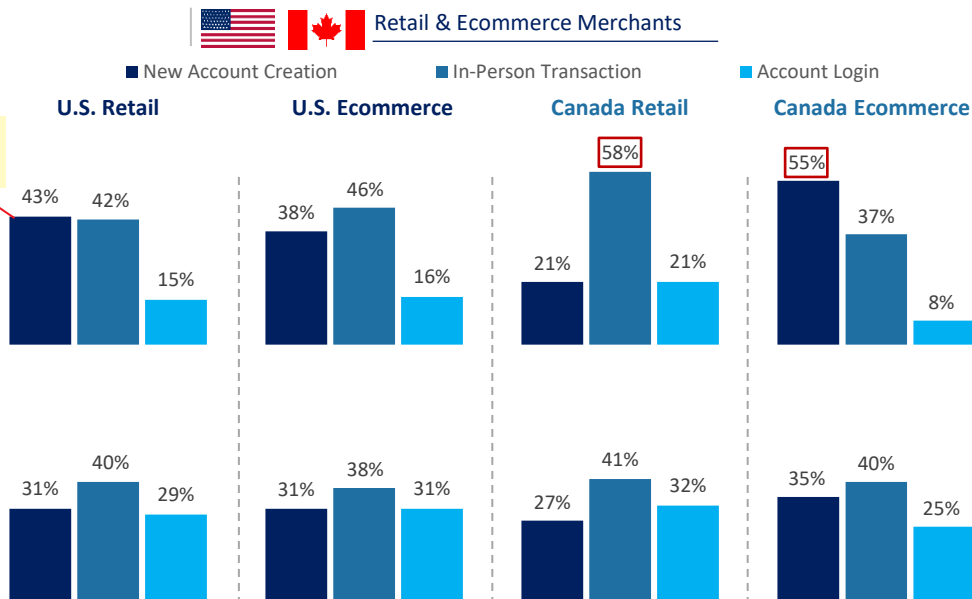
Robust Practices

Recommendations

Survey Questions:  
Q12n: Which of the following online customer journey stages is your organization MOST susceptible to with fraud? Q11b: Approximately, how much of your fraud losses would you attribute to each of the customer journey stages?

### Customer Journey Stage MOST Susceptible to Fraud

### % Fraud Costs by Customer Journey Stage



□ = significantly or directionally higher than other markets

**While in-person transactions represent a sizeable portion of identity-related fraud, this is a growing threat with new account creation for U.S. and Canadian merchants.**

Overview

Key Findings

Transaction Trends

Fraud Attacks &amp; Losses

The Customer Journey

Robust Practices

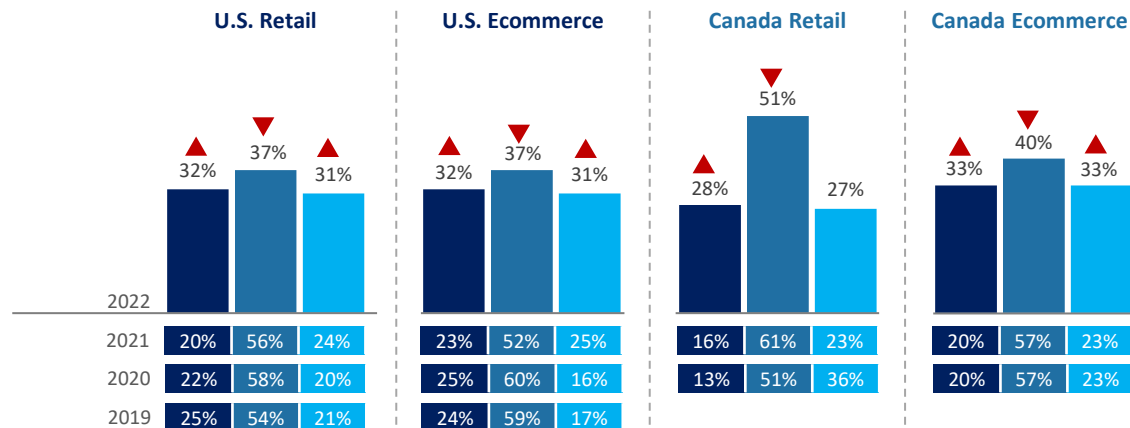
Recommendations

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

■ New Account Creation

■ In-Person Transaction

■ Account Login



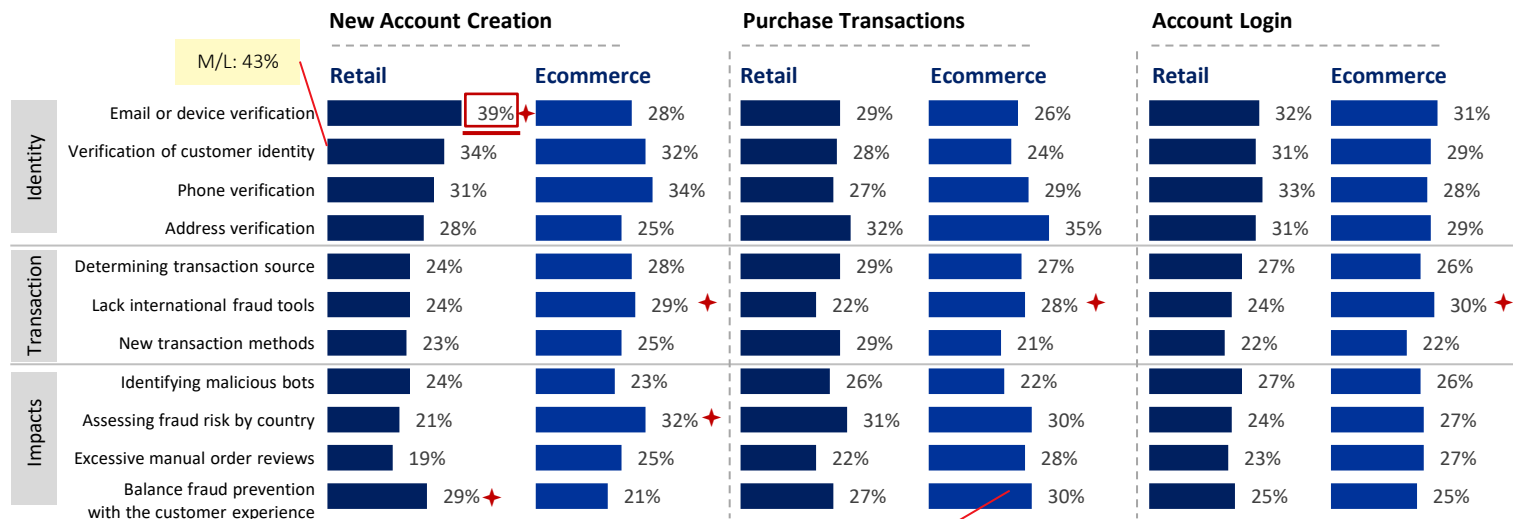
Survey Questions:  
Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?

▲ = significantly or directionally higher/lower than previous period

# Digital identity verification is a particular online channel challenge at new account creation, where customer history and online behaviors have not yet been established with the retailer/merchant.

Along with this comes concern about balancing fraud prevention with the customer experience, particularly at the front end. With a sizeable portion of fraud costs involving international transactions, assessing fraud by country is one of the top online challenges at point of purchase, with U.S. ecommerce merchants somewhat more likely than retailers to indicate lack of fraud tools for these cross-border transactions. This is a reminder of the importance for assessing both identity and transaction risk.

## Top Three Ranked ONLINE Fraud Challenges Retail & Ecommerce Merchants



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

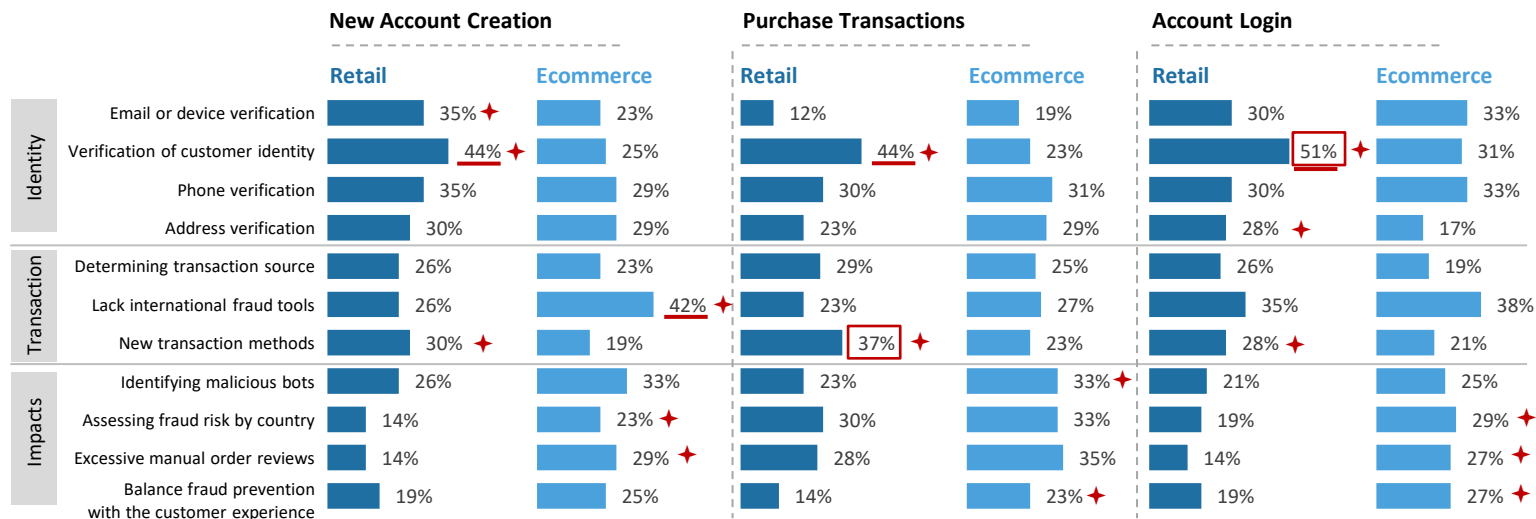
— = significantly or directionally higher than other challenges within customer journey stage  
 □ = significantly or directionally higher than same challenge at other customer journey states

\* = significantly or directionally higher than other segment (retail or ecommerce) within customer journey stage


# Canadian retailers are even more likely than their U.S. counterparts to rank customer verification as a top online channel challenge – and particularly more so across the customer journey.


Canadian retailers that rank new transaction methods as a top online challenge during in-person transactions are those who have also experienced an increase in the average volume of transactions through mobile/digital wallets.

## Top Three Ranked ONLINE Fraud Challenges Retail & Ecommerce Merchants



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 customer journey stage

 = significantly or directionally higher than same challenge at other customer journey states

 = significantly or directionally higher than other segment (retail or ecommerce) with in customer journey stage

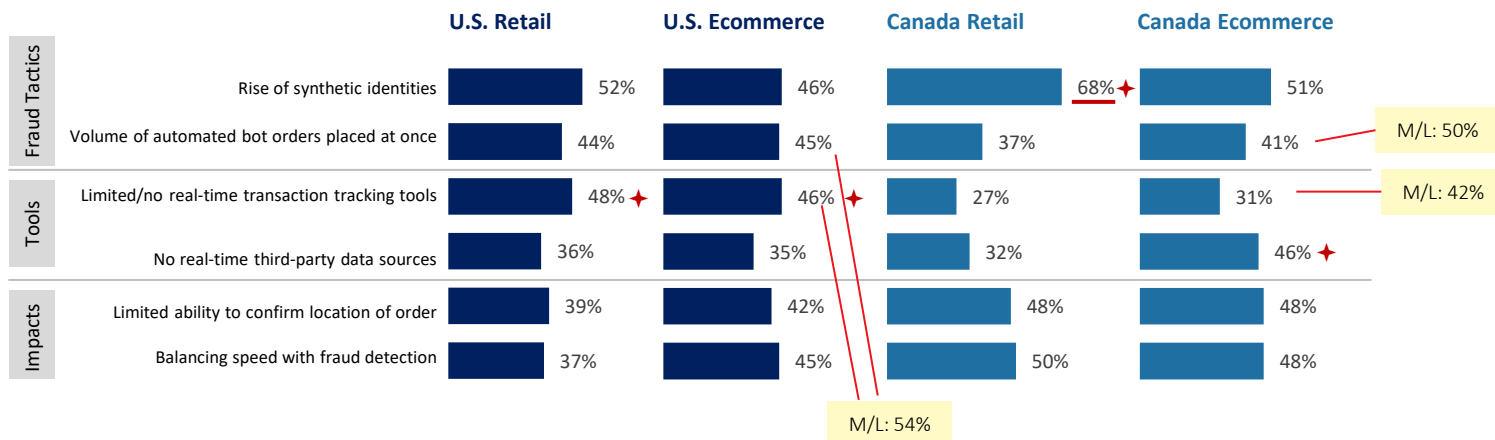
## Synthetic identities are a leading cause for online channel identity verification challenges, though so too is limited use/access to real-time transaction tracking and third-party data sources.

Synthetic identities are difficult to detect using traditional fraud resources that verify physical attributes (name, DOB, address) because they are a combination of real and fake data.

### Top Three Ranked Factors Making Customer Identity Verification a Challenge ONLINE



Retail & Ecommerce Merchants



Survey Questions:  
Q20c: Please rank the top 3 factors that make customer identity verification a challenge when serving customers through the online channel.

— = significantly or directionally higher than other challenges within segment  
+ = significantly or directionally higher than other segments



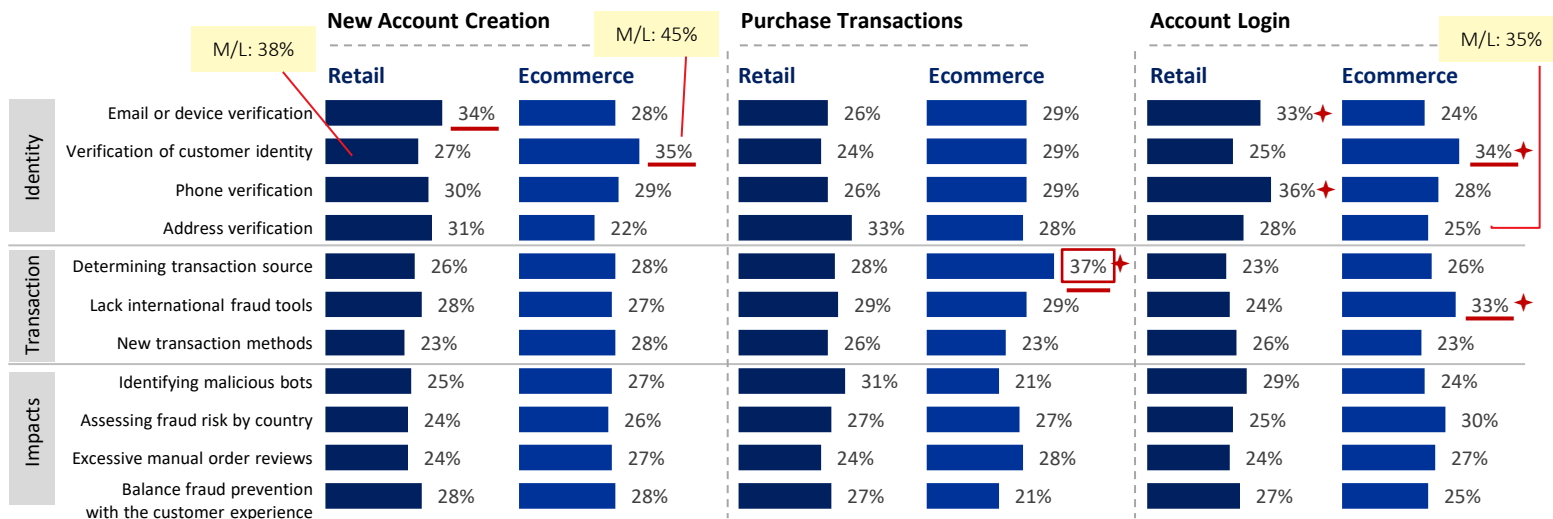
# U.S. retailer challenges with account-based digital identity verification continues with mobile channel transaction as well, specifically verifying email addresses, phone numbers or devices.

U.S. ecommerce merchants also indicate identity verification challenges in general, as well as transaction related ones (determining source, lacking tools for assessing international transaction fraud) at the purchase or login stage.

## Top Three Ranked MOBILE Fraud Challenges



Retail & Ecommerce Merchants



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 customer journey stage

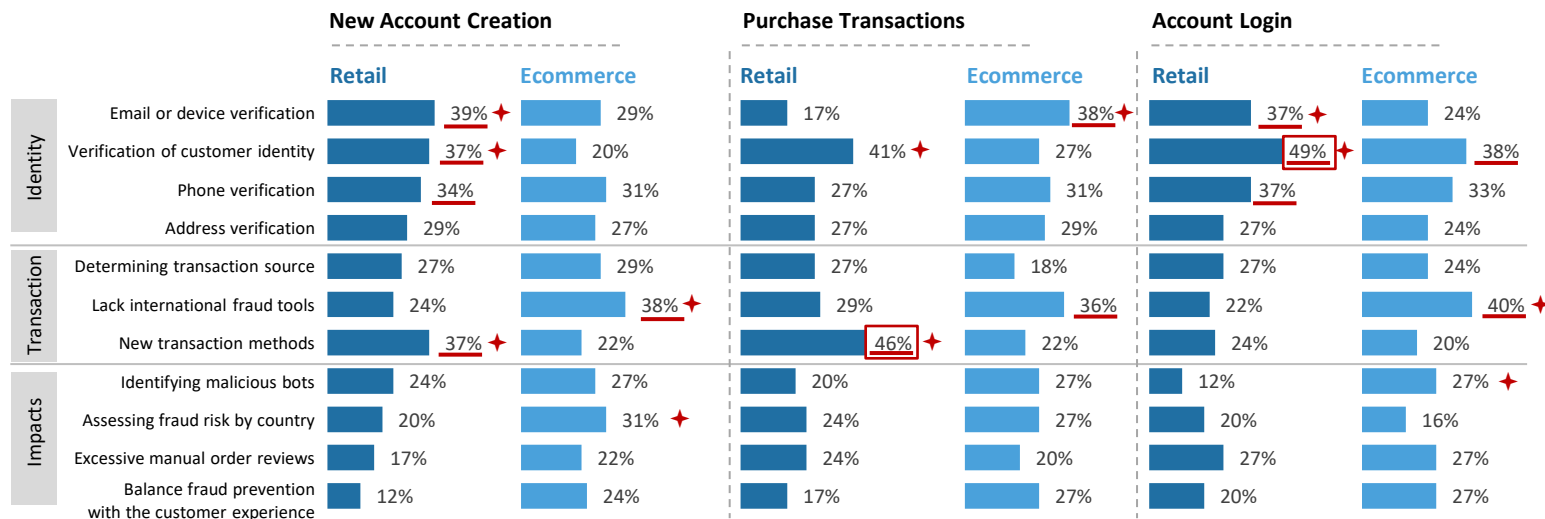
□ = significantly or directionally higher than same challenge at other customer journey states

\* = significantly or directionally higher than other segment (retail or ecommerce) with in customer journey stage

## Compared to online account creation and logins, device/email verification becomes more of a challenge for Canadian retailers when authenticating these through the mobile channel.

As shown later, there is limited use of digital identity solutions, such as device ID and authentication by biometrics, that are designed specifically for mobile channel identity authentication. There is also limited use of real-time transaction risk assessment solutions by Canadian ecommerce merchants.

### Top Three Ranked MOBILE Fraud Challenges Retail & Ecommerce Merchants



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 customer journey stage

□ = significantly or directionally higher than same challenge at other customer journey states

↑ = significantly or directionally higher than other segment (retail or ecommerce) with in customer journey stage

## Key Finding 03

### SYNTHETIC IDENTITY VERIFICATION AS A KEY MOBILE CHANNEL CHALLENGE

**Synthetic identities and mass automated bot orders are complicating mobile channel identity verification efforts, again with limited use of real-time transaction risk assessment and third-party data.**

Overview

Key Findings

Transaction Trends

Fraud Attacks & Losses

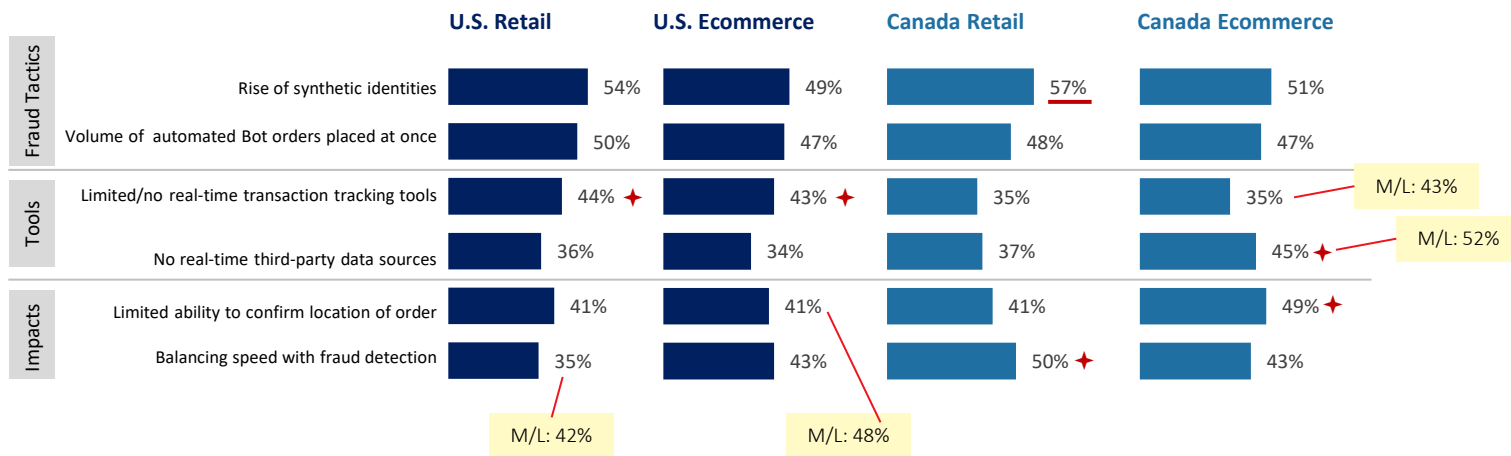
The Customer Journey



Robust Practices

Recommendations

#### Top Three Ranked Factors Making Customer Identity Verification a Challenge for MOBILE

  Retail & Ecommerce Merchants



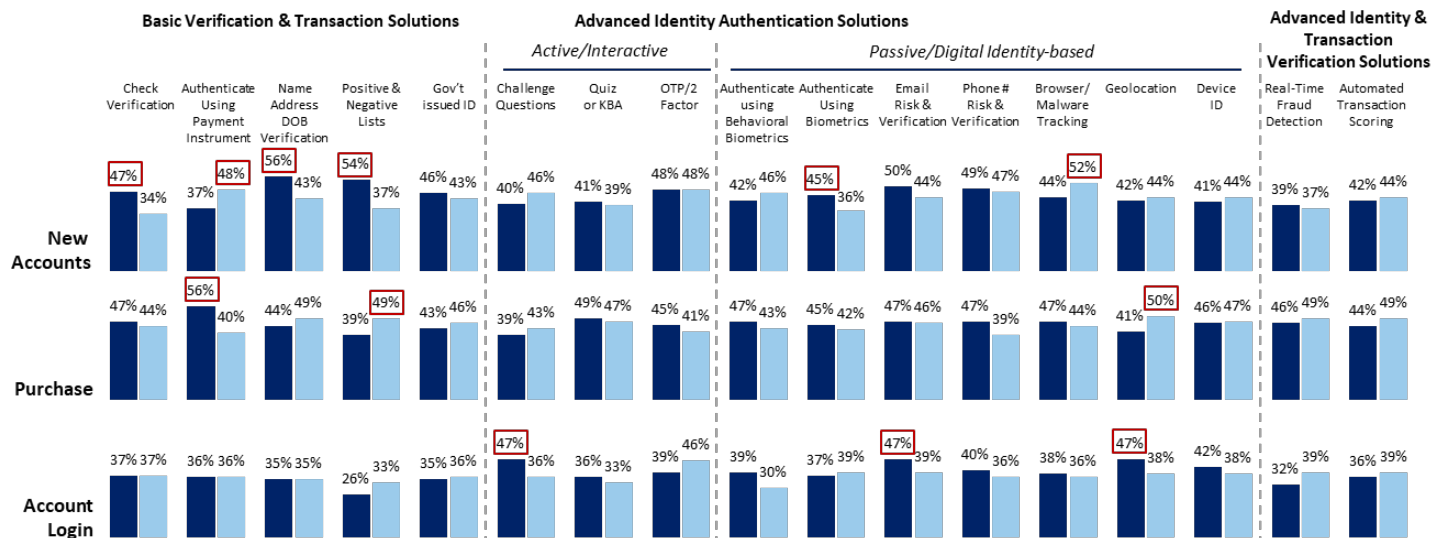
 = significantly or directionally higher than other challenges within segment  
 = significantly or directionally higher than other segments

# There is moderate use of digital identity and transaction verification solutions among U.S. retailers and ecommerce merchants. It is more limited with account login verification, where identity fraud has increased.

Lack of real-time tracking solutions is cited earlier as a key barrier to identity verification, yet use of those solutions is very limited at new account creation and login. Similarly, email/device risk assessment is a top online and mobile channel challenge, though use of geolocation or device ID is also limited.

## % Indicating Use of the Following Fraud Mitigation Solutions Use Retail Merchants

■ US Retail ■ US e-Commerce



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

Red box = significantly or directionally higher than same solution in other segment (retail, or ecommerce) within journey phase

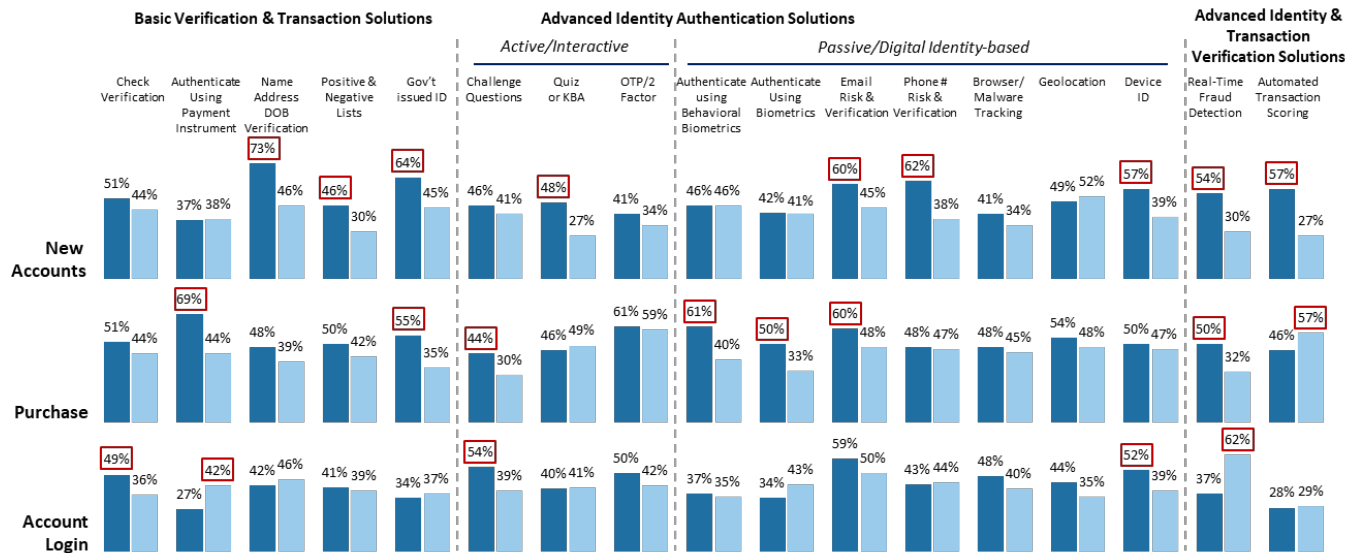
# Just over half of Canadian retail respondents indicated use of digital identity and transaction verification solutions for the new account and purchase stages of the customer journey.

Solutions use among Canadian ecommerce merchants is more fragmented and limited.

For both segments, solutions use is more limited with account login, which is a risk for fraud.

## % Indicating Use of the Following Fraud Mitigation Solutions Use Retail Merchants

■ Canada Retail ■ Canada e-Commerce



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

  = significantly or directionally higher than same solution in other segment (retail, or ecommerce) within journey phase

# KEY FINDING 04

Robust practice fraud detection and prevention includes a multi-layered solution approach for specific customer journey points, and the integration of fraud prevention with cybersecurity operations and the digital customer experience. Layering in supportive capabilities such as social media intelligence and AI/ML further strengthens fraud prevention.

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 weakens fraud prevention efforts.

Roughly half of merchants indicate that they have fully integrated their cybersecurity and digital customer experience operations with fraud prevention approaches. A sizeable minority are at least partially moving towards this objective. Robust practice fraud detection approaches should include solutions that can work behind-the-scenes, uncovering anomalies in digital attributes and behaviors while minimizing customer friction/effort.

Further, many are using cybersecurity alerts and social media intelligence as supportive capabilities, with an uptick in those indicating use of AI/ML.

Findings show that those using this robust practice approach, including layering of specific solutions at different points in the customer journey, are less likely to be challenged with identity verification, botnet attacks and balancing fraud detection with the customer experience. They also experience fewer successful fraud attacks per month and realize a lower cost of fraud.

**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.

**Robust practice approaches involve a layering of different solutions to address unique risks from different channels, payment methods and products. And they 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 & Prevention Solution Layering

A multi-layered solution approach is essential to fighting fraud while optimizing the customer experience.

Address both identity and transaction fraud risks



Different risks selling digital versus physical goods

Different challenges and risks for mobile versus online

Botnets and malware can compromise mobile devices. Authenticate the user device

### Strategy & Focus

#### *Optimizing Customer Experience 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



## A significant majority of U.S. and Canadian retailers and ecommerce merchants say that they track friendly fraud.

They also report tracking synthetic identity fraud losses separately from credit losses.



Overview



Key Findings



Transaction Trends



Fraud Attacks & Losses



The Customer Journey



Robust Practices



Recommendations

Survey Questions:  
Q14c: (ASK ONLY IF Q14a = 2/3) Does your organization track authorized-party fraud in its overall measurement of payment method fraud?

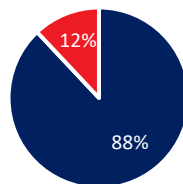


Retail & Ecommerce Merchants

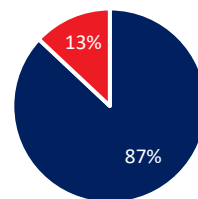
■ Yes ■ No

### % Businesses Tracking Friendly Fraud in Overall Measurement of Payment Method Fraud

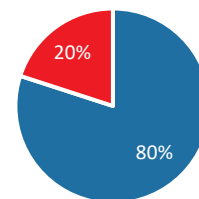
U.S. Retail



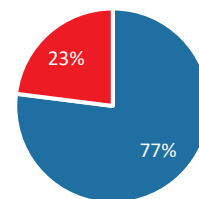
U.S. Ecommerce



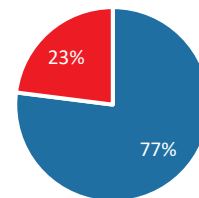
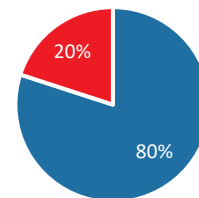
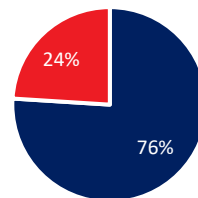
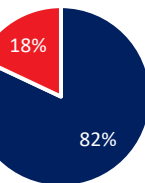
Canada Retail



Canada Ecommerce



### % Businesses Tracking Synthetic Identity Fraud Losses Separately From Credit Losses



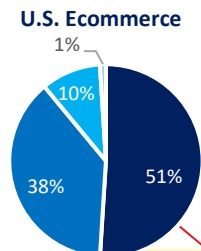
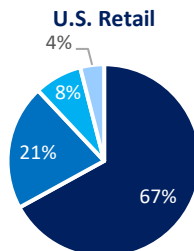
**There is sizeable familiarity with and use of the FraudClassifier<sup>SM</sup> Model across U.S. and Canadian retail and ecommerce merchants, with many others planning to make it a part of their fraud prevention efforts within the year.**

### % Businesses Familiar With/Plan to Use FraudClassifier<sup>SM</sup> Model

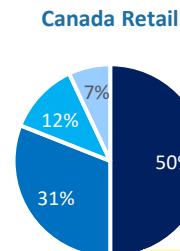


Retail & Ecommerce Merchants

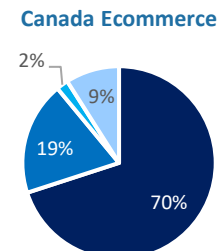
■ Familiar and using ■ Familiar but not using ■ Have heard of it but don't know what it involves ■ Have never heard of it



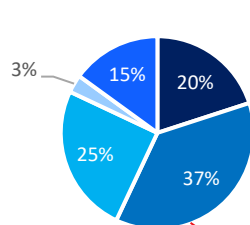
M/L: 60%



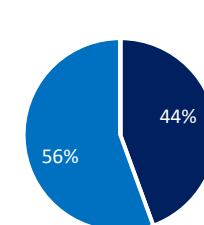
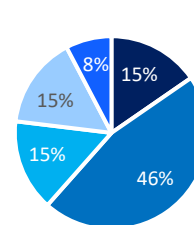
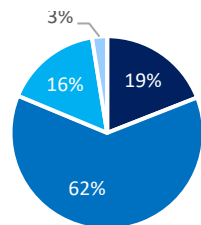
M/L: 62%



■ Yes, within the next 6 months ■ Yes, within the next 6 – 12 months ■ Yes, within the next 12 – 24 months ■ No plans to use it ■ Don't Know



M/L: 53%



Survey Questions:  
Q14e: To what degree is your organization familiar with the FraudClassifier<sup>SM</sup> model published by the Federal Reserve in June 2020?  
Q14f: (ASK ONLY IF Q14e = 2) Does your organization have plans to use the FraudClassifier<sup>SM</sup> model to classify fraud related to payments?

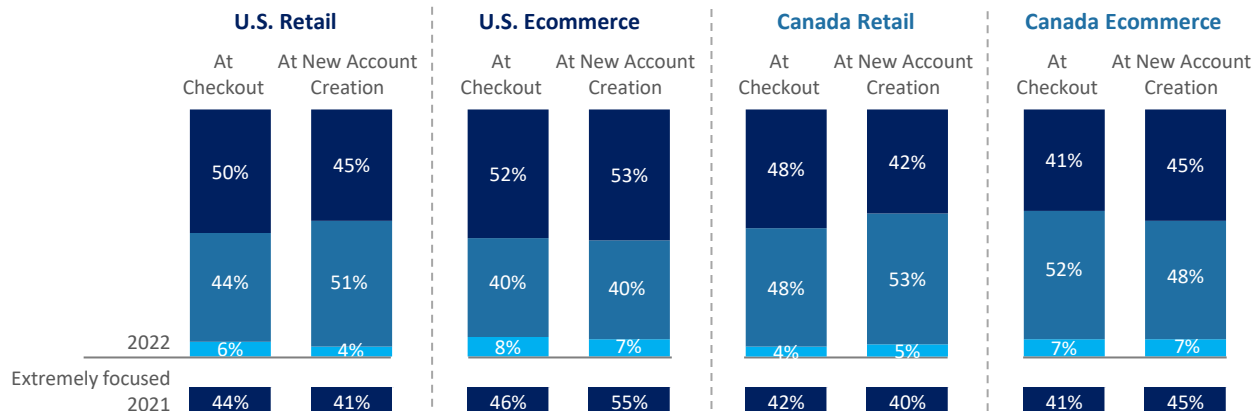
## As with last year, just under half of U.S. and Canadian merchants report that they are extremely focused on optimizing risk level with the customer experience.

Somewhat more U.S. ecommerce merchants are focused on this at both the new account and transaction stages in the customer journey compared to others.

### Degree of Focus on Optimizing Risk Level to Appropriate Customer Experience Level

  Retail & Ecommerce Merchants

Extremely focused Fairly focused Net: Not focused/not sure



### RECOMMENDATION

Friction is a concern. Minimize that through layered approaches that 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.

# Roughly half of merchants report integration of their digital/customer experience operations with fraud prevention. A similar percentage also reports cybersecurity integration.

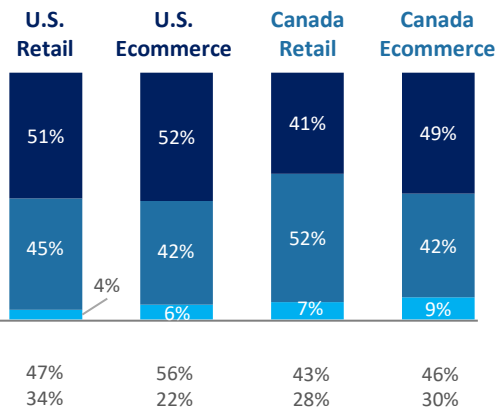
Canadian retailers lag others with this robust practice approach.



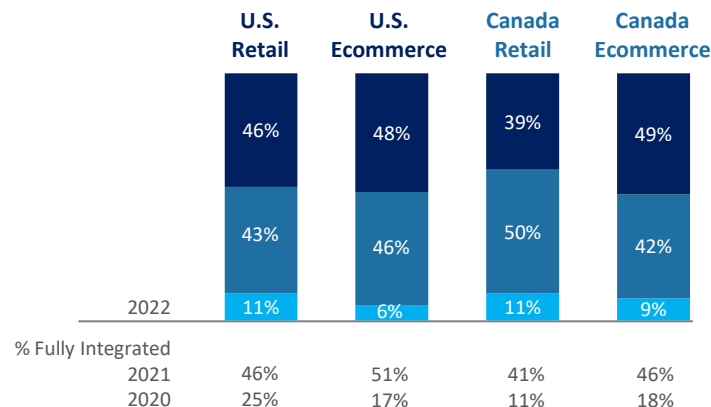
Retail & Ecommerce Merchants

Fully integrated Partially integrated Net: Not integrated

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



## Integration of Cybersecurity Operations w/ Fraud Prevention\*



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

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

**As cybersecurity alerts and social media intelligence continue to support fraud capabilities among at least half of U.S. and Canadian merchants, there is also increasing consideration of AI/ML models.**



Overview



Key Findings



Transaction Trends



Fraud Attacks &amp; Losses



The Customer Journey



Robust Practices



Recommendations

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

▲ = significantly or directionally higher/lower than previous period

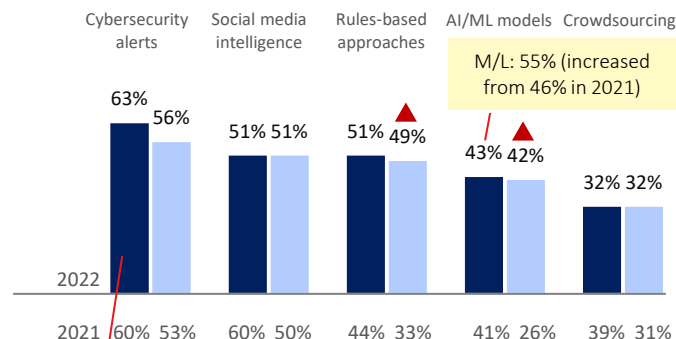
### % Using Supportive Capabilities to Fight Fraud



Retail &amp; Ecommerce Merchants

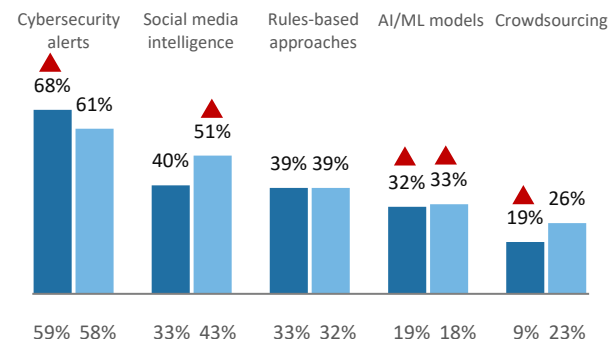
■ U.S. Retail ■ U.S. E-commerce

■ Canada Retail ■ Canada E-commerce

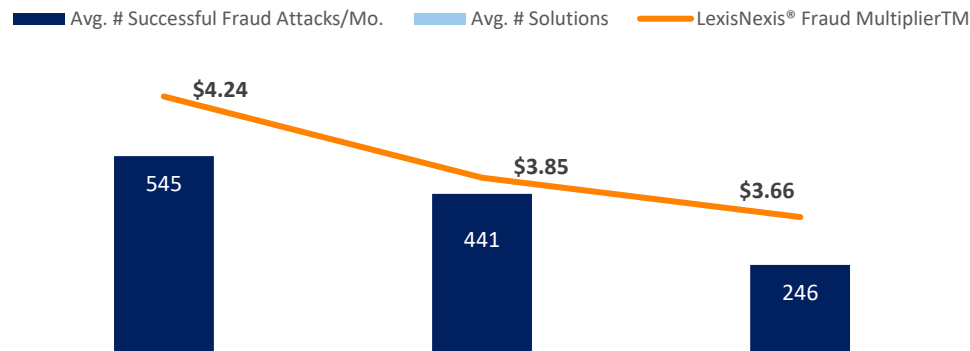


M/L: 55% (increased from 46% in 2021)

M/L: 70% (increased from 68% in 2021)



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



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., Email, 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		✓

## Retailers and ecommerce merchants that use this approach for new accounts are better able to verify digital attributes and malicious bots.

This includes use of email/phone verification and risk assessment, device ID and geolocation.

### Overview

### Key Findings

### Transaction Trends

### Fraud Attacks & Losses

### The Customer Journey

### Robust Practices

### Recommendations

#### % Ranking as Top Online Challenge

Balancing fraud prevention with customer experience	30%	48%	19%
Email risk & verification	39%	31%	21%
Phone number risk & verification	49%	43%	25%

#### % Ranking as Top Mobile Challenge

Identity verification	49%	43%	33%
Phone/email risk & verification	42% / 43%	30% / 28%	32% / 29%
Identifying malicious bots	41%	52%	17%

#### USE OF ROBUST PRACTICE APPROACH

Integration of Cybersecurity, Digital Experience with Fraud Ops

NO

No

PARTIALLY

No

FULLY

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., Email, phone # risk, biometrics)

Limited or None

✓

Solution(s) to assess device risk, location (e.g., Device ID, Geolocation)

Limited or None

Some Limited Use

✓

Solution(s) to assess behavior (e.g., Behavioral Biometrics, Transaction Risk)

Limited or None

✓

## A robust approach for the purchasing phase increases identity verification effectiveness and risk assessment of the transaction.

This includes the addition of real-time transaction monitoring, behavioral biometrics and/or automated transaction scoring along with solutions to assess digital identities (email, phone, device, location, biometrics).

### Overview

### Key Findings

### Transaction Trends

### Fraud Attacks & Losses

### The Customer Journey

### Robust Practices

### Recommendations

#### % Ranking as Top Online Challenge

Determine transaction source	41%	51%	19%
Email risk & verification	51%	21%	14%
Assess fraud risk by country	37%	25%	23%

#### % Ranking as Top Mobile Challenge

Identity verification	40%	53%	20%
Balancing fraud detection with customer experience	41%	9%	14%
Identifying malicious bots	48%	32%	22%

#### USE OF ROBUST PRACTICE APPROACH

Integration of Cybersecurity, Digital Experience with Fraud Ops

NO

No

PARTIALLY

No

FULLY

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., Email, phone # risk, biometrics)

Limited or None

✓

Solution(s) to assess device risk, location (e.g., Device ID, Geolocation)

Limited or None

Some Limited Use

✓

Solution(s) to assess behavior (e.g., Behavioral Biometrics, Transaction Risk)

Limited or None

✓



## And, a robust practice approach for the account login phase can reduce account takeovers through solutions that assess digital identities, behaviors and transaction risk.

This includes the addition of real-time transaction monitoring, behavioral biometrics and/or automated transaction scoring along with solutions to assess digital identities (email, phone, device, location, biometrics). Challenge questions are also part of the combination.

## Overview

## Key Findings

## Transaction Trends

## Fraud Attacks &amp; Losses

## The Customer Journey

## Robust Practices

## Recommendations

**% Ranking as Top Online Challenge**

Determine transaction source	40%	48%	28%
Identity verification	40%	56%	31%
Identifying malicious bots	68%	9%	12%

**% Ranking as Top Mobile Challenge**

Email risk & verification	43%	31%	29%
Identity verification	30%	51%	18%
Identifying malicious bots	48%	41%	18%

**USE OF ROBUST 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., Email, phone # risk, biometrics)

Limited or None

✓

Solution(s) to assess device risk, location (e.g., Device ID, Geolocation)

Limited or None

Some Limited Use

✓

Solution(s) to assess behavior (e.g., Behavioral Biometrics, Transaction Risk)

Limited or None

✓

# RECOMMENDATIONS

The background of the slide features a blue-tinted image of a person's hands typing on a laptop keyboard. Overlaid on this image are several white, semi-transparent hexagonal icons. These icons include: a large checkmark inside a circle, a document with a checklist, a group of three people, a notepad with a pencil, and a computer monitor displaying a checklist. The overall aesthetic is professional and tech-oriented.

## Recommendation #1

### IDENTITY PROOFING SHOULD INCLUDE ASSESSING DIGITAL IDENTITY ATTRIBUTES. TECHNOLOGY IS KEY TO THIS EFFORT OF DETECTING AND MITIGATING FRAUD WHILE OPTIMIZING THE CUSTOMER EXPERIENCE.



Overview



Key Findings



Transaction Trends



Fraud Attacks & Losses



The Customer Journey



Robust Practices



Recommendations



Identity proofing involves both verification and authentication. **Verification** relates to self-provided data (date of birth, national ID number, address, etc.) to determine if the person/identity is real and that the data relates to a single identity; this is particularly important with the rise of synthetic identity fraud. **Authentication** is about confirming that the person is legitimate (who they say they are).



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



The digital transformation among consumers to more online and mobile transactions means that more of these transactions are occurring in an anonymous environment compared to traditional in-person interactions. Assessing only the physical identity attributes (name, address, date of birth, Social Security Number, etc.) won't help businesses authenticate the identity. Businesses need to also assess the device risk, as well as the online/mobile behaviors and transaction risk.



Businesses need a robust fraud and security technology platform that helps them adapt to this changing digital environment, offering strong fraud management and resulting in a positive experience for genuine customers.



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 #2

### A MULTI-LAYERED SOLUTION APPROACH IS RECOMMENDED — CUSTOMIZED TO EACH PHASE OF THE CUSTOMER JOURNEY AND TRANSACTION CHANNEL



Overview

Key Findings

Transaction Trends

Fraud Attacks & Losses

The Customer Journey

Robust Practices

Recommendations



Account Creation



Account Login



Account Transaction



Single point protection is no longer enough and results 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.



Further, each stage of the customer journey is a unique interaction, requiring different types of identity verification, data and solutions to let your customers in and keep the fraudsters out.



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.

## Recommendation #3

# STOP FRAUD AT THE FIRST POINT OF THE CUSTOMER JOURNEY BY PROTECTING ENDPOINTS AND USING DIGITAL IDENTITY SOLUTIONS AND BEHAVIORAL ANALYTICS THAT ASSESS RISK WHILE OPTIMIZING THE CUSTOMER EXPERIENCE.

New account opening is the customer journey point where fraudsters can become established, causing problems at later stages. It is also the first point of contact for many legitimate customers; too much friction and they may abandon the effort.



Overview

Key Findings

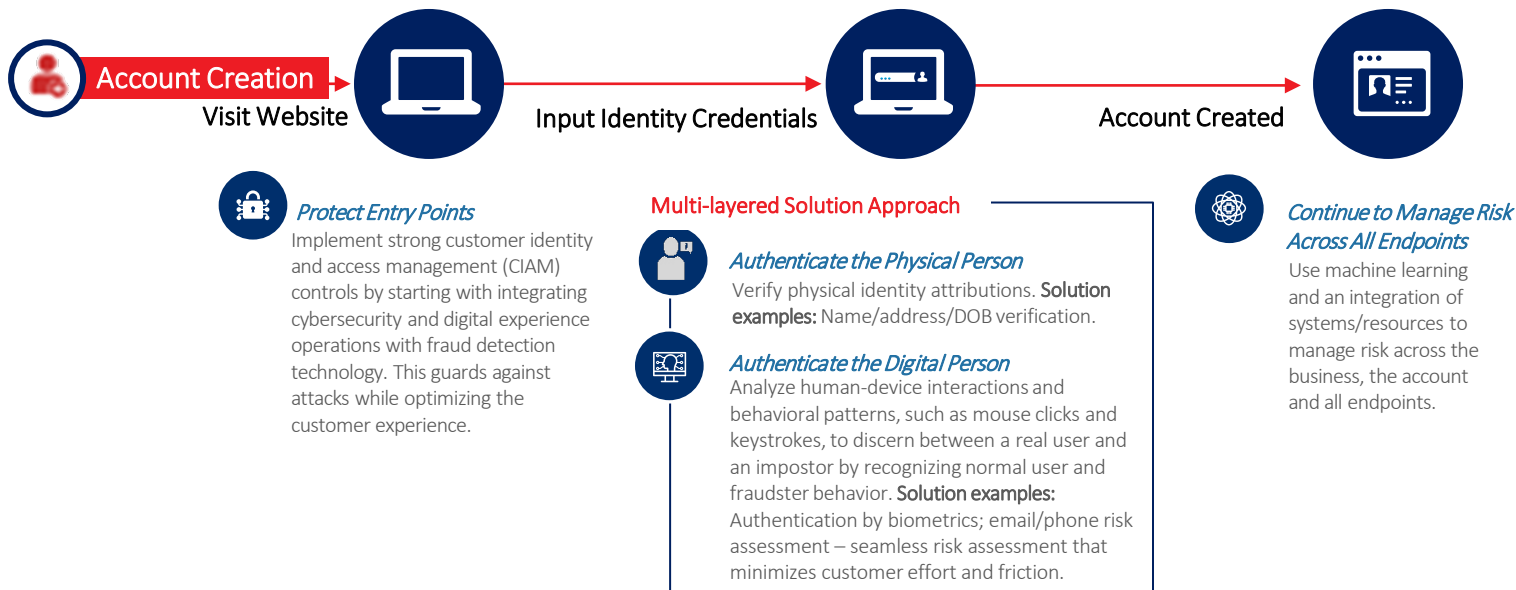
Transaction Trends

Fraud Attacks & Losses

The Customer Journey

Robust Practices

Recommendations



## Recommendation #4

# USE TECHNOLOGIES THAT RECOGNIZE YOUR CUSTOMERS, DETERMINE THEIR POINT OF ACCESS AND DISTINGUISH THEM FROM FRAUDSTERS AND MALICIOUS BOTS. LAYERED SOLUTIONS LET YOU APPLY MORE OR LESS FRAUD ASSESSMENT IN ORDER TO OPTIMIZE THIS WITH THE CUSTOMER EXPERIENCE.

### Overview

Biometrics using fingerprint or facial recognition are particularly useful for account login, based on this information gathered during account creation; this also provides a secure means of identification that speeds the process and optimizes the customer experience. Further layering should include device risk assessment to recognize the customer and assess anomalies with location of login. Where anomalies suggest potential risk, authenticate the person through more active ID authentication.

### Key Findings

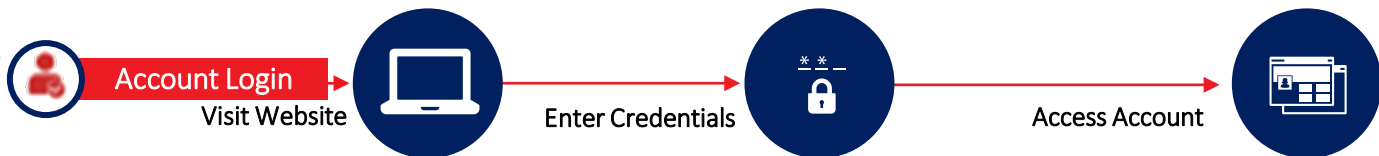
### Transaction Trends

### Fraud Attacks & Losses

### The Customer Journey

### Robust Practices

### Recommendations



### Protect Entry Points

Implement strong customer identity and access management (CIAM) controls by starting with integrating cybersecurity and digital experience operations with fraud detection technology. This helps guard against attacks while optimizing the customer experience.



Breached data used to access accounts requires more levels of security and authentication of the person from a bot or synthetic identity.

### Multi-layered Solution Approach



### Authenticate the Digital Person to Distinguish Between Legitimate and Fake Customers/Fraudsters

Analyze 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 – seamless risk assessment that minimizes customer effort and friction.

This is particularly important at account login since fraudsters deploy mass bot attacks, using breached data to test passwords for account takeover.

Synthetic identities involve real and fake identity data. Physical identity attribute assessment alone will not make this distinction.



### Authenticate the Device

Identify a remote computing device or user. **Solution examples:** Device ID/ fingerprint; geolocation.



### Active Identity Authentication

Use 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, quiz or shared secrets; authentication using OTP/ 2 factor.

## Recommendation #5

### ADD TRANSACTION RISK TECHNOLOGY TO THE LAYERING OF DIGITAL ATTRIBUTES, BEHAVIORAL ANALYTICS AND DEVICE ASSESSMENT SOLUTIONS DURING THE TRANSACTION/DISTRIBUTION OF FUNDS JOURNEY POINT.

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



#### Multi-layered Solution Approach



##### *Authenticate the Digital Person*

Analyze human-device interactions and behavioral patterns, such as mouse clicks and keystrokes, to help discern between a real user and an impostor by recognizing normal user and fraudster behavior. **Solution examples:** Authentication by biometrics; email/phone risk assessment – seamless risk assessment that minimizes customer effort and friction.



##### *Authenticate the Device*

Identify a remote computing device or user. **Solution examples:** Device ID/ fingerprint; geolocation.



##### *Active Identity Authentication*

Use 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, quiz or shared secrets; authentication using OTP/ 2 factor.



##### *Assess the Transaction Risk*


###### **Velocity checks/transaction scoring:**


Monitor 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.

# LexisNexis® Risk Solutions can help.

For more information:

 [risk.lexisnexis.com/FIM](https://risk.lexisnexis.com/FIM)

 +1 800 953 2877  
+408 200 5755



## About LexisNexis Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit [www.risk.lexisnexis.com](https://www.risk.lexisnexis.com) and [www.relx.com](https://www.relx.com). Our solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. LexisNexis Fraud Multiplier is trademark of RELX Inc. True Cost of Fraud is a trademark of LexisNexis Risk Solutions Inc. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2022 LexisNexis Risk Solutions Group. NXR15605-00-0822-EN-US

This document is for informational purposes only and does not guarantee the functionality or features of any LexisNexis Risk Solutions products or services identified. LexisNexis Risk Solutions does not represent nor warrant that this document is complete or error free.

