

Trust and Collaboration as Foundations to Fight Fraud

Canadian Cybercrime and Fraud Trends



The LexisNexis® Risk Solutions Cybercrime Report 2022

Table of Contents



Foundations to Fight Fraud:

01 Global Insights **02** Canadian Transactions and Attacks Overview
03 Canadian Industry Spotlight **04** Summary

The Cybercrime Report Methodology

Report based on attacks, Jan-Dec 2022, detected by the LexisNexis® Digital Identity Network®	Using digital identity intelligence to distinguish good users from fraudsters	Analysis from 79.8B global transactions, across industries and use cases
Device, location, behavior and threat data helps verify legitimacy of transactions	Attacks = “high-risk” transactions as scored by customers	Focused on interactions with digital services – not network intrusion attacks



01 Global Insights

Global Transaction Patterns

Mobile App Transactions Dominate the Field of Play,
as Customer Retention Becomes the Name of the Game

Overall Transactions:

The growth in digital transactions continues to flourish despite a myriad of world events including armed conflict, inflation and an economic downturn. In 2022 the number of transactions analyzed in the Digital Identity Network® approached 80 billion.

Customer Journey Observations:

A stable rate of new account creations confirms the change in focus of digital consumers away from the early pandemic days where new account growth had taken off around the world and especially across emerging markets.

The growth in logins dominates as consumers explore expanded digital service offerings. Organizations emphasize the need to provide a tailored journey for their customer base, knowing customer retention and upsell is where the value is rather than customer acquisition. Payments have also seen a healthy growth, despite recession alarm bells. Digital payment innovation and choice continue to draw consumers, with digital payment methods also being used to settle in store purchases as consumers return to physical shopping locations.

Mobile Focus:

Mobile apps have become the preferred channel for digital transactions. Businesses, particularly in emerging markets, are several years into their digital transformation strategies and have prioritized mobile apps as a way to retain and upsell to their existing customer base. Originally the preserve of a select few super-apps, more and more organizations are expanding their in-app offerings, building an interconnected ecosystem within the app, ensuring their customers never need to leave.

Global Transaction Patterns in Numbers

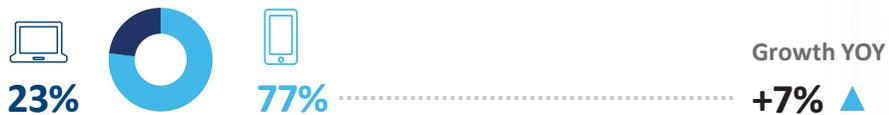
Mobile App Transactions Dominate the Field of Play, as Customer Retention Becomes the Name of the Game

TRANSACTIONS ANALYZED JANUARY-DECEMBER 2022

79.8B Growth YOY **+24% ▲**

TRANSACTIONS BY CHANNEL

Desktop / Mobile



Mobile Browser / Mobile App



TRANSACTIONS BY USE CASE

			Growth YOY
	New Account Creations	1.0B	+0.4% ▲
	Logins	58.7B	+27% ▲
	Payments	12.7B	+19% ▲

Global Attack Patterns in Numbers

Automated Bots for Harvesting, Human-Initiated Attacks to Reap the Rewards



HUMAN-INITIATED ATTACKS

Attack rates on individual online transactions that typically return full digital identity data have seen a significant rise in 2022, outpacing the growth in good customer transactions, with attacks continuing to shift to the mobile channels.

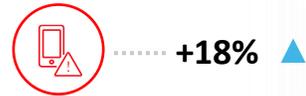
ATTACK VOLUME

905M Growth YOY **+56%** ▲

Attack Split by Desktop / Mobile



Percentage of attacks coming from mobile devices has increased YOY



ATTACK RATE

		Growth YOY
⚠ Overall	1.3%	+20% ▲
💻 Desktop	1.7%	+8% ▲
📱 Mobile Browser	2.7%	+37% ▲
📲 Mobile App	0.8%	+58% ▲



ATTACK VOLUME

Automated bot attacks (typically used to credential test stolen identities at high volume) have shifted focus away from the communications, mobile and media (CMM) industry in 2022, focusing now predominantly on the ecommerce sector.

ATTACK VOLUME

3.5B Growth YOY **+27%** ▲



Financial Services

1.9B Growth/Decline YOY **+23%** ▲



Ecommerce

1.4B **+195%** ▲



CMM

46M **-91%** ▼



Gaming & Gambling

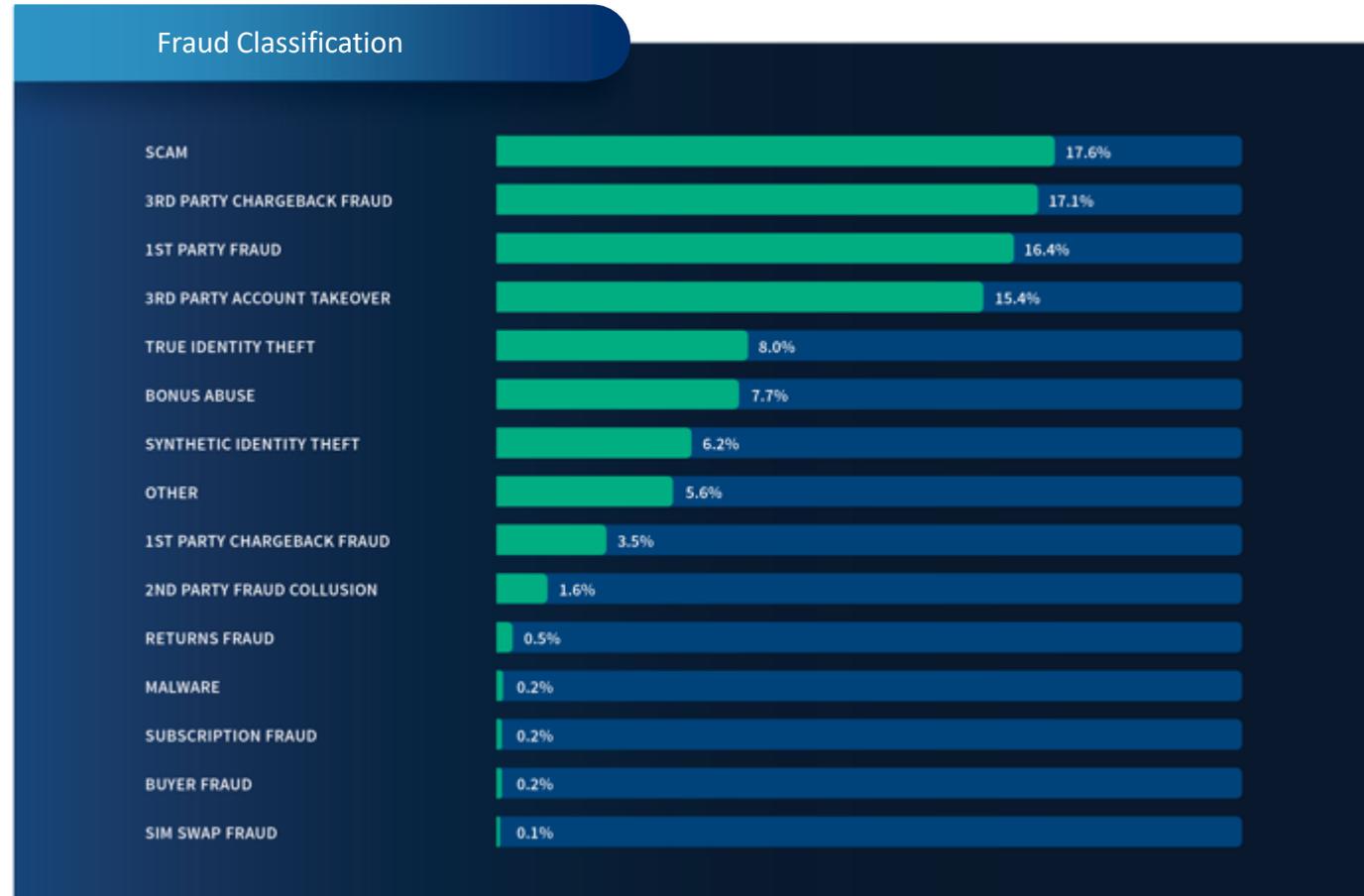
99M **-33%** ▼

The Complexity of Digital Fraud

Fraud Classifications from a Client Perspective

As fraud becomes more complex, it is important to classify fraud attempts based on their context and modus operandi. Sophisticated fraud detection systems enable multiple, targeted models to assess risk in real time, looking for the anomalies associated with different types of attacks. Alerts generated by these models can be directed at different operational teams to be handled in different ways: for example, interaction with a potential victim would likely be different in a 3rd party account takeover scenario versus a suspected authenticated push payment scam.

The chart on this page shows how fraud attempts in the Digital Identity Network® are classified by our clients. Third-party account takeover, 3rd party chargeback fraud, scams and 1st party fraud are the four most common classifications in 2022, although the broad range of classifications highlights the breadth of use cases and industries using the network.



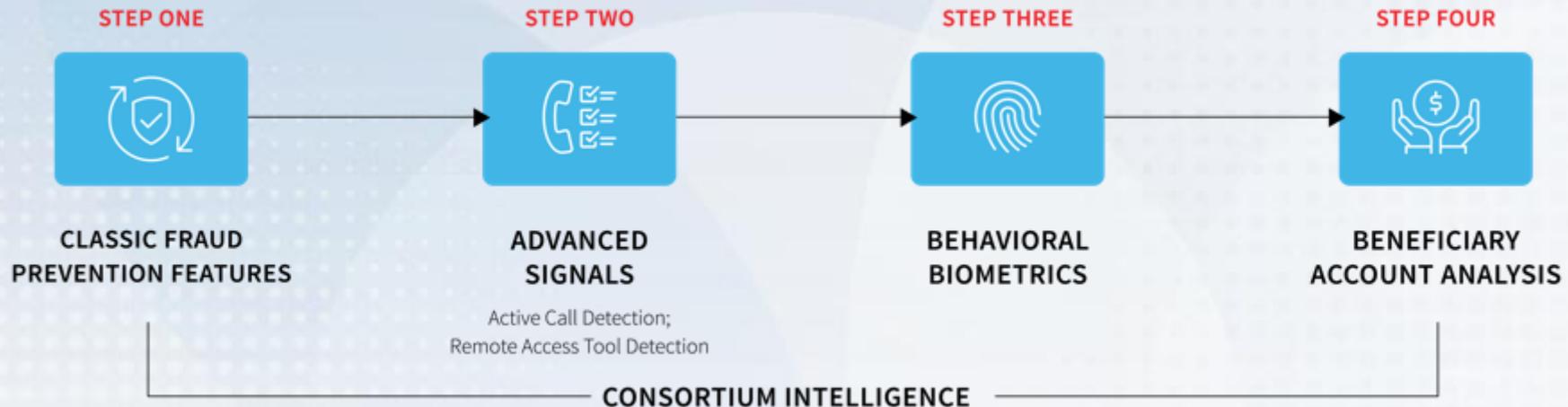
A Consolidated Approach To Preventing Scams

Bringing Together Data, Organizations and Technology

Many individual signals can provide clues to a scam being in progress: for example, classic fraud detection signals such as unusual amounts of money being transferred, or new advanced indicators around active cell phone calls being in progress during a payment attempt; behavioral biometric indications of hesitation or coaching of the victim; or risk associated with the destination account. Shared intelligence from across the industry can also identify attacks from specific cybercriminal gangs.

Advanced machine learning models with access to this range of information are able to identify many of these scams at the moment of payment. The challenge is often to ensure all signals across the user journey are available, in the same system as the fraud detection models, together with access to the consortium intelligence. Only then can these features work together in collaboration, with the correct weightage assigned to them, as so not to impact genuine customers.

Machine Learning Scam Model



A man with a goatee, wearing a green cardigan over a white t-shirt, is sitting at a desk and looking at a laptop. The background shows a window with natural light and a teal wall. A semi-transparent network diagram with blue and orange nodes and connecting lines is overlaid on the left side of the image. A dark blue banner is positioned at the bottom left, containing the text '02 Canadian Transactions and Attacks Overview'.

02 Canadian Transactions and Attacks Overview

Digital Transactions Increased Significantly in Canada YOY, with Most Transactions Occurring Via a Mobile Device



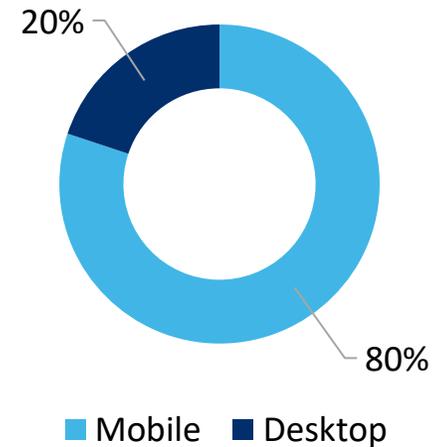
TRANSACTIONS PROCESSED

8B

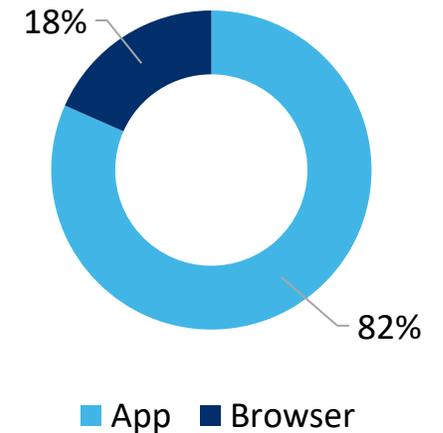
Growth in Transactions YOY

+32% ▲

Transaction Breakdown



Mobile Transaction Breakdown



Human-Initiated Attacks and Bot Attacks Were Notable

Human-Initiated Attacks

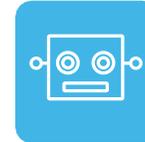


ATTACK VOLUME

79M

Growth YOY
+30% ▲

Automated Bot Attacks



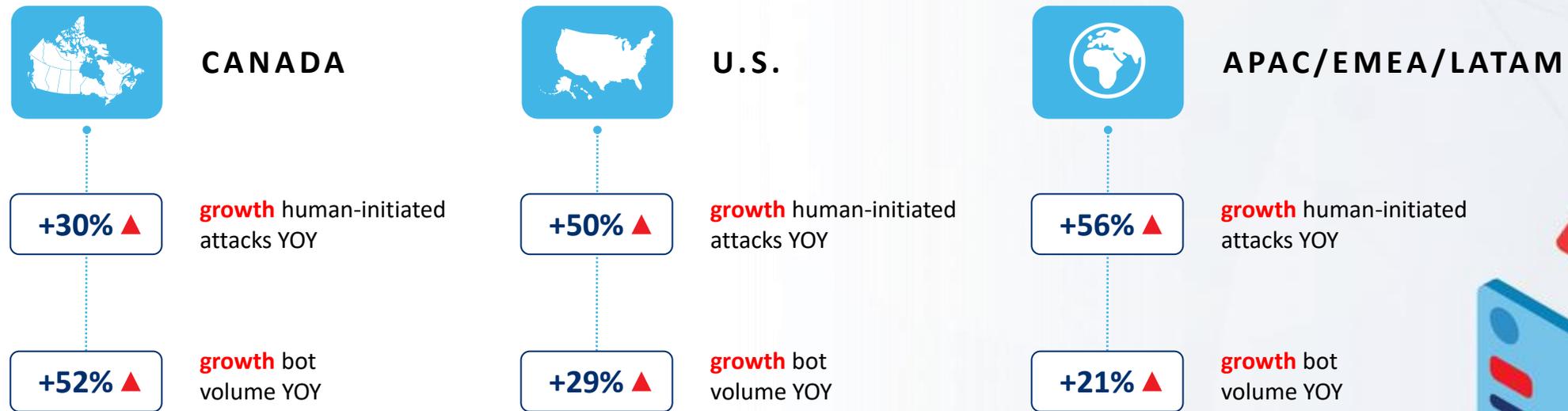
ATTACK VOLUME

271M

Growth YOY
+52% ▲

Attack Volume Comparison Around the World

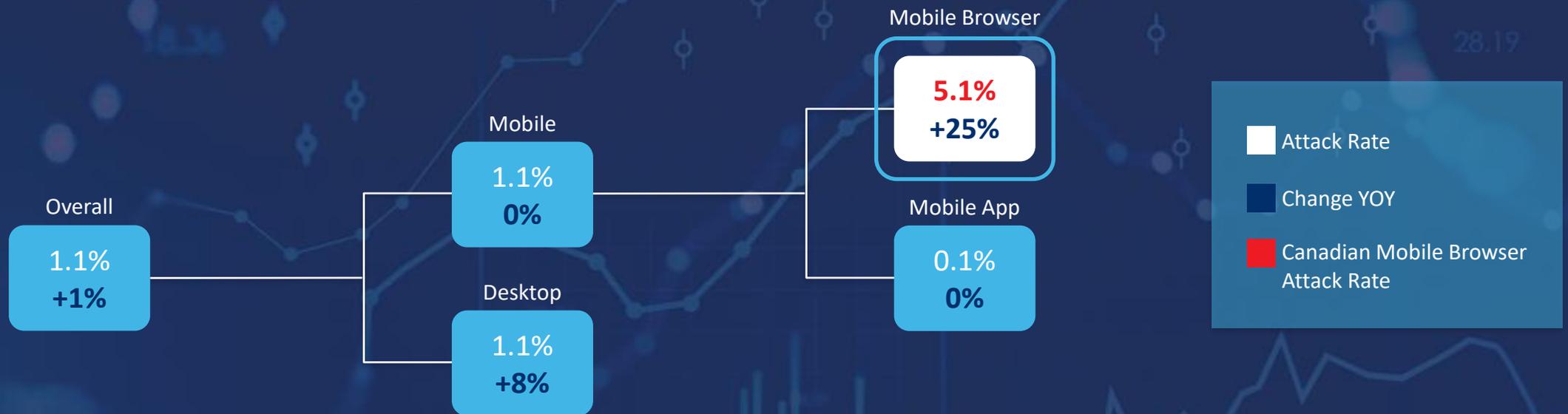
While human-initiated attacks grew 30% YOY, other regions around the world experienced significantly higher increases in human-initiated attacks. Conversely, Canada experienced a 52% increase in bot attacks which was substantially higher than other regions.



Attack Rate by Channel

Mobile browser had the highest attack rate of any channel and experienced a 25% increase YOY. **The Canadian mobile browser attack rate was nearly double that of the worldwide average of 2.7%.** The desktop channel experienced an 8% increase YOY and had the second highest attack rate of all channels. Mobile app had the lowest attack rate, and experienced 0% change YOY.

Attack Rate by Channel



Canadian Fraud Trends Across the Customer Journey

While login experienced the lowest attack rate, in part due to very high volumes of transactions, key risk points in the journey experienced relatively high attack rates, such as new account opening and payments.

Transactions across all industries increased by the highest growth rate for password resets while new account opening transaction changes YOY varied considerably depending on industry.

	 NEW ACCOUNT	 LOGIN	 PASSWORD RESETS	 DETAIL CHANGES	 PAYMENTS
Transactions	+3%	+38%	+68%	+12%	+20%
Attack Rate	5.9%	0.1%	4.4%	4.1%	5.6%



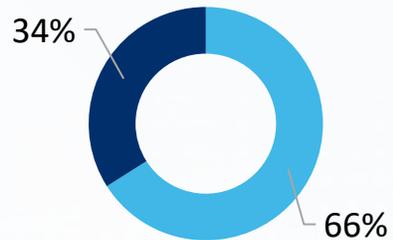
03 Canadian Industry Spotlight

Transactions Across Industries in Canada



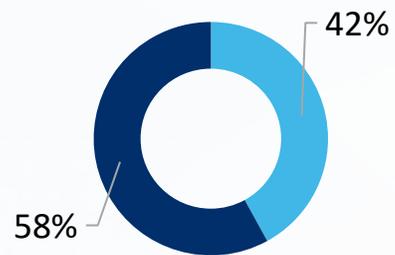
ECOMMERCE

Transaction Split



Desktop Mobile

Mobile Transaction Split

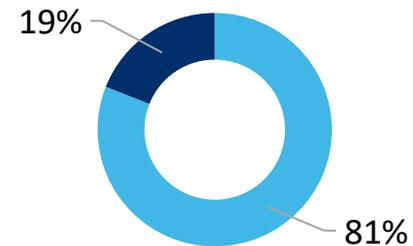


Mobile App Mobile Browser



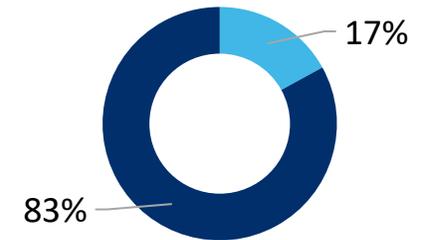
FINANCIAL SERVICES

Transaction Split



Desktop Mobile

Mobile Transaction Split



Mobile App Mobile Browser

While Both Ecommerce and Financial Services Industries in Canada Saw Increases in Attacks, Ecommerce Experienced a Sizable 183% Increase in Bot Attacks

	Ecommerce	Financial Services
 Bot Attacks	+183%	+48%
 Human Initiated Attacks	+22%	+31%
 Attack Rate	1.2%	1.1%

The Canadian Financial Services Industry Saw a Higher Overall Attack Rate Than Other Financial Services Industries Across All Regions Except LATAM

Attack Rates Around the World



APAC

0.9%



EMEA

0.5%



LATAM

1.9%



U.S.

0.8%



CANADA

1.1%

Financial Services: Attack Rates Across the Customer Journey in Canada

	 NEW ACCOUNT	 LOGIN	 PASSWORD RESETS	 DETAIL CHANGES	 PAYMENTS
Transactions	+83%	+40%	+104%	+12%	+22%
Attack Rate	5.2%	0.1%	4.6%	4.2%	5.8%
Attack Rate Change	-26%	+150%	-16%	+218%	+24%

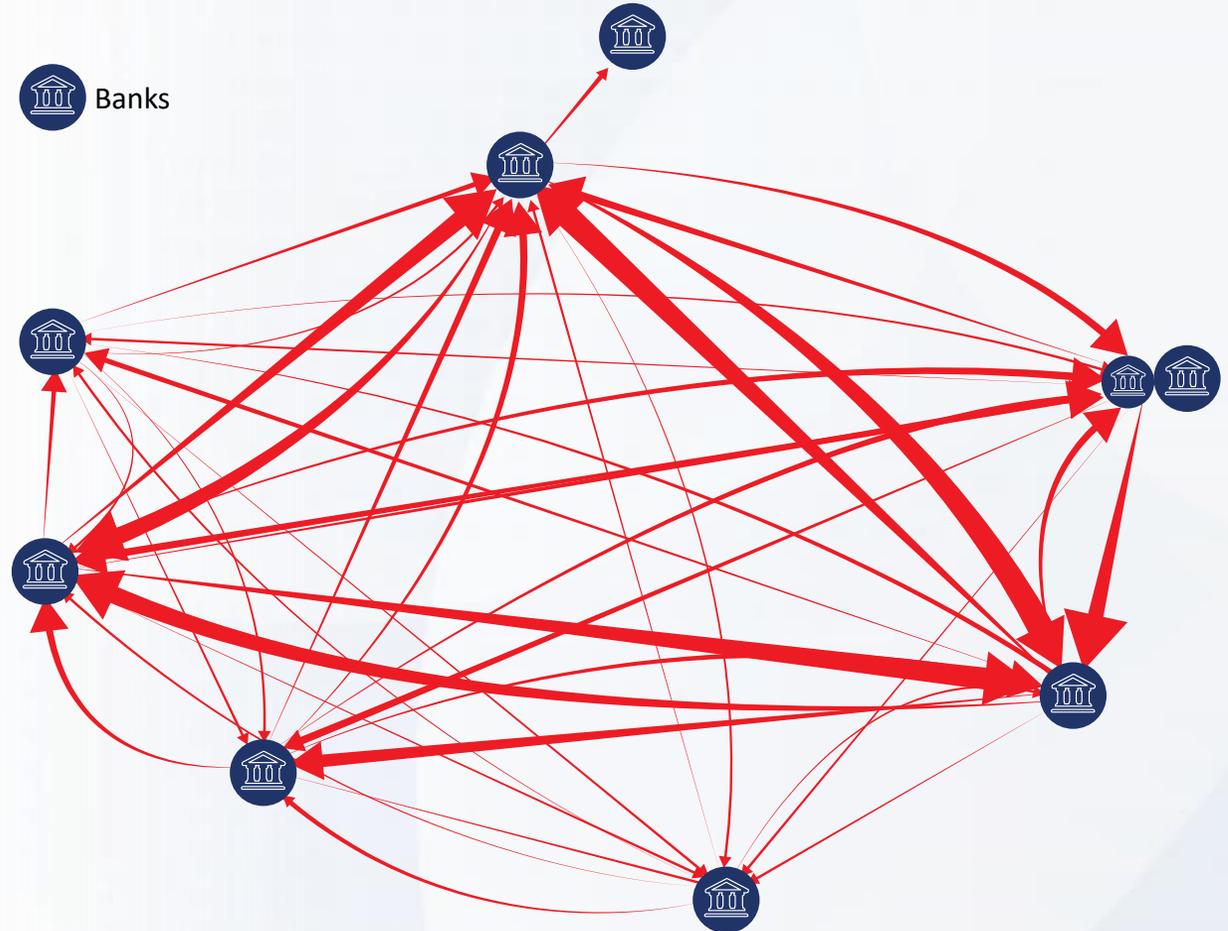
- In 2022, payments incurred the highest attack rate at **5.8%**, a 24% increase YOY
- New account opening experienced the most significant decline in YOY attack rate, however this point in the customer journey continued to have the second highest attack rate at 5.2%
- Detail changes experienced the most significant YOY increase in attack rate, at **+218%**

Network Analysis Reveals a Significant Overlap in Fraudulent Devices Attempting to Transact with Multiple Canadian Financial Services Organizations

Three-month time period: Oct-Dec 2022

Each arrow illustrates the number of devices associated with confirmed fraud attempts at one bank, crossing over to another bank in the Digital Identity Network

A thicker line denotes a higher volume of overlapping fraudulent devices





04 Summary

Key Takeaways in Canada



Digital transactions grew 32% in 2022 compared to 2021, as online traffic continues to increase.



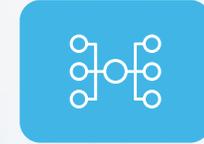
Mobile continues to be a critical channel for Canada, with 80% of transactions occurring via the mobile channel. **Canada is consistently a highly mobile country** relative to other regions.

The mobile browser channel attack rate was especially high at 5.1%, almost double that of the global average at mobile browser.



Canada experienced a +30% increase in human-initiated attacks and a +52% increase in bot attacks year-over-year.

Different industries, such as ecommerce and financial services, encountered different attack trends. Additionally, **Canadian financial services organizations experienced relatively high attack rates** compared to other regions.



Leading organizations detect and stop global fraud by leveraging critical global networks and layering risk-appropriate solutions in the customer journey.

Network analysis of Canadian financial services organizations revealed that fraudsters attack across organizations.

Recommendations for Canadian Organizations



• **Digital channels should continue to be an area of focus, as digital interactions continue to increase in Canada and both human-initiated and bot attacks increase YOY.**



• **Secure interactions between your organizations and consumers across the customer journey with particular attention at new account opening (NAO), payments and password resets.**

- NAO continued to be the highest attack rate across the customer journey in Canada. Protect the “front door” by obtaining a 360-degree view of these transactions.
- Payments had the second highest attack rate of 5.6% in 2022. Points in the customer journey where money transfers occur continue to be prime targets for fraudsters.
- Password reset experienced the third highest attack rate of 4.4%, which is notable as password resets are a key target for fraudsters attempting account takeover.



• **Organizations should continue to invest in securing the mobile channel as most Canadian transactions were processed via this popular access point (both mobile browsers and mobile apps). Of note, the mobile browser should be a key area for consideration as this channel in Canada experienced an attack rate almost double the global average.**



• **Combat against increasingly dynamic and interconnected global fraud threats by leveraging the power of global networks and shared digital intelligence.**

Fraud and Identity Solutions



For More Information

risk.lexisnexis.com/fraudandidentity

LexisNexis Cybercrime Report

risk.lexisnexis.com/cybercrime-report

LexisNexis® ThreatMetrix®

risk.lexisnexis.com/threatmetrix

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions includes seven brands that span multiple industries and sectors. We harness the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. 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 [LexisNexis Risk Solutions](#) and [RELX](#).

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis® Risk Solutions products identified. LexisNexis Risk Solutions does not warrant that this document is complete or error-free. If written by a third party, the opinions may not represent the opinions of LexisNexis Risk Solutions. LexisNexis, the Knowledge Burst logo and LexID are registered trademarks of RELX Inc. ThreatMetrix and Digital Identity Network are registered trademarks of ThreatMetrix, Inc. Emailage is a registered trademark of Emailage Corp. Trueld is a registered trademark of LexisNexis Risk Solutions Inc. InstantID is a registered trademark of LexisNexis Risk Solutions FL Inc. BehavioSec is a registered trademark of Behaviometrics AB. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2023 LexisNexis Risk Solutions. NXR16142-00-0823-EN-US

For more information, please visit risk.lexisnexis.com and relx.com

