LexisNexis®
RISK SOLUTIONS

LexisNexis® True Cost of Fraud™ Study
Financial Services and Lending Report

January 2022

U.S. and Canada Edition

The LexisNexis® 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 financial services and lending markets
- Key pain points related to adding new payment mechanisms, transacting though online and mobile channels and expanding internationally

COVID-19 Impact:

- Data collection occurred during August and September 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:

- The cost of fraud is more than the actual dollar value of a fraudulent transaction. It also includes additional costs related to labor/investigation, fees incurred during the applications/underwriting/processing stages, legal fees and external recovery expenses. Therefore, the total cost of fraud is expressed by saying that for every $1 of lost value due to fraud, the actual cost is higher based on a multiplier representing these additional costs.
- For a common base of comparison between the U.S. and Canada, all currency is in USD.

The study included a comprehensive survey of 502 risk and fraud executives in financial services and lending companies in the U.S. (426) and Canada (76).

	Total	Company Type		Size	
		Financial Services	Credit and Lending	Small (<$10M)	Mid/Large ($10M+)
# Completions	502	250	252	117	385

Financial Services Companies Include:

- Retail/Commercial Banks
- Credit Unions
- Investments
- Trusts
- Wealth Management

Lending Institutions Include:

Auto Lenders
Finance Companies
Mortgage Companies
Non-Bank Credit Card Issuer
Non-Bank Personal Loan Issuer

Segment Definitions

Small
Earns less than $10 million in annual revenues

Mid/Large
Earns $10 million+ in annual revenues

Online Commerce
Accept payments or transactions through an Internet web browser via a laptop or desktop computer

Mcommerce
Accept payments or transactions through either a mobile browser or app, or "bill to mobile phone"

1 **Attacks and Costs**: Fraud costs and attack volumes remain significantly higher compared to before the COVID-19 pandemic. U.S. banks and mortgage lenders are driving much of this.

2 **Mobile Channel Impact**: The mobile channel continues to impact higher fraud costs and volumes, as financial services and lending firms say that criminals have particularly targeted this channel for fraud during the pandemic.

3 **Customer Journey Fraud Risks:** Fraud losses are occurring across the customer journey, though the point of funds distribution is seen as most susceptible for fraud by many, with banks and mortgage firms also indicating new account creation. Identity verification is a top challenge, while others are more specific to journey points. Study findings show that layering specific digital identity solutions at different journey points can lessen these challenges.

4 **Fraud Prevention Best Practice:** Best practice fraud detection and prevention includes a multi-layered solutions approach, and the integration of fraud prevention with cybersecurity operations and the digital customer experience. Laying in supportive capabilities such as social media intelligence and AI/ML further strengthens fraud prevention. Study findings show that firms which follow this approach have lower fraud costs and challenges.

Key Finding 1

Fraud costs and attack volumes remain significantly higher compared to before the COVID-19 pandemic. U.S. banks and mortgage lenders are driving much of this.

The cost of fraud for U.S. financial services and lending firms is between 6.7% and 9.9% higher than before the pandemic. This is driven by mortgage lending (up 23.5% since pre-COVID-19) and a continued upward trend among banks (+13.0%).

There was clearly a spike in fraud costs and volume at the start of the pandemic, as these rose significantly in 2020 and have softened some for credit lending and investment firms (though still above pre-pandemic levels).

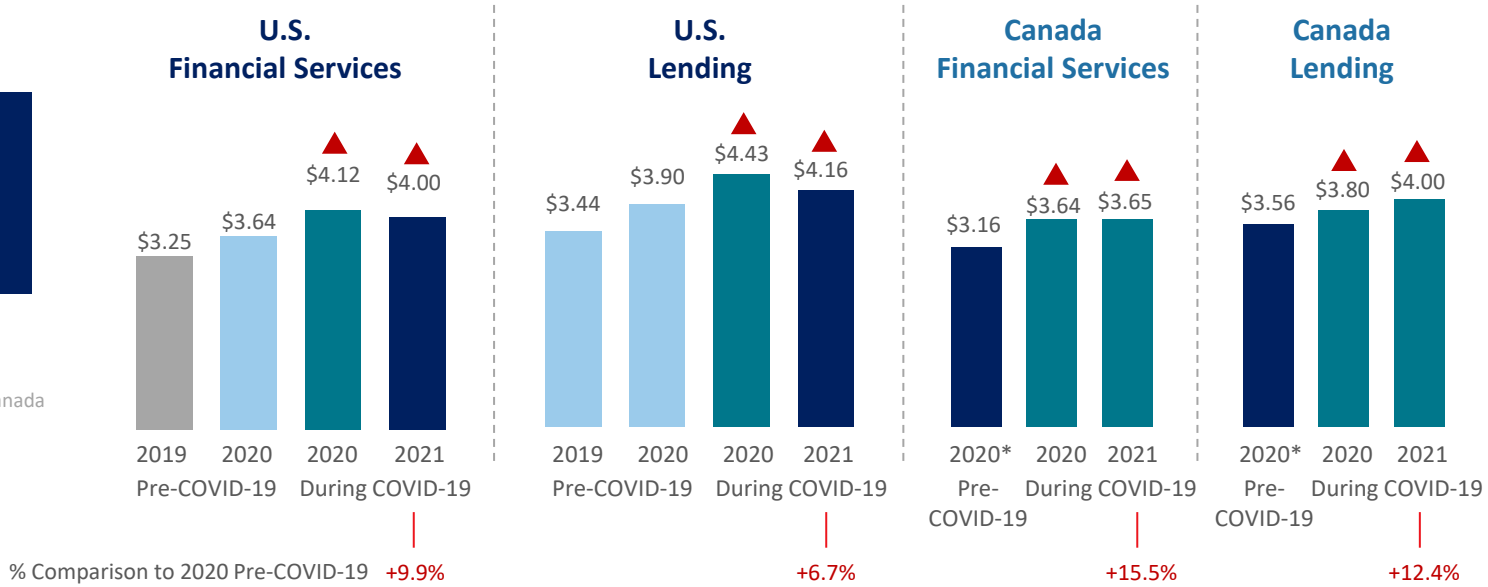
The cost of fraud continues to be significantly higher than pre-COVID-19 for both U.S. and Canadian financial services and lending firms.

For every $1 of fraud loss, it costs U.S. financial services firms $4.00 compared to $3.25 in 2019 and $3.64 in 2020 (pre COVID-19). While the LexisNexis® Fraud Multiplier™ is slightly less for Canadian financial services firms at $3.65, they have experienced a sharper year-over-year rise (15.5% compared to 9.9% for U.S. firms).

As has been the trend, lending firms have a somewhat higher cost of fraud compared to financial services firms.

Such fraud costs involve losses related to the transaction face value for which firms are held liable, plus fees/interest incurred during applications/underwriting/processing stages, fines/legal fees, labor/investigation and external recovery expenses. In this case, there have been increases related to labor and external recovery support. This reminds us that the cost of fraud is not just about the level of successful attacks, but the time and resources that are applied to preventing attacks as well.

Cost of Fraud: LexisNexis Fraud Multiplier™



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 pre-COVID-19

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

SEGMENT HIGHLIGHTS

The cost of fraud for Canadian lending firms has come closer to parity with U.S. lending firms compared to 2020.

U.S. mortgage lenders have experienced a significant rise in fraud costs since the start of the COVID-19 pandemic; it continues to be higher than other segments.

Attacks on larger mortgage lenders have been increasing in recent years, particularly among those originating a majority of loans through online/mobile channels. While slightly down from the early pandemic spike, every $1 of mortgage lending fraud loss actually costs them $4.40.

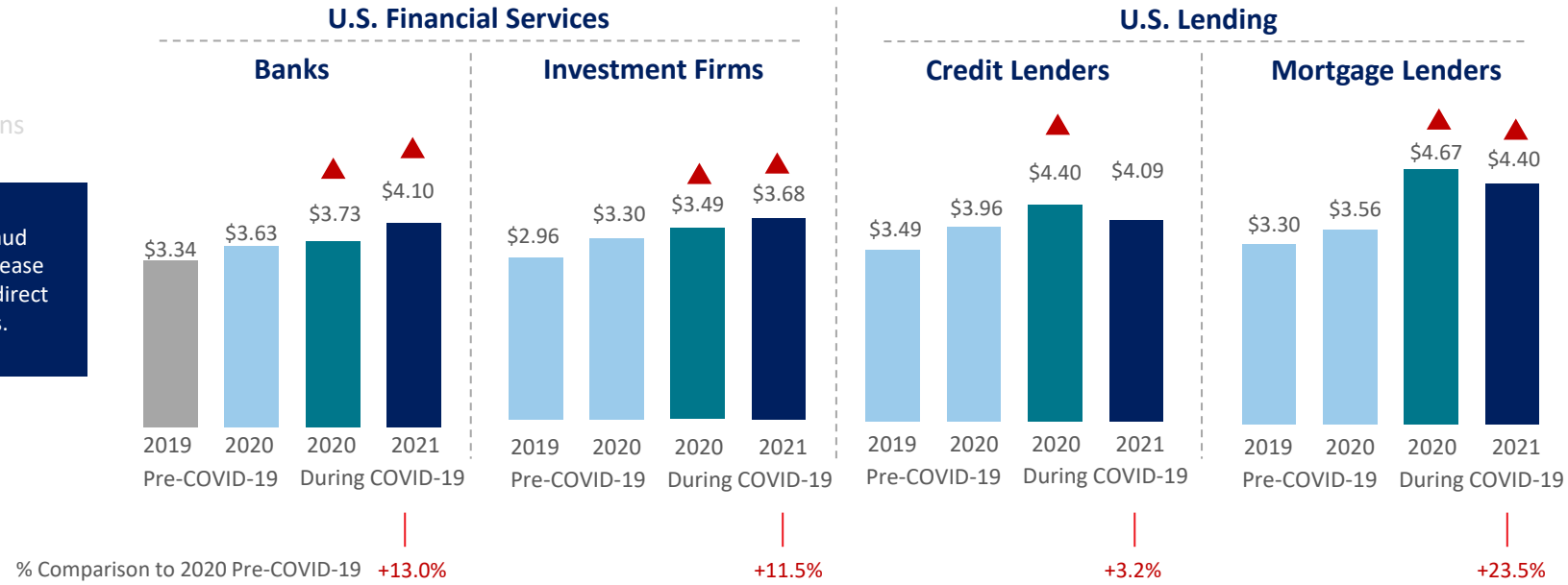
U.S. banks and investment firms' fraud costs continue an upward trend over pre- and early pandemic periods.

Overall, these findings tell us that the impact of COVID-19 on fraud costs is still in progress.

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 pre-COVID-19

Cost of Fraud: LexisNexis Fraud Multiplier™



SEGMENT HIGHLIGHTS

Mortgage lending fraud costs are 23.5% higher than just before COVID-19 hit in early 2020.

Banks and investment firm lending costs continue to rise above the early pandemic period.

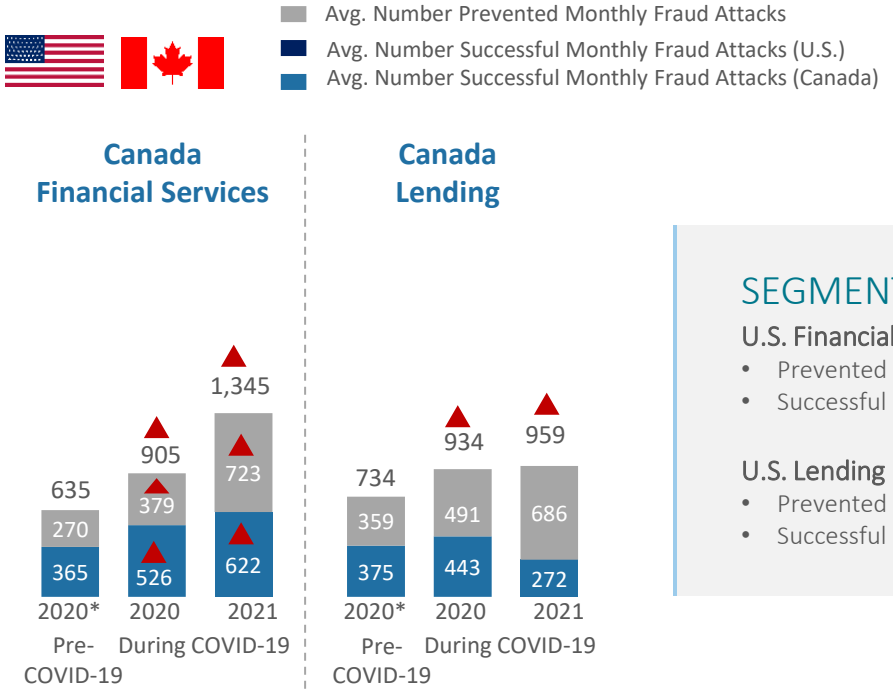
Average successful monthly fraud attacks against financial services and lending firms remain above pre-COVID-19 pandemic levels, with financial services firms' attacks continuing to rise.

This is driven by larger firms.

U.S. and Canadian lenders experienced a dramatic spike in average monthly fraud volume during the early pandemic months. While their month fraud volumes have dipped (U.S.) or remained constant (Canada), they remain above pre-COVID periods.

This is a key indicator that fraudsters are still looking for ways to exploit the pandemic at a time when mobile banking options increase for consumers, including bill-to-mobile payments and adoption of a financial firm's branded apps for transactions.

Average Monthly Fraud Attacks



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 pre-COVID-19

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

SEGMENT HIGHLIGHTS

U.S. Financial Services
- Prevented Attacks: M/L = 1,427
- Successful Attacks: M/L = 893

U.S. Lending
- Prevented Attacks: M/L = 953
- Successful Attacks: M/L = 737

Larger banks, on average, have a higher number of monthly fraud attacks, which have increased year-over-year.

Average monthly fraud volume continues to rise among U.S. banks and mid/large mortgage firms as other segments have seen their attack volumes soften a bit from the initial pandemic spike.

As shown earlier, the cost of fraud is highest among mortgage firms and continues an upward trend among banks – which also act as mortgage originators. A pandemic such as COVID-19 brings market uncertainty and unemployment, which increases the risk of mortgage fraud through misrepresentation and credit washing.[1] Increased use of synthetic identities adds to the difficulty of battling fraud and increases the cost of resources where solutions are not being used to assess the digital transaction risk and behaviors.

SEGMENT HIGHLIGHTS

U.S. Banks
The average volume of monthly attacks has increased since 2020 for **mid/large banks (from 1,977 to 2,320).**

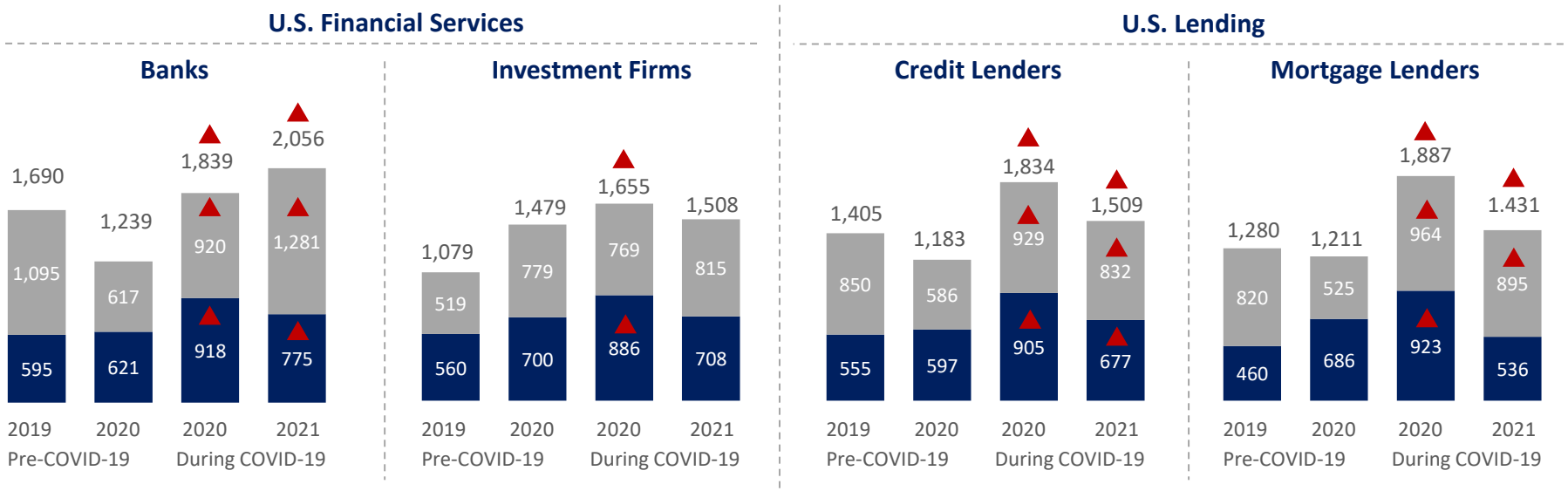
U.S. Mortgage
The average volume of monthly attacks has also increased for **mid/large mortgage firms (from 1,452 to 1,655).**

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 pre-COVID-19

Average Monthly Fraud Attacks

Avg. Number Prevented Monthly Fraud Attacks
Avg. Number Successful Monthly Fraud Attacks (U.S.)



[1] https://www.wsj.com/articles/SB10001424052748703824304575435383161436658

Canadian financial services and lending firms have experienced a significant increase in the percent of fraud attributed to international transactions.

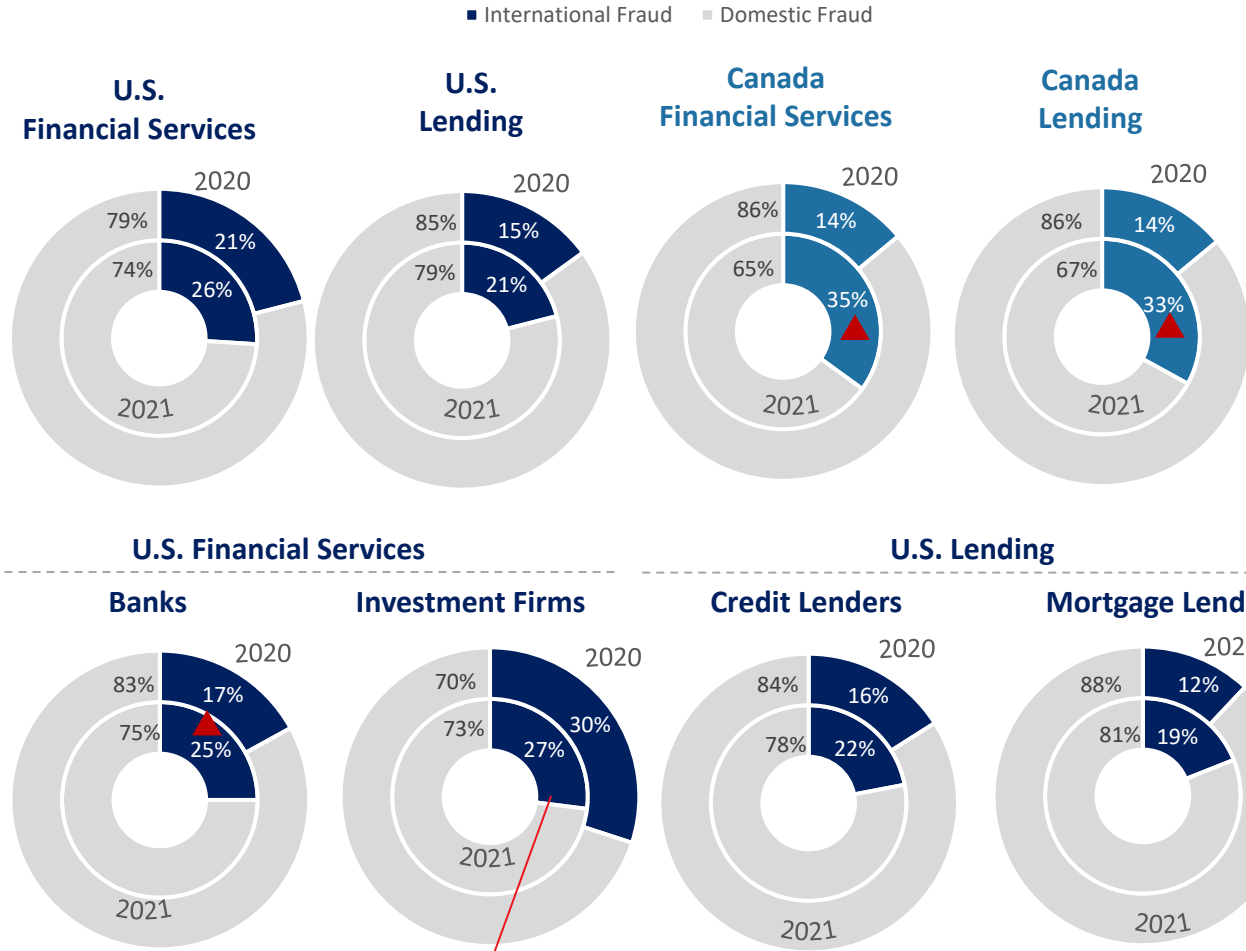
U.S. firms have had only a directional increase, with investment firms continuing to record the highest percent of fraud from international transactions (39% in 2021, 34% in 2020).

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.

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

% Fraud from Domestic and International Transactions



SEGMENT HIGHLIGHTS

U.S. Investment Firms - M/L = 39%

Key Finding 2

The mobile channel continues to impact higher fraud costs and volumes, as financial services and lending firms say that criminals have particularly targeted this channel for fraud during the pandemic.

Where mobile transactions are, fraudsters tend to follow. As banks and mortgage lenders have conducted more transactions through the mobile channel, these firms have also begun to attribute more of their fraud costs to it.

And these two segments are getting hit harder by fraud costs and volume as noted earlier.

Some of this can be the relational overlap between these types of organizations where fraud involves loan originations.

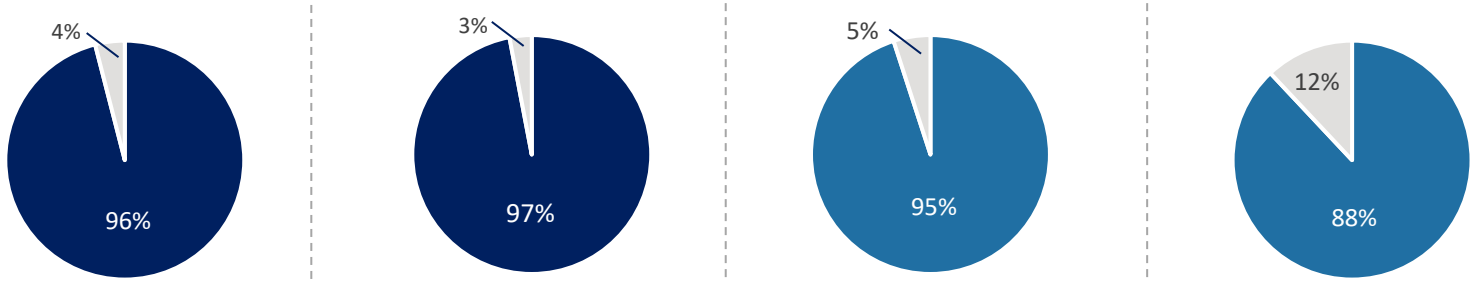
But across financial services and lending firms, there is a significant rise in the percent of transactions that are malicious bots. Without support from digital identity and transaction fraud detection solutions, it is difficult to identify such bots, as well as other types of fraudulent transactions involving synthetic identities.

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

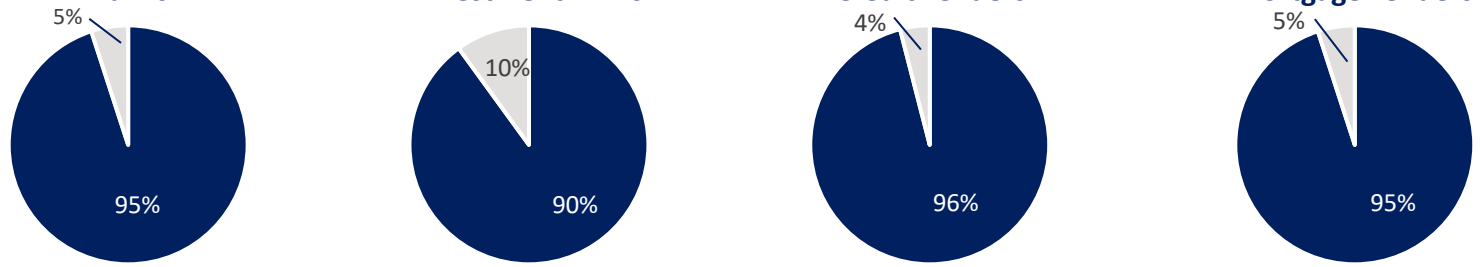
The percent of financial services and lending firms which offer mobile channel transactions remains high, continuing a significant increase since the start of the pandemic.

Businesses Offering Mcommerce

Allow Mcommerce | Do not allow Mcommerce



	U.S. Financial Services	U.S. Lending	Canada Financial Services	Canada Lending
% Allowing Mcommerce in 2020	91%	93%	94%	87%
% Allowing Mcommerce in 2019	68%	71%		



	Banks	Investment Firms	Credit Lenders	Mortgage Lenders
% Allowing Mcommerce in 2020	94%	84%	92%	95%
% Allowing Mcommerce in 2019	77%	59%	71%	71%

Both online and mobile have become the dominant channels for U.S. banks and mortgage lenders since the start of the pandemic.

A significant shift to remote transactions isn't surprising given early COVID-19 period shutdowns.

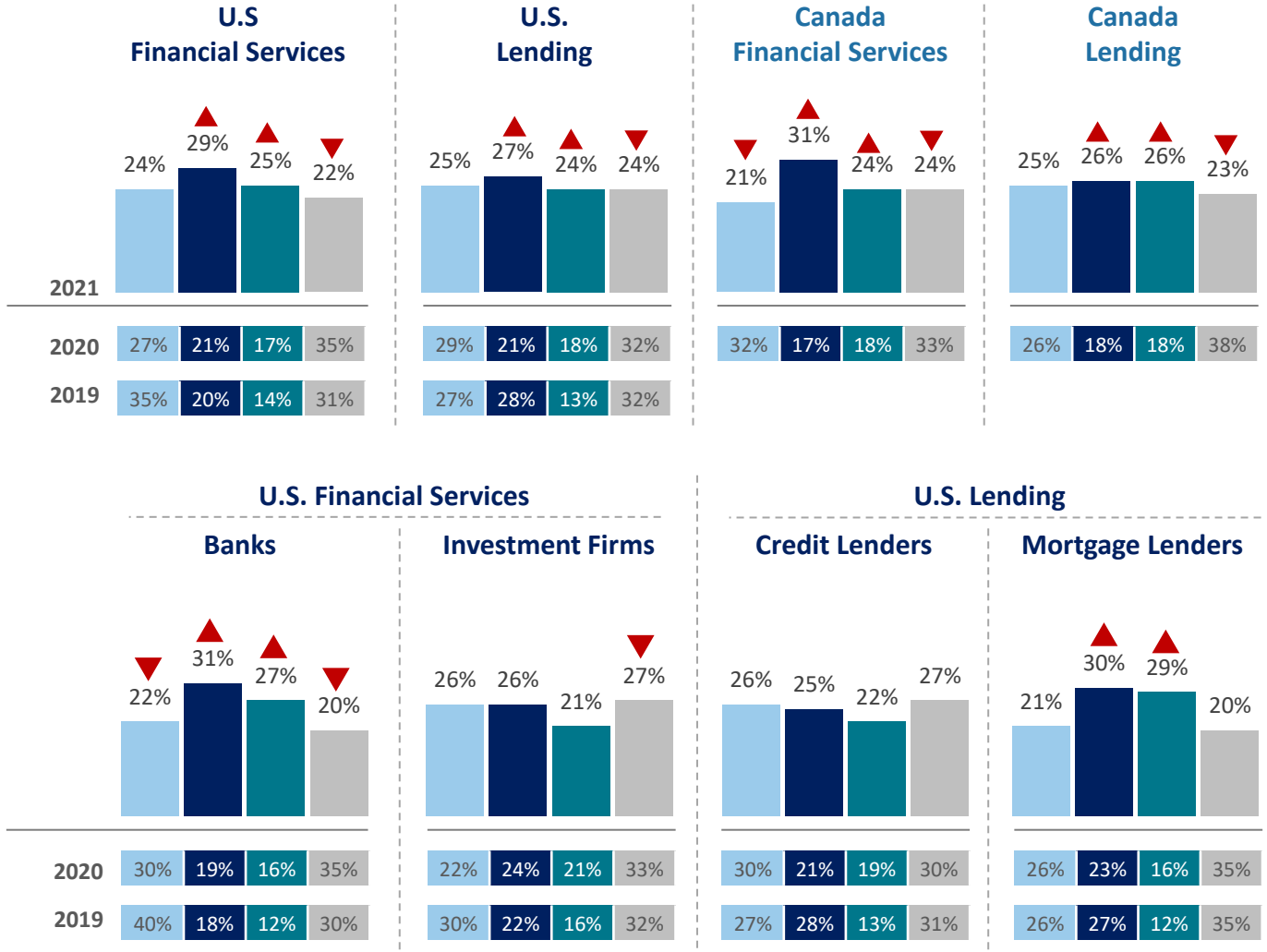
Some of the mobile channel growth is due to changed consumer environments/behaviors. Working remotely did not necessarily mean more laptop time; blurring home and office did allow for more mobile device time (free from the boss' eyes).

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

% Transaction Volume by Channel

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



Mobile channel transactions continue to increase as a contributor to U.S. financial services firms' fraud costs.

This is driven by a significant increase of mobile channel-related fraud costs among U.S. banks since the start of the pandemic.

U.S. financial services and lending firms with higher volumes of mobile transactions attribute a higher percentage of fraud costs to that channel compared to those with less mobile transaction volume. They also have a higher cost of fraud.

MOBILE = FRAUD

U.S. FINANCIAL SERVICES FIRMS

- Above avg. mobile transactions (>25%); percent of fraud costs from **mobile = 33%, with a Fraud Multiplier™ of $4.01**.
- Below avg. mobile transactions (<25%); % fraud costs from **mobile = 19%, with a Fraud Multiplier™ of $3.63.**

U.S. LENDING FIRMS

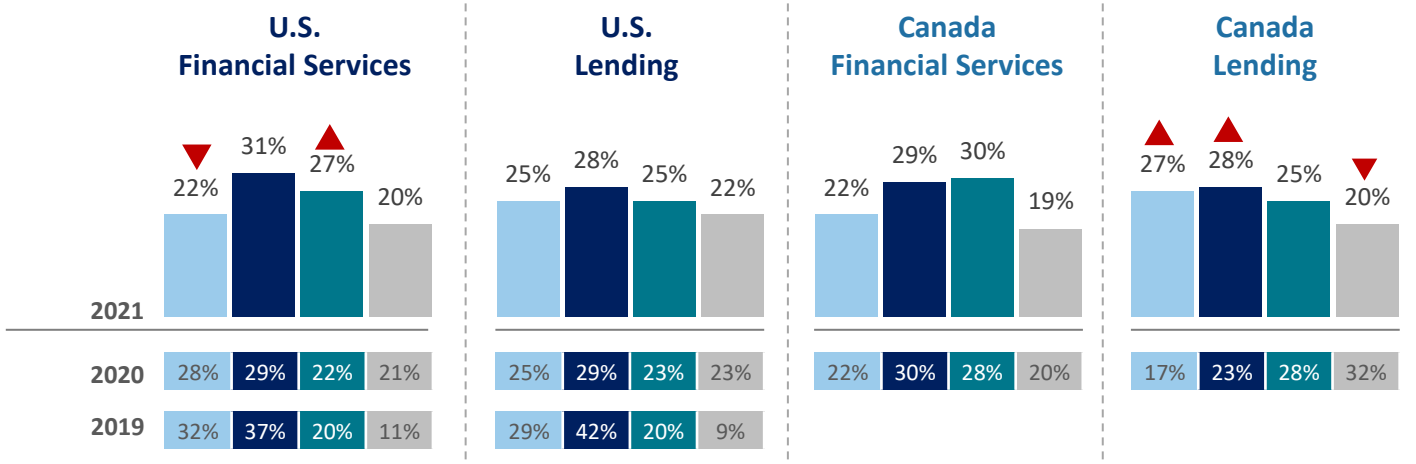
- Above avg. mobile transactions (>25%); percent of fraud costs from **mobile = 33%, with a Fraud Multiplier™ of $4.42**.
- Below avg. mobile transactions (<25%); % fraud costs from **mobile = 18%, with a Fraud Multiplier™ of $3.79.**

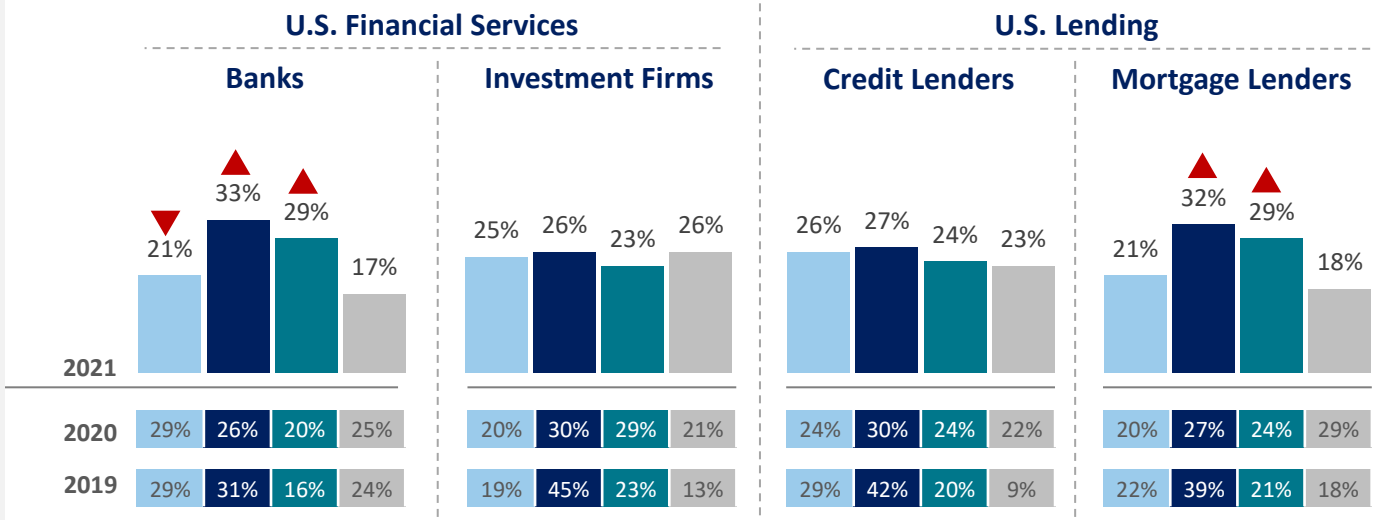
Survey Questions:
Q15. Please indicate the percent of fraud costs generated through each of the following transaction channels used by your company.

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

% Fraud Costs by Channel

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





And where transactions are, fraudsters go. Nearly all U.S. financial services and lending firms surveyed said that there has been an increase in fraud targeting mobile channel transactions.

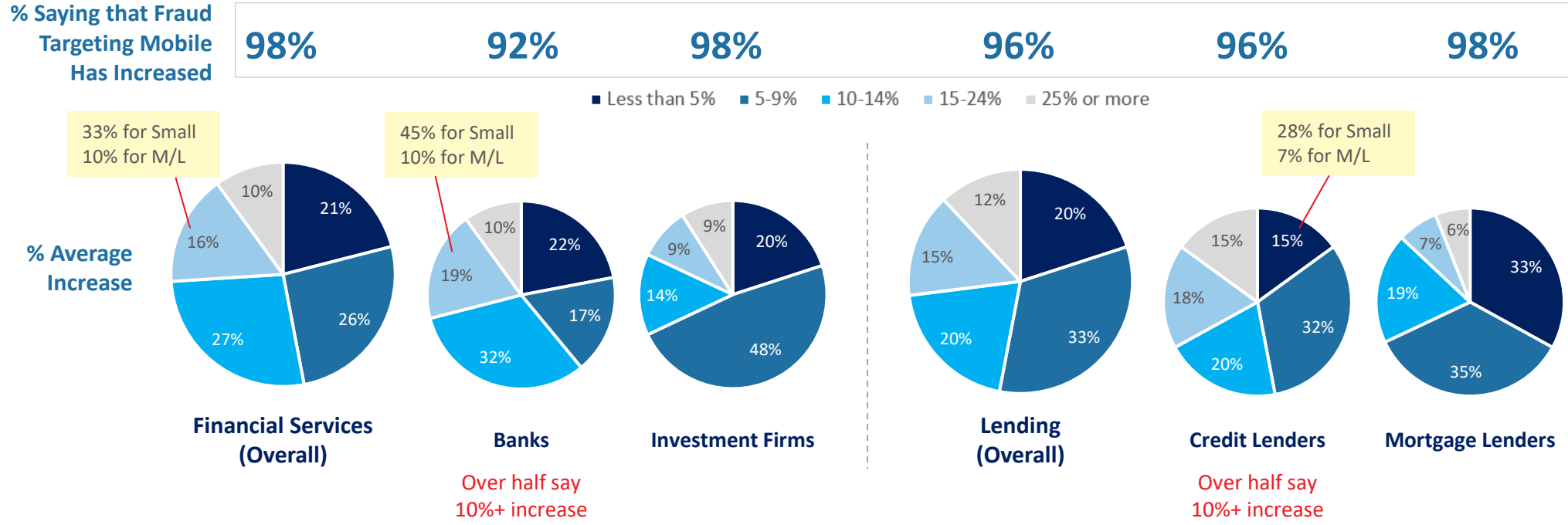
More than half of U.S. banks and credit lenders indicated a 10% or more increase in mobile channel fraud.

Survey Questions:
Q17B: To what degree has fraud that targets your mobile channel transactions increased during the past 12 months?

= significantly or directionally higher/lower than previous period

Fraud Targeting Mobile Channel Transactions

U.S. Financial Services vs. Lending



Similarly, nearly all Canadian financial services and lending firms surveyed said that there has been an increase in fraud targeting mobile channel transactions.

Compared to U.S. firms, the average percentage increase is slightly lower for Canadian firms (up to 9%), but still sizeable.

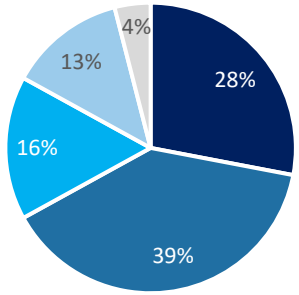
Fraud Targeting Mobile Channel Transactions

Canada Financial Services vs. Lending

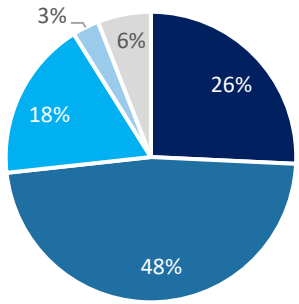
% Saying that Fraud Targeting Mobile Has Increased

95%	89%

% Average Increase



Financial Services (Overall)



Lending (Overall)

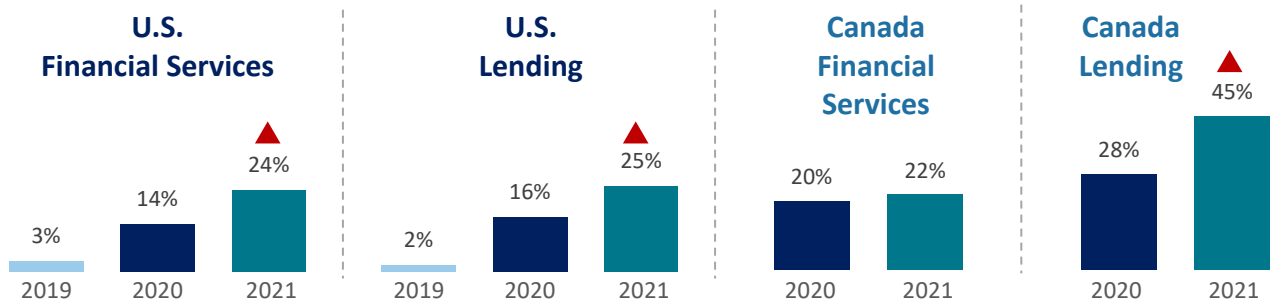
Less than 5% | 5-9% | 10-14% | 15-24% | 25% or more

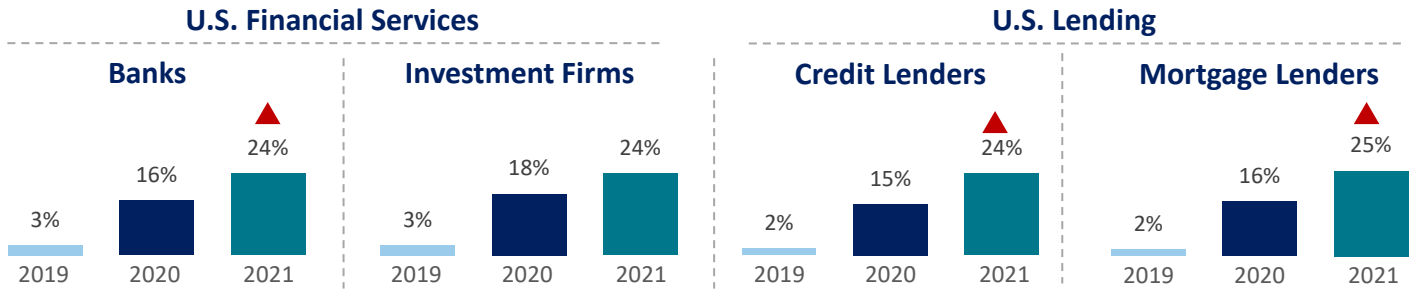
Survey Questions:
Q17B: To what degree has fraud that targets your mobile channel transactions increased during the past 12 months?

= significantly or directionally higher/lower than previous period

The average percent of transactions representing malicious botnet attacks has increased significantly for U.S. banks and lending firms.

Average % of Transactions Determined as Malicious Bot Attacks





Survey Questions:
B1: In a typical month, what percent of your transactions are determined to be malicious automated bot attacks (i.e., rapid creation and placement of hundreds of orders/transactions by fraudulent automated bots at the same time)?

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

SEGMENT HIGHLIGHTS

U.S. Financial Services

- Bot Attacks: S = 15%; M/L = 28%

SEGMENT HIGHLIGHTS

U.S. Investment Firms

- Bot Attacks: S = 12%; M/L = 34%

Key Finding 3

Fraud losses are occurring across the customer journey, though the point of funds distribution is seen as most susceptible for fraud by many, with banks and mortgage firms also indicating new account creation. Identity verification is a top challenge, while others are more specific to journey points. Study findings show that layering specific digital identity solutions at different journey points can lessen these challenges.

Identity verification, including digital attributes, is a top challenge across the customer journey. This aligns with identity fraud representing a significant percent of fraud losses at the point of funds distribution while these losses continue to grow with new account openings as well.

There are additional challenges that tend to be more pronounced for banks and mortgage lenders at certain points in the journey.

- For banks, balancing fraud detection with customer friction is a top challenge with new account openings and account logins, while identifying malicious bots and the transaction origination are more concerning at funds distribution.
- Mortgage lenders tend to rank balancing fraud detection with customer friction, identifying malicious bots and knowing the transaction origination as top challenges across the customer journey. But they are also more likely than others to include lack of tools to detect and prevent international fraud, especially with account takeover.

Financial services and lending firms are taking a limited approach in their use of fraud detection solutions across the customer journey. This weakens fraud prevention efforts and contributes to the above challenges.

As challenges and the nature of the transaction/customer interaction changes by journey point, there is no single solution to address these issues. A multi-layered solutions approach is required, particularly including those which assess the digital identity and transaction risk. Different combinations may be required at different stages. For example, this could include layering behavioral biometrics with other digital identity solutions for new account creation; laying device assessment tools at the point of funds distribution; and both of these layers plus other biometrics at account login.

Study findings show that the above layering approach can significantly reduce the challenges across each customer journey point.

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

New Account Opening	Account Login	Distribution of Funds
On-boarding a new customer Establishing a new account	Accessing an account	Disbursing funds from a bank or investment account Disbursing funds for a loan
Verifying new identity, credentials	Verifying identity before allowing access to the account	Verifying identity before distribution of funds

Fraud losses are occurring across the customer journey for U.S. financial services and lending firms, though distribution of funds is perceived to be most susceptible to fraud.

Directionally, U.S. banks and mortgage lenders attribute somewhat more losses at account login, with roughly one-third saying that this is most susceptible to fraud. But, there is still a sizeable percentage occurring at distribution of funds where these firms feel most vulnerable, as do credit lenders.

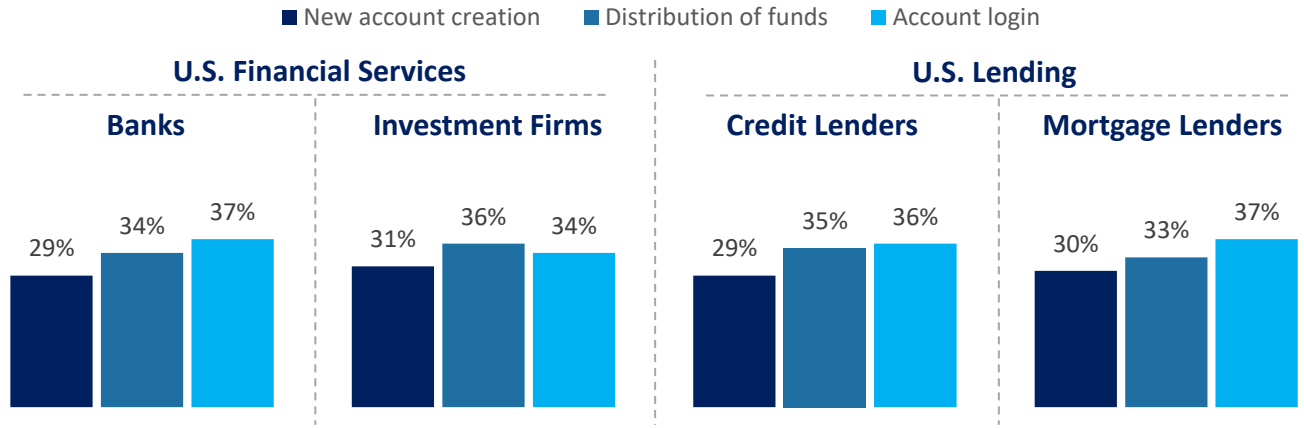
The exception to this is with investment firms, with just under half pointing to new account creation as generating the most fraud risk.

The COVID-19 pandemic saw a rise in phishing scams designed to trick consumers into giving away their passwords and account information in response to seemingly legitimate messages from their bank.[2] This contributes to fraud at both the account login and payments/funds distribution points in the customer journey.

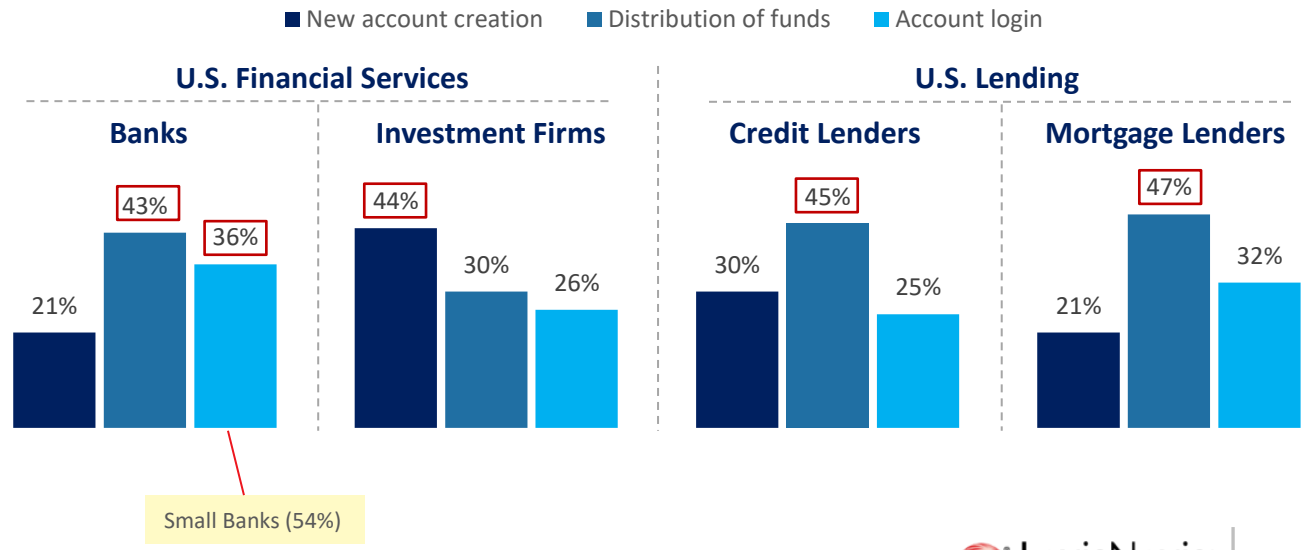
Survey Questions:
Q11B: Approximately, how much of your fraud losses would you attribute to each of the customer journey stages: new account creation (fraudulent new accounts), distribution of funds and account login/security (i.e., related to account takeover)?

= significantly or directionally higher than same response in other segment within the same industry

% Distribution of Fraud Losses by Customer Journey Stages



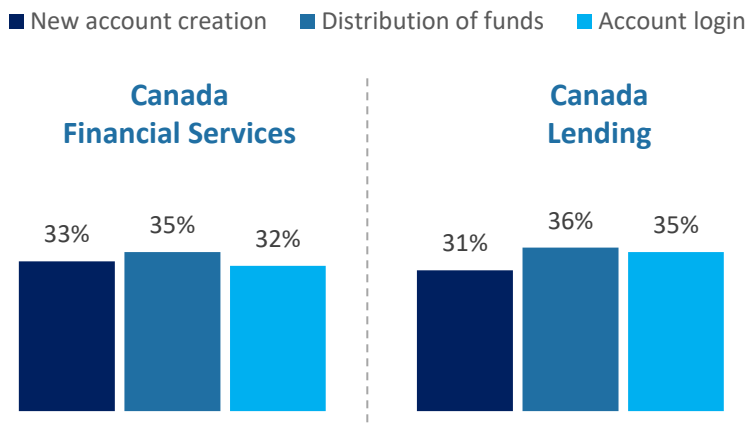
Customer Journey Stage MOST Susceptible to Fraud



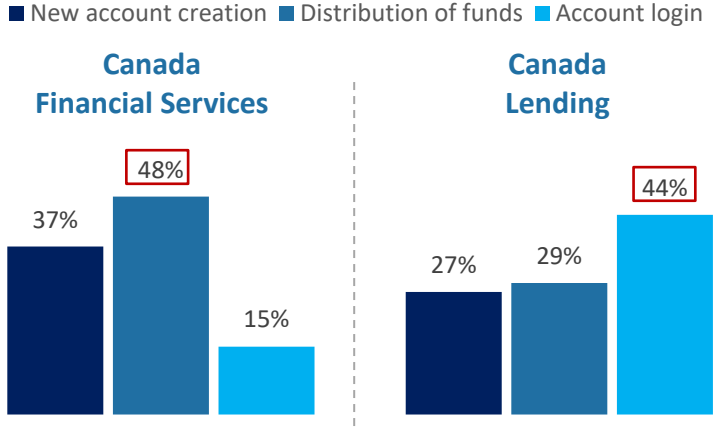
[2] https://www.atmmarketplace.com/articles/cyber-fraud-surges-as-covid-19-changes-banking-e-commerce-2

Fraud losses are also occurring across the customer journey for Canadian financial services and lending firms, though they differ on which part is most susceptible to fraud.

% Distribution of Fraud Losses by Customer Journey Stages



Customer Journey Stage MOST Susceptible to Fraud



Survey Questions:
Q11B: Approximately, how much of your fraud losses would you attribute to each of the customer journey stages: new account creation (fraudulent new accounts), distribution of funds and account login/security (i.e., related to account takeover)?

= significantly or directionally higher than same response in other segment within the same industry

Identity verification, including digital identities through devices, email and phone numbers, is a top online and mobile challenge for U.S. banks and investment firms at various points along the customer journey.

This contributes to other challenges related distinguishing malicious bots from legitimate customers, manual reviews, determining origination source and optimizing risk assessment with the customer experience.

There are issues that are more of a top challenge for certain journey points than others. Balancing fraud with friction is more of an account creation/login challenge for banks than at the point of funds distribution, where identifying malicious bots and determining the transaction source become more pressing.

Survey Questions:
Q20B: Please rank the top 3 challenges for each customer journey stage related to fraud faced by your company when serving customers using the MOBILE channel.

= significantly or directionally higher than same response in other segment within the same industry

⚠ = point of customer journey selected by many as being most susceptible to fraud

U.S. Financial Services

	Account Opening		Account Login		Distribution of Funds	
	Banks ⚠	Investment Firms ⚠	Banks ⚠	Investment Firms	Banks ⚠	Investment Firms
Top Online Channel Challenges	• Balancing fraud with friction (35%) • **Verification** – Address (34%) – Identity (31%)	• Manual reviews (42%) • Phone number **verification** (37%)	• **Verification** – Address (41%) – Phone # (32%) – Identity (29%) – Email, device (34%) • ID malicious bots (29%)	• **Verification** – Address (36%) – Email, device (32%)	• **Verification** – Phone # (36%) – Identity (31%) • Identifying malicious bots (34%) • Knowing origination source (31%)	• **Verification** – Address (37%) – Identity (32%) • Assessing risk by country (33%)
Top Mobile Channel Challenges	• Balancing fraud with friction (32%) • **Verification** – Address (36%) – Identity (36%) – Email, device (31%)	• Assessing risk by country (43%) • Address **verification** (39%)	• Balancing fraud with friction (34%) • Phone number **verification** (33%) • ID malicious bots (32%)	• Manual reviews (38%) • Address **verification** (32%)	• Identifying malicious bots (32%) • ID **verification** (30%) • Knowing origination source (31%) • New payment methods (32%)	• **Verification** – Address (30%) – Identity (32%) – Phone # (32%)

Identity verification is also a top online and mobile challenge for U.S. lending firms. Additionally, there are challenges with assessing fraud from other countries and determining origination source while trying to balance fraud detection with friction.

At the same time, there is limited use of fraud assessment solutions among lenders that can provide insights into transaction risk and location as well as distinguishing malicious bots from legitimate customers.

Unlike with banks, balancing fraud detection with customer friction, identifying malicious bots and determining the transaction origination source are mortgage firm challenges across the customer journey. There is also need for tools that can support detection of international-based fraud.

Survey Questions:
Q20B: Please rank the top 3 challenges for each customer journey stage related to fraud faced by your company when serving customers using the MOBILE channel.

= significantly or directionally higher than same response in other segment within the same industry

⚠ = point of customer journey selected by many as being most susceptible to fraud

U.S. Lending Firms

	Account Opening		Account Login		Distribution of Funds	
	Credit Lending	Mortgage Firms	Credit Lending ⚠	Mortgage Firms ⚠	Credit Lending	Mortgage Firms
Top Online Channel Challenges	• **Verification** – Address (39%) – Identity (32%)	• **Verification** – Address (43%) – Phone # (38%) – Email/device (29%) • Identifying malicious bots (29%)	• **Verification** – Phone # (41%) – Identity (33%) – Email, device (31%) – Address (30%) • Assessing fraud by country (30%)	• **Verification** – Email, device (39%) – Identity (32%) • Lack tools for international fraud (35%)	• **Verification** – Address (32%) – Identity (31%) • Identifying malicious bots (34%) • Knowing origination source (29%)	• Manual reviews (46%) • Balancing fraud w/ friction (41%) • Knowing origination source (38%) • ID verification (30%)
Top Mobile Channel Challenges	• **Verification** – Identity(40%) – Phone # (29%) – Address (34%)		• Balancing fraud with friction (34%) • Phone number **verification** (33%) • ID malicious bots (32%)	• Lack tools for international fraud (46%) • Manual reviews (35%) • Identifying malicious bots (33%) • Phone # **verification** (32%)	• Knowing origination source (34%) • Balancing fraud w/ friction (33%) • Identifying malicious bots (32%) • ID **verification** (30%)	

Survey Questions:
Q20B: Please rank the top 3 challenges for each customer journey stage related to fraud faced by your company when serving customers using the MOBILE channel.

= significantly or directionally higher than same response in other segment within the same industry

⚠ = point of customer journey selected by many as being most susceptible to fraud

Identity verification is also a top online and mobile challenge for Canadian financial services and lending firms, as well as with international fraud and balancing fraud detection with friction.

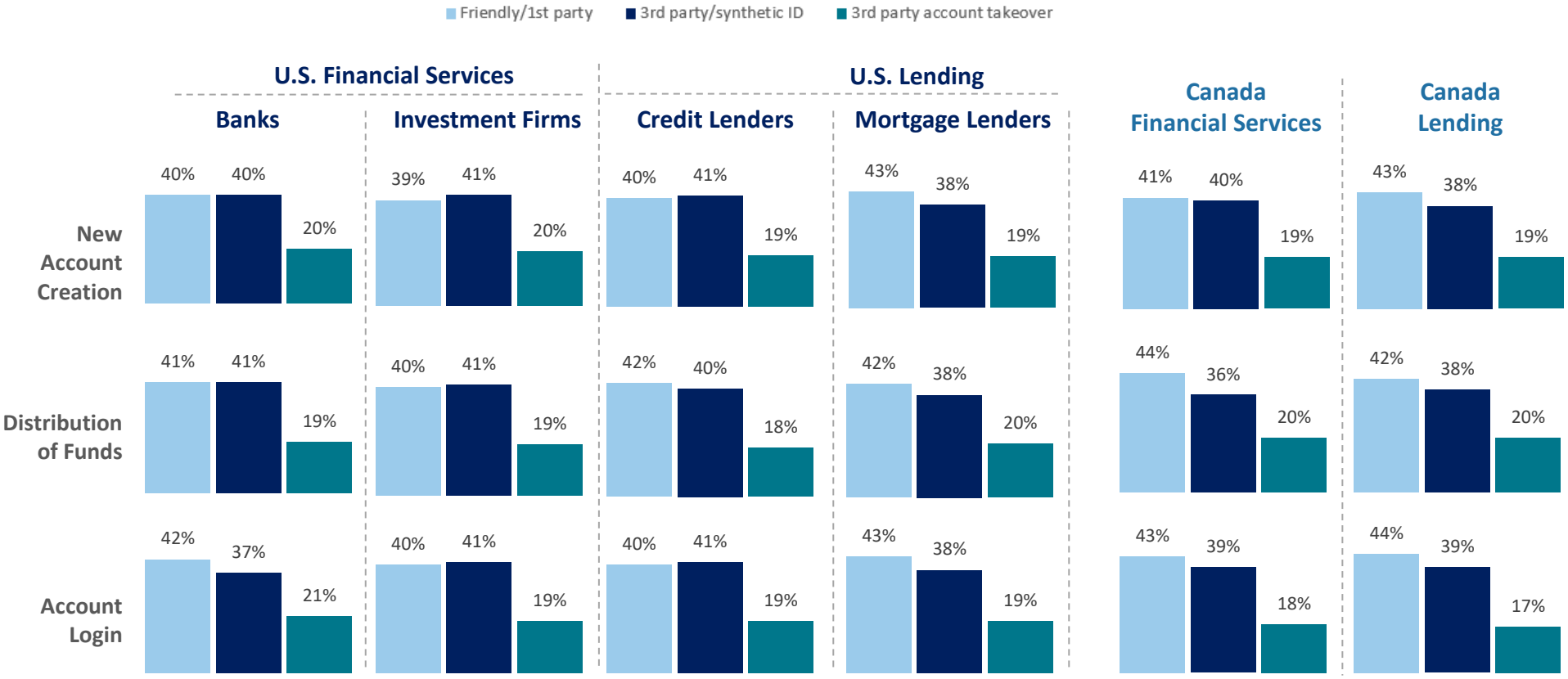
As with other segments, this contributes to other challenges related distinguishing malicious bots from legitimate customers, manual reviews and determining origination source.

Canadian Financial Services and Lending

	Account Opening		Account Login		Distribution of Funds	
	Financial Services	Lending	Financial Services ⚠	Lending	Financial Services	Lending ⚠
Top Online Channel Challenges	• Manual reviews (32%) • Balancing fraud w/ friction (31%) • **Verification** – Email, device (33%) – Identity (32%)	• Balancing fraud w/ friction (40%) • **Verification** – Address (44%) – Phone # (38%)	• Lack tools for international fraud (40%) • Assessing fraud by country (28%) • **Verification** – Phone # (33%) – Identity (32%)	• Identifying malicious bots (39%) • **Verification** – Identity (32%) – Email, device (31%) – Phone # (30%)	• **Verification** – Phone # (32%) – Identity (31%) • Lack tools for international fraud (35%) • Knowing origination source (34%) • Balancing fraud w/ friction (33%)	• Lack tools for international fraud (47%) • Assessing risk by country (44%) • Knowing origination source (39%)
Top Mobile Channel Challenges	• **Verification** – Identity (47%) – Address (31%) • Balancing fraud w/ friction (31%) • Knowing origination source (28%)	• **Verification** – Identity (43%) – Phone # (31%) • Assessing risk by country (40%) • Identifying malicious bots (33%)	• Assessing fraud by country (46%) • Address **verification** (30%) • ID malicious bots (30%) • Knowing transaction source (30%)	• Phone # **verification** (44%) • Assessing risk by country (36%) • Lack tools for international fraud (30%)	• Identifying malicious bots (41%) • Knowing origination source (34%) • **Verification** – Email, device (36%) – Phone (32%)	• Knowing origination source (54%) • Lack tools for international fraud (49%) • New transaction methods (41%) • Manual reviews (36%)

Friendly/first party and third party/synthetic identity fraud are driving financial services and lending fraud losses across the customer journey.

% Distribution of Fraud Losses by Fraud Type



Survey Questions:
Q12aa, Q12bb, Q12cc: For each specific customer journey stage, please indicate the percentage distribution your past 12-month's fraud losses across the following fraud methods.

Identity-related fraud is occurring similarly across the customer journey for U.S. financial services and lending firms, with new account creation continuing its upward trend as a source of this type of fraud.

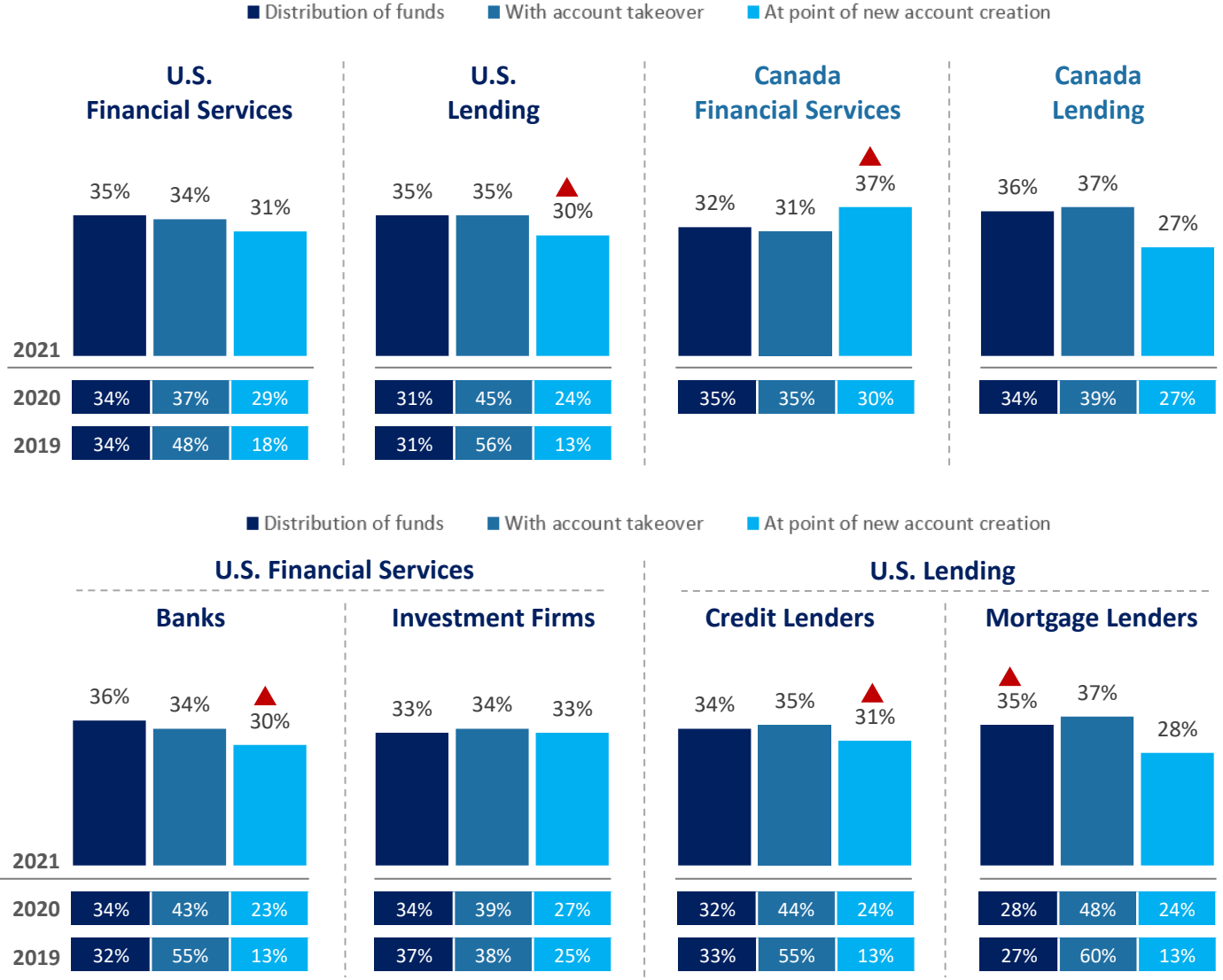
Increased identity-fraud related to new account creation has primarily come from U.S. banks and credit lenders, though this is not perceived as the most susceptible part of the customer journey for them.

Canadian financial services firms also attributed an increased percentage of identity-related fraud to new account creation, though again distribution of funds is viewed as being the riskier customer journey point.

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

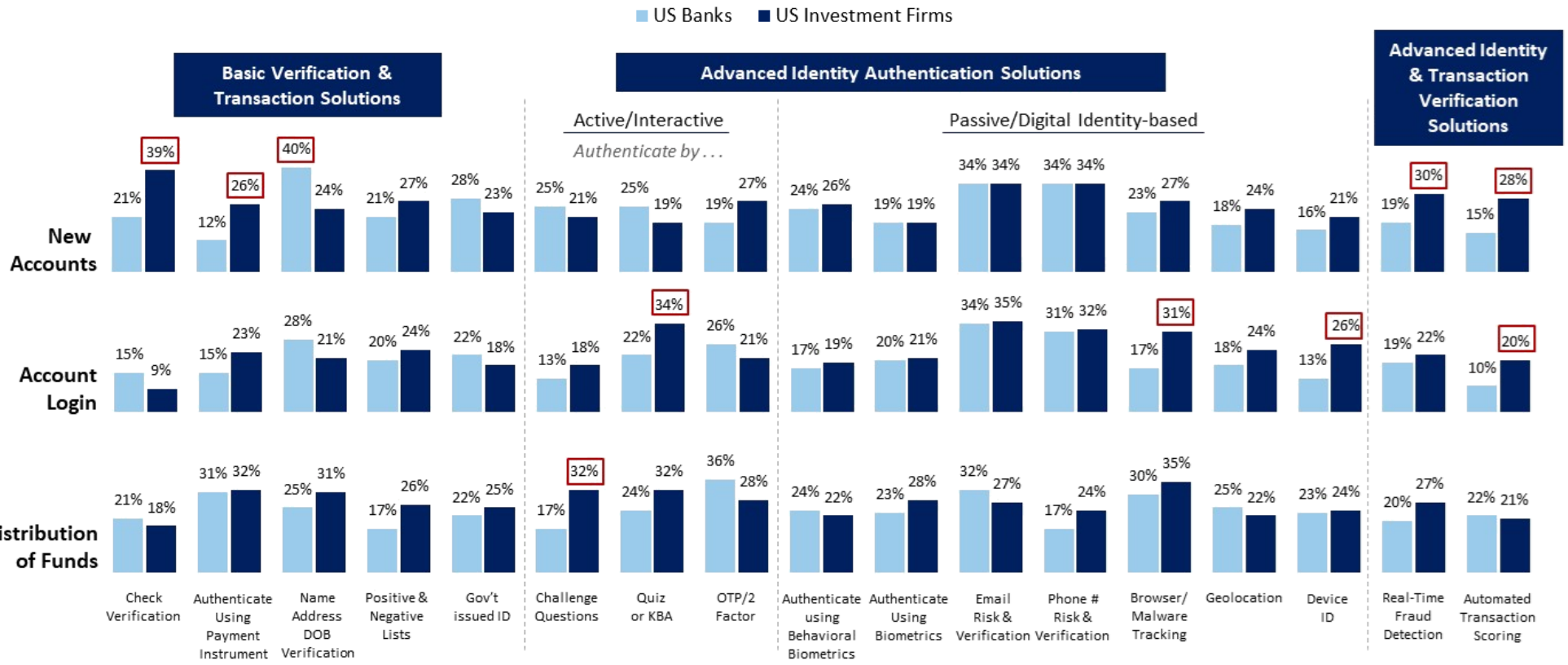
Identity-Related Fraud: % Distribution by Activity



Across the customer journey, there is limited financial services use of solutions to assess digital identity threats that contribute to key online and mobile channel challenges.

Latter slides illustrate case studies in which the use of a multi-layered solutions approach, involving those that detect and assess fraud within the digital channels, can lessen these challenges and increase the effectiveness of fraud verification efforts.

Fraud Mitigation Solutions Use | U.S. Financial Services



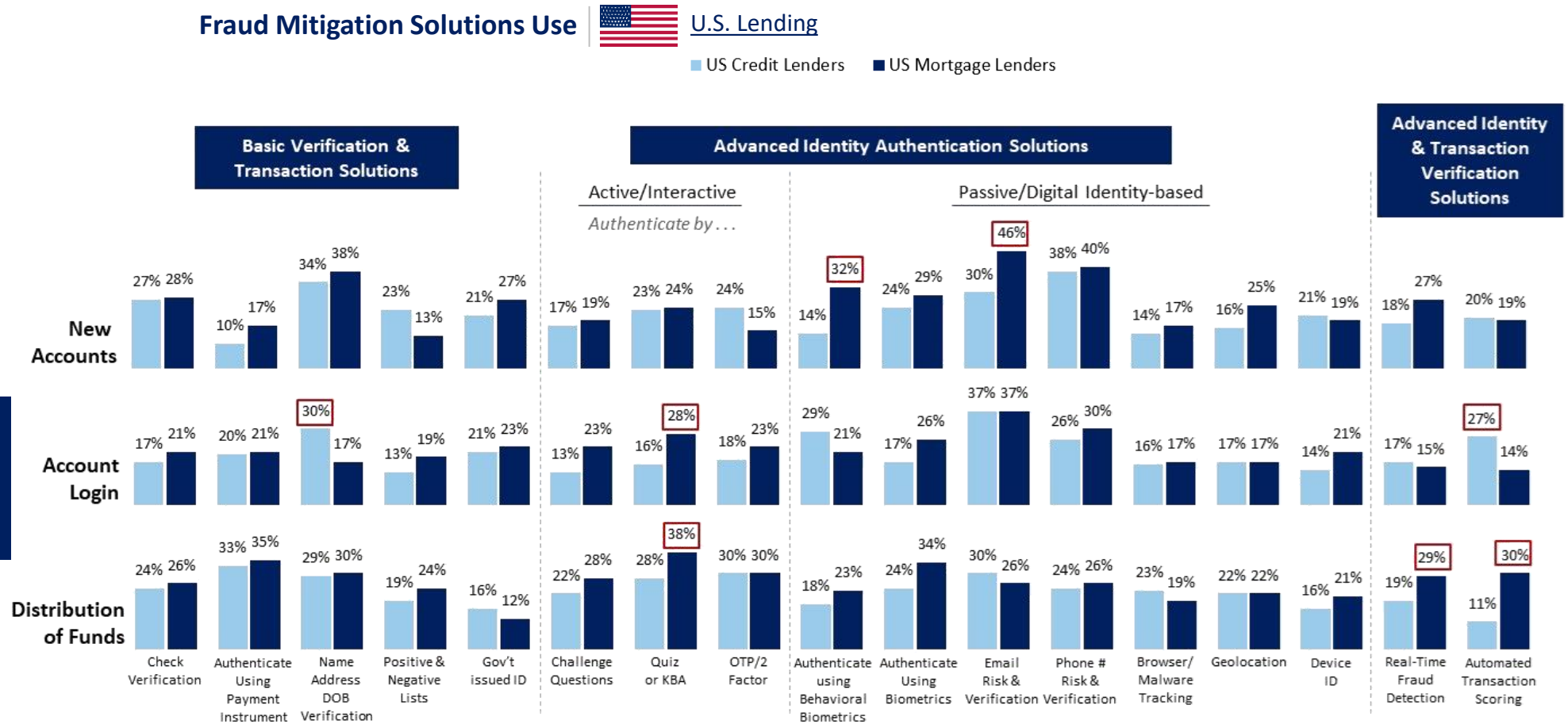
Survey Questions:
Q27: Which fraud detection/ mitigation solutions does your company currently use for the following transaction or customer journey points?

= significantly or directionally higher than same response in other segment

There is also limited use of digital identity solutions among U.S. lenders across the customer journey, with an average number of 3-4 solutions used per stage.

Survey Questions:
Q27: Which fraud detection/ mitigation solutions does your company currently use for the following transaction or customer journey points?

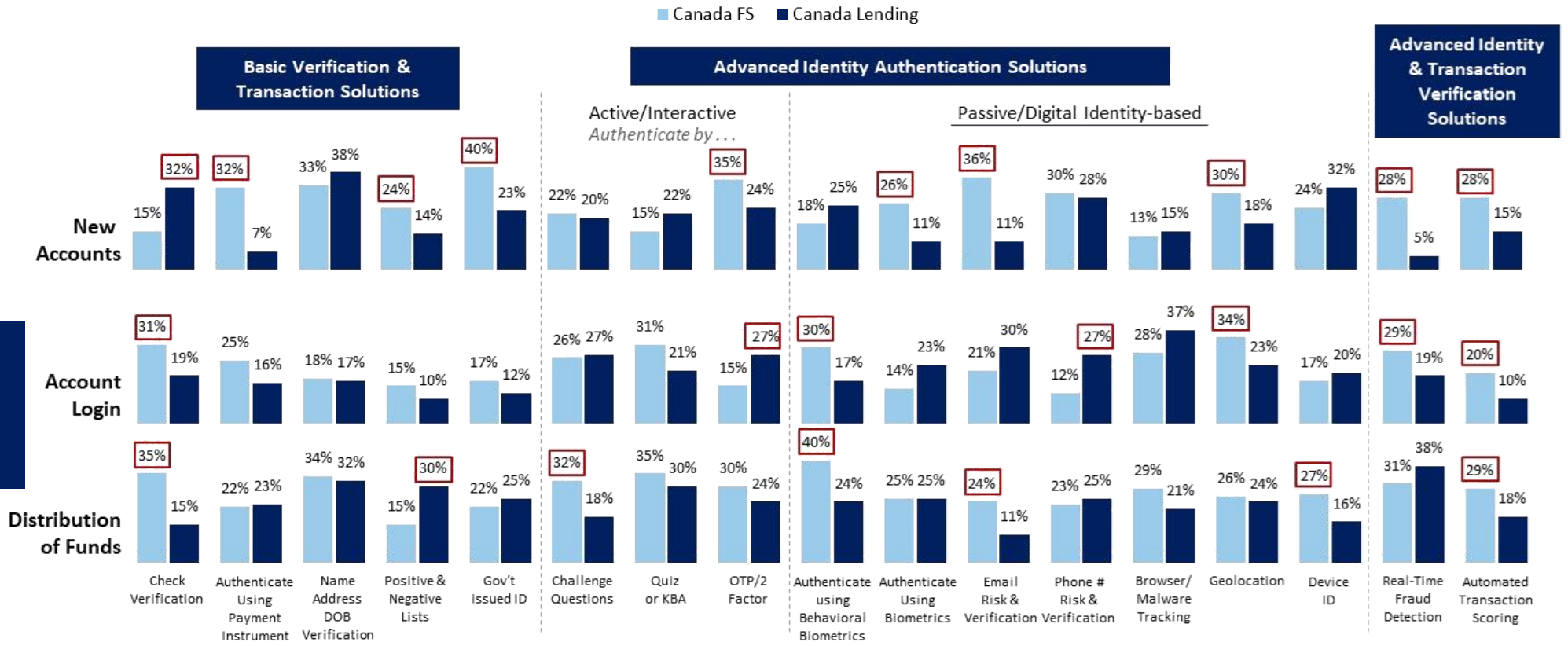
= significantly or directionally higher than same response in other segment



There is limited solutions use among Canadian financial services and lending firms.

To the degree differences emerge between financial services and lending, there is broader use of solutions by financial services firms, particularly at the new account creation and login journey points. Canadian financial services use an average of 4-5 solutions at each customer journey point, compared to 3-4 for lending firms. That said, there is varied use of specific solutions and limited use of those that support digital identity proofing.

Fraud Mitigation Solutions Use | Canada Financial Services and Lending



Survey Questions:
Q27: Which fraud detection/mitigation solutions does your company currently use for the following transaction or customer journey points?

= significantly or directionally higher than same response in other segment

Findings show that a multi-layered digital identity solutions approach, including behavioral biometrics, for new account openings is significantly more effective at verifying identities while reducing customer friction and fraud costs.*

Survey Questions:
Q20: Please rank the top 3 challenges for each customer journey stage related to fraud faced by your company when serving customers using the ONLINE/MOBILE channel.

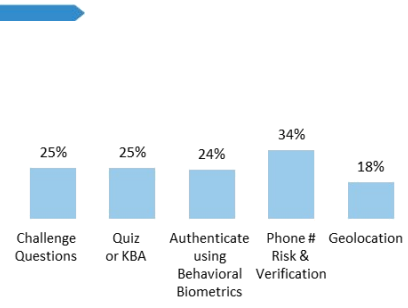
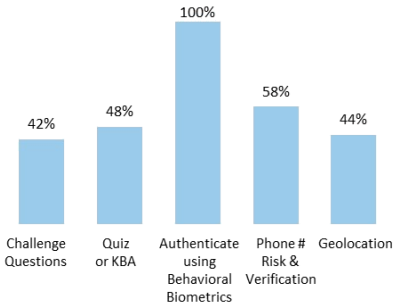
= significantly or directionally higher than same response in other segment within the same industry

= point of customer journey selected by many as being most susceptible to fraud

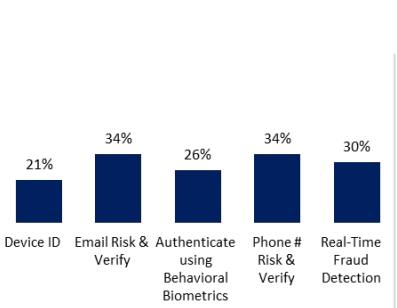
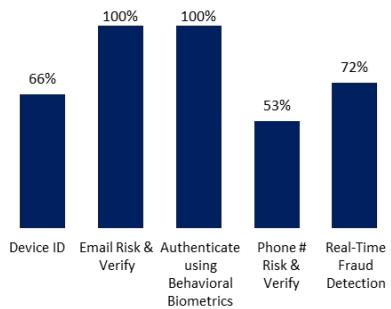
* Represents one type of multi-layered digital solutions approach; each organization has its own unique circumstances and challenges such other multi-layered combinations are required/will produce effective fraud mitigation results

Account Opening

U.S. Banks

	Limited Digital Solutions Use	Multi-Layered Digital Solutions Use Involving Behavioral Biometrics*
Fraud Mitigation Solutions Use		
Top Online Channel Challenges	• Balancing fraud w/ friction (35%) • **Verification** – Address (34%) – Identity (31%)	• Balancing fraud w/ friction (35%) • **Verification** – Address (15%) – Identity (21%)
Top Mobile Channel Challenges	• Balancing fraud w/ friction (32%) • **Verification** – Address (36%) – Identity (36%) – Email, device (31%)	• Balancing fraud w/ friction (21%) • **Verification** – Address (15%) – Identity (26%) – Email, device (21%)
Every $1 of fraud loss actually costs	**$4.00**	**$3.54**

U.S. Investment Firms ⚠

	Limited Digital Solutions Use	Multi-Layered Digital Solutions Use Involving Behavioral Biometrics*
Fraud Mitigation Solutions Use		
Top Online Channel Challenges	• Manual reviews (42%) • **Verification** – Phone # (37%) – Identity (34%)	• Manual reviews (42%) • **Verification** – Phone # (14%) – Identity (15%)
Top Mobile Channel Challenges	• Assessing risk by country (43%) • Address **verification** (39%)	• Assessing risk by country (19%) • Address **verification** (20%)
Every $1 of fraud loss actually costs	**$4.00**	**$3.68**

Digital identity solutions assessing the device, transaction and behaviors can also provide more effective fraud detection and mitigation during the account login stage.

Survey Questions:
Q20: Please rank the top 3 challenges for each customer journey stage related to fraud faced by your company when serving customers using the ONLINE/MOBILE channel.

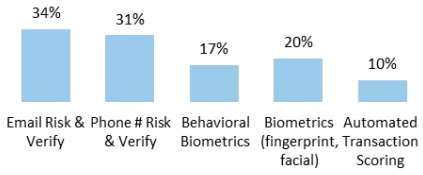
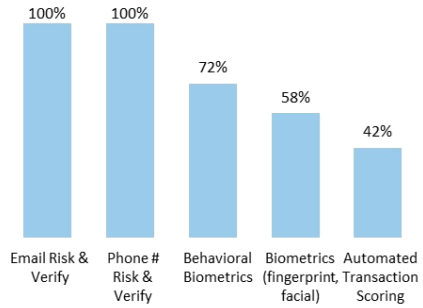
= significantly or directionally higher than same response in other segment within the same industry

= point of customer journey selected by many as being most susceptible to fraud

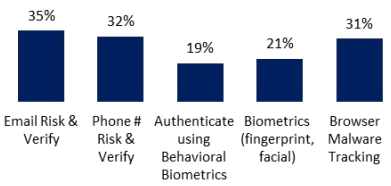
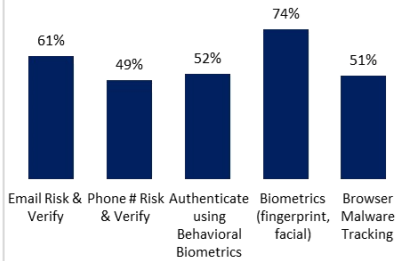
* Represents one type of multi-layered digital solutions approach; each organization has its own unique circumstances and challenges such other multi-layered combinations are required/will produce effective fraud mitigation results

Account Login

U.S. Banks

	Limited Digital Solutions Use	Multi-Layered Digital Solutions Assessing Device, Biometric Behaviors/Attributes and Transaction*
Fraud Mitigation Solutions Use		
Top Online Channel Challenges	• Identifying malicious bots (29%) • **Verification** – Address (41%) – Phone # (32%) – Identity (29%) – Email/device (34%	• Identifying malicious bots (14%) • **Verification** – Address (41%) – Phone # (14%) – Identity (14%) – Email/device (34%)
Top Mobile Channel Challenges	• Identifying malicious bots (32%) • **Phone # verification (33%)** • Balancing fraud/friction (34%)	• Identifying malicious bots (32%) • **Phone # verification (33%)** • Balancing fraud/friction (34%)
Every $1 of fraud loss actually costs	**$4.02**	**$3.82**

U.S. Investment Firms

	Limited Digital Solutions Use	Multi-Layered Digital Solutions Assessing Device, Biometric Behaviors/Attributes and Transaction*
		
	• **Verification** – Address (36%) – Email/device (32%)	• **Verification** – Address (16%) – Email/device (25%)
	• **Address verification (32%)** • Manual reviews (38%)	• **Address verification (21%)** • Manual reviews (38%)
	$3.72	**$3.67**

Survey Questions:
Q20: Please rank the top 3 challenges for each customer journey stage related to fraud faced by your company when serving customers using the ONLINE/MOBILE channel.

= significantly or directionally higher than same response in other segment within the same industry

= point of customer journey selected by many as being most susceptible to fraud

* Represents one type of multi-layered digital solutions approach; each organization has its own unique circumstances and challenges such other multi-layered combinations are required/will produce effective fraud mitigation results

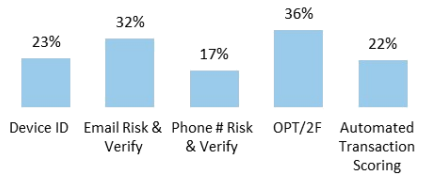
During distribution of funds, a multi-layered digital identity solutions approach assessing the device, transaction and behaviors can significantly improve identity verification by determining bots, origination source and risk by country. It can also lower costs.

Distribution of Funds

U.S. Banks

Limited Digital Solutions Use

Fraud Mitigation Solutions Use



Top Online Channel Challenges

- Identifying malicious bots (34%)
- Knowing origination source (31%)
- **Verification**
  - Phone # (36%)
  - Identity (31%)

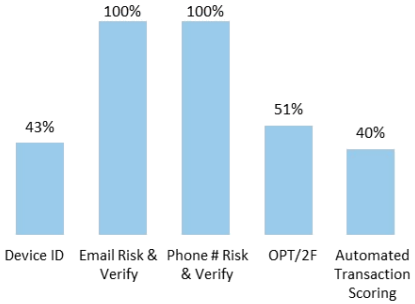
Top Mobile Channel Challenges

- Identifying malicious bots (32%)
- **Identity verification (30%)**
- Knowing origination source (31%)
- New payment methods (32%)

Every $1 of fraud loss actually costs

$4.33

Multi-Layered Digital Solutions Assessing Device and Transaction*



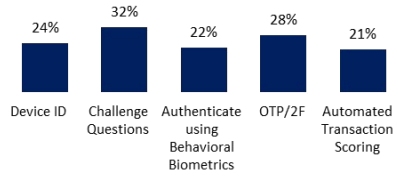
- Identifying malicious bots (17%)
- Knowing origination source (11%)
- **Verification**
  - Phone # (23%)
  - Identity (12%)

- Identifying malicious bots (22%)
- **Identity verification (12%)**
- Knowing origination source (11%)
- New payment methods (32%)

$3.37

U.S. Investment Firms

Limited Digital Solutions Use

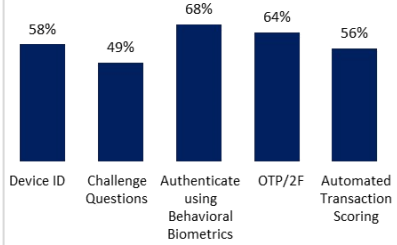


- Assessing risk by country (33%)
- **Verification**
  - Address (37%)
  - Identity (32%)

- **Verification**
  - Address (30%)
  - Identity (32%)
  - Phone # (32%)

$4.16

Multi-Layered Digital Solutions Assessing Behavioral Biometrics, Device, Transaction*



- Assessing risk by country (5%)
- **Verification**
  - Address (12%)
  - Identity (12%)

- **Verification**
  - Address (12%)
  - Identity (12%)
  - Phone # (12%)

$3.68

Key Finding 4

Best practice fraud detection and prevention includes a multi-layered solutions approach, and the integration of fraud prevention with cybersecurity operations and the digital customer experience. Laying in supportive capabilities such as social media intelligence and AI/ML further strengthens fraud prevention.

Fraud prevention must assess both the physical and digital identity attributes, as well as the risk of the transaction. Without the aid of solutions that detect digital behaviors, anomalies, device risk and synthetic identities, it is difficult for even the best trained professional to detect the increasingly sophisticated crime occurring in the remote digital channels.

Some financial services and lending firms are doing this, along with fully integrating cybersecurity operations, the digital customer experience and fraud prevention. These firms tend to have a lower cost of fraud and fewer challenges.

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

Best 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.

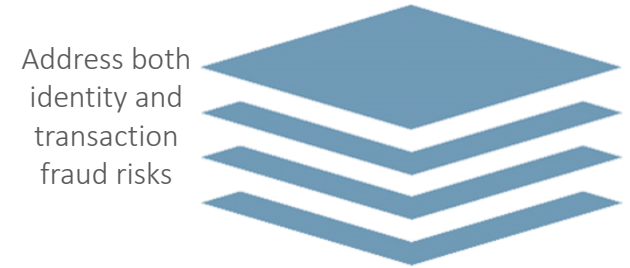
Integration

Tools and 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.



Strategy and 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

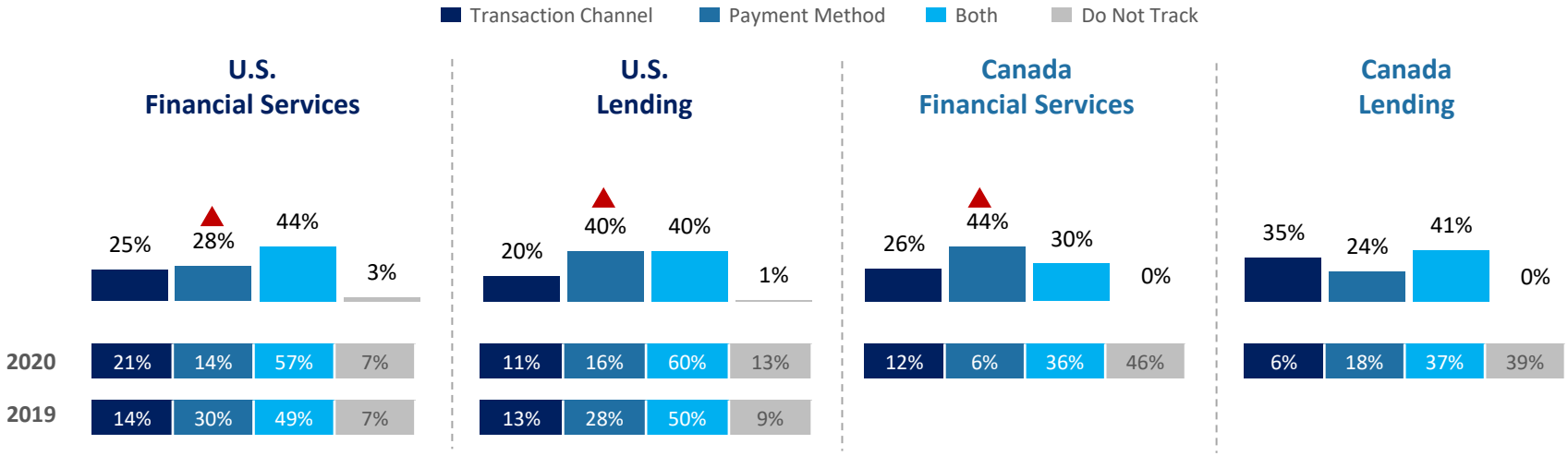
Integration of Cybersecurity and Digital Customer Experience Operations with Fraud Prevention Approach

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.

While **there are more firms tracking fraud costs by payment method compared to previous years**, there has been a drop in the number which track by both transaction channel and payment method.

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.

% Businesses Tracking Fraud Costs by Channel and/or Payment Method



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

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

Of those who do track fraud costs by payment method, a significant number of firms say that this includes tracking authorized-party fraud.

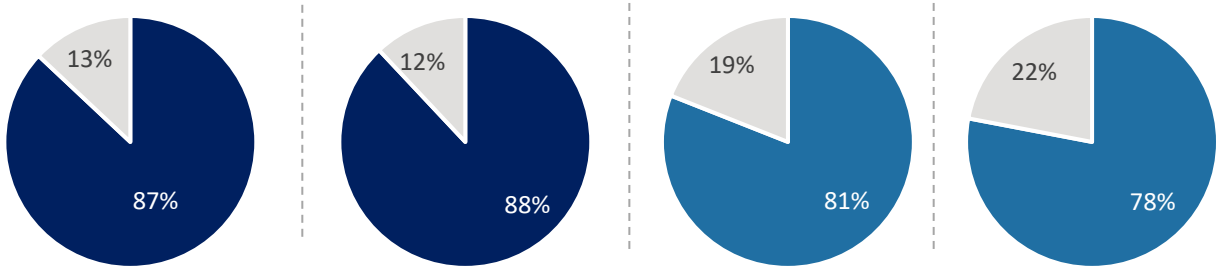
They also indicate tracking synthetic identity fraud separately from credit losses.

Survey Questions:
Q14c: Does your organization track authorized-party fraud in its overall measurement of payment method fraud?

* Asked of those whose company track cost of fraudulent transactions by transaction/payment method only or both transaction channel and method

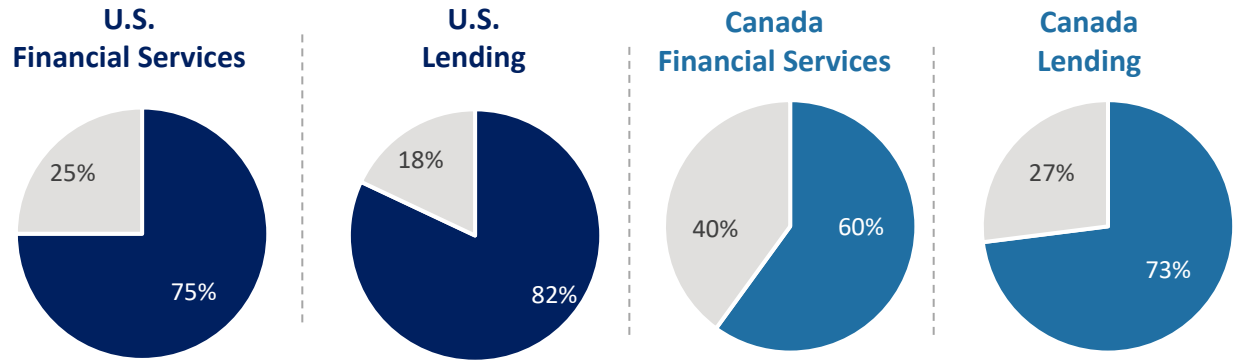
% Businesses Tracking Authorized-Party Fraud in its Measurement of Payment Method Fraud

■ Yes ■ No



% Businesses Tracking Synthetic Identity Fraud Separately From Credit Losses

■ Yes ■ No



There is sizeable familiarity with the FraudClassifier℠ Model to classify across mid/large U.S. and Canadian financial services and lending firms, with just over half or so using it to classify fraud related to payments.

Awareness and use is somewhat higher among Canadian firms. Canadian lending firms are most likely to be using this model; among firms aware but not using, roughly four in ten Canadian firms expect to do so within the next 6 months.

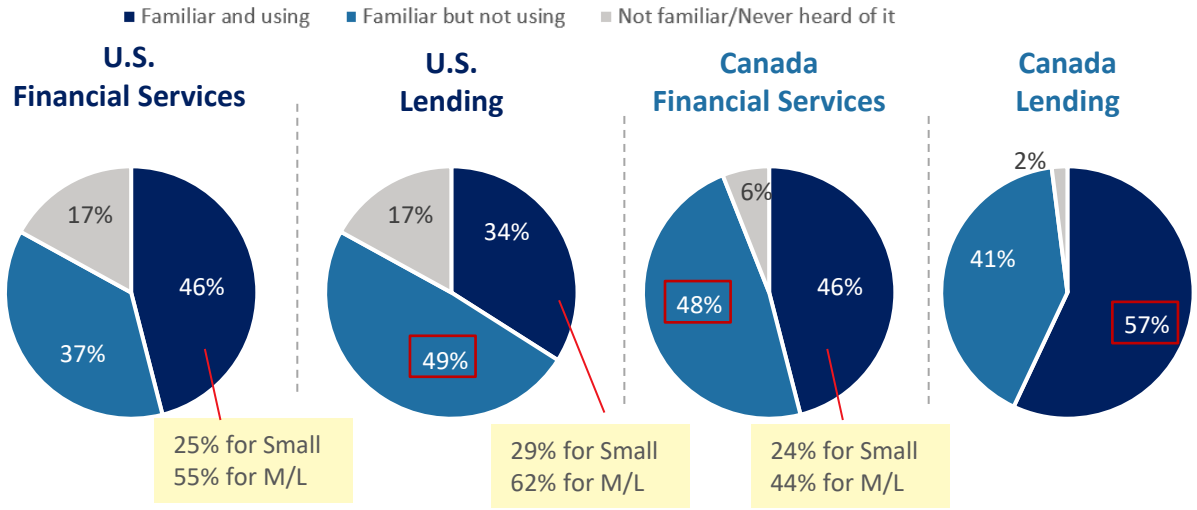
A majority of U.S. mid/large firms indicate current use of the model, with over half of those familiar and not using expecting to do so within the next 12 months.

Survey Questions:
Q14e: To what degree is your organization familiar with the FraudClassifier℠ Model, published by the Federal Reserve in June 2020, to classify fraud related to payments?

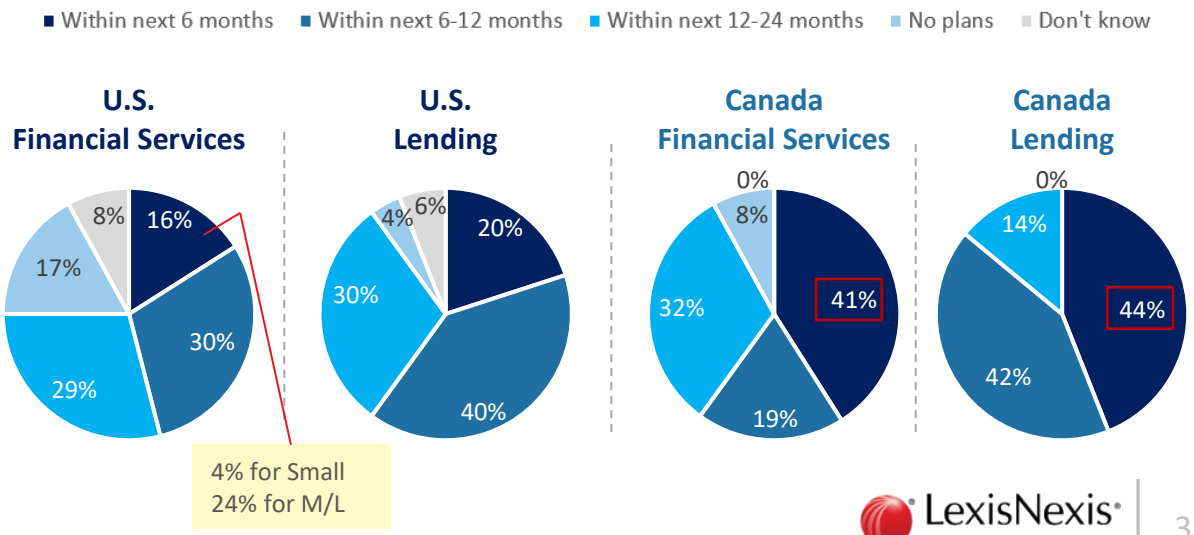
= significantly or directionally higher than same category in other industry segments

* Asked of those whose company is familiar with the FraudClassifier℠ Model but are not using it in their organization

Degree of Familiarity with FraudClassifier℠ Model



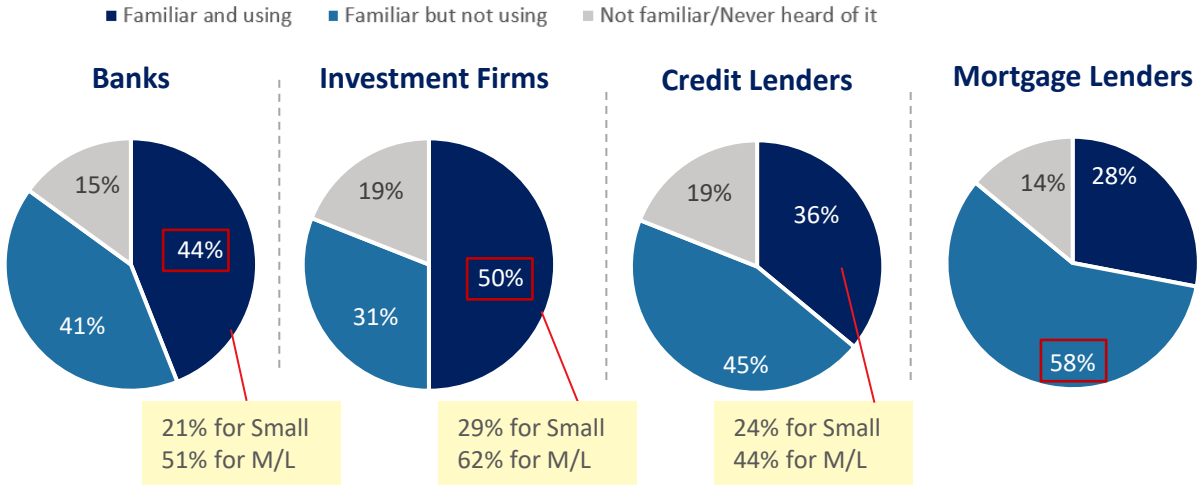
Future Plans to Use FraudClassifier℠ Model*



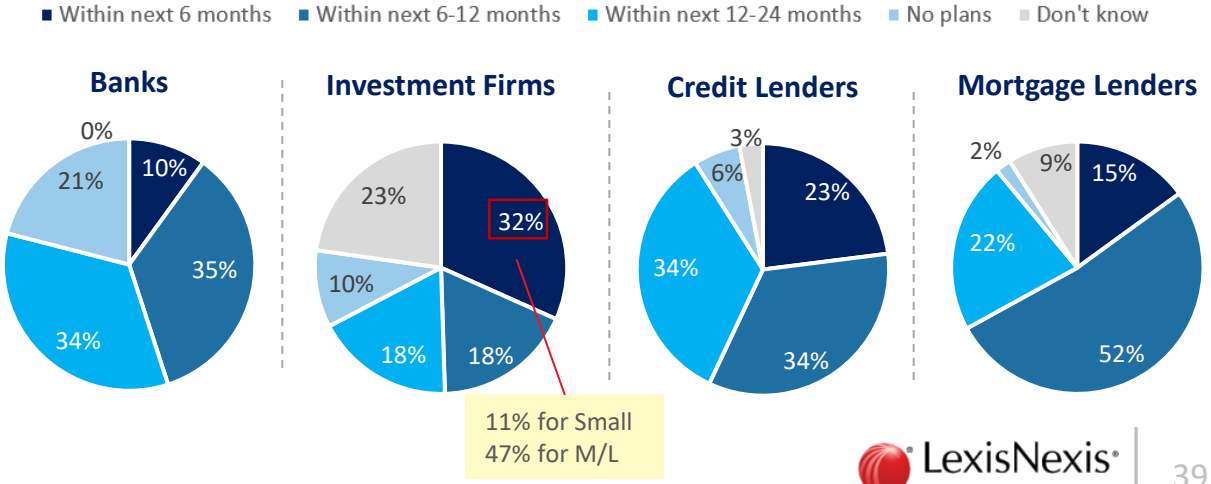
Mid/large U.S. banks and investment firms are more likely to be using the FraudClassifier℠ Model than lenders.

However, a majority of lenders familiar with but not using this model expect to do so within the next 12 months.

Degree of Familiarity with FraudClassifier℠ Model



Future Plans to Use FraudClassifier℠ Model*



Survey Questions:
Q14e: To what degree is your organization familiar with the FraudClassifier℠ Model, published by the Federal Reserve in June 2020, to classify fraud related to payments?

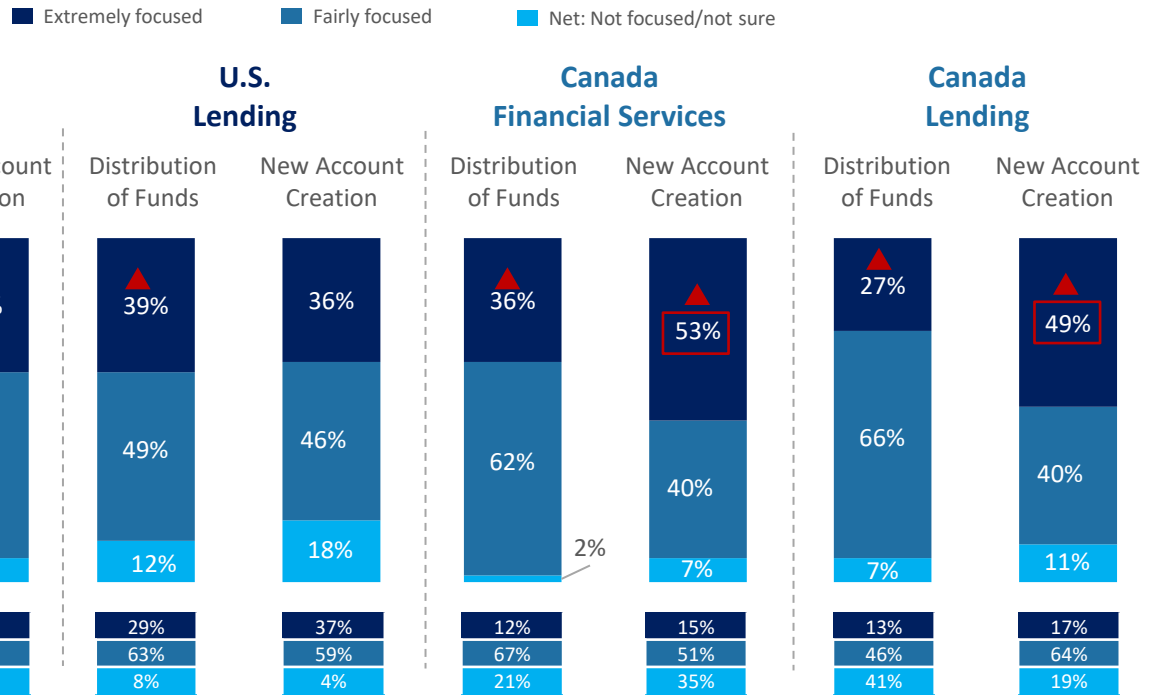
= significantly or directionally higher than same category in other industry segments

* Asked of those whose company is familiar with the FraudClassifier℠ Model but are not using it in their organization

While somewhat more U.S. financial services and lending firms have become extremely focused on optimizing risk assessment with the customer experience, Canadian firms represent a significant year-over-year increase.

Significantly more Canadian financial services and lending firms indicate being extremely focused on optimizing risk levels with the customer experience compared to 2020.

Degree of Focus on Optimizing Risk Level to Appropriate Customer Friction Level



* Asked of those with online and/or mobile channel translations; first asked in 2020

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?

= significantly or directionally higher than same category in other industry segments

= significantly or directionally higher/lower than previous period

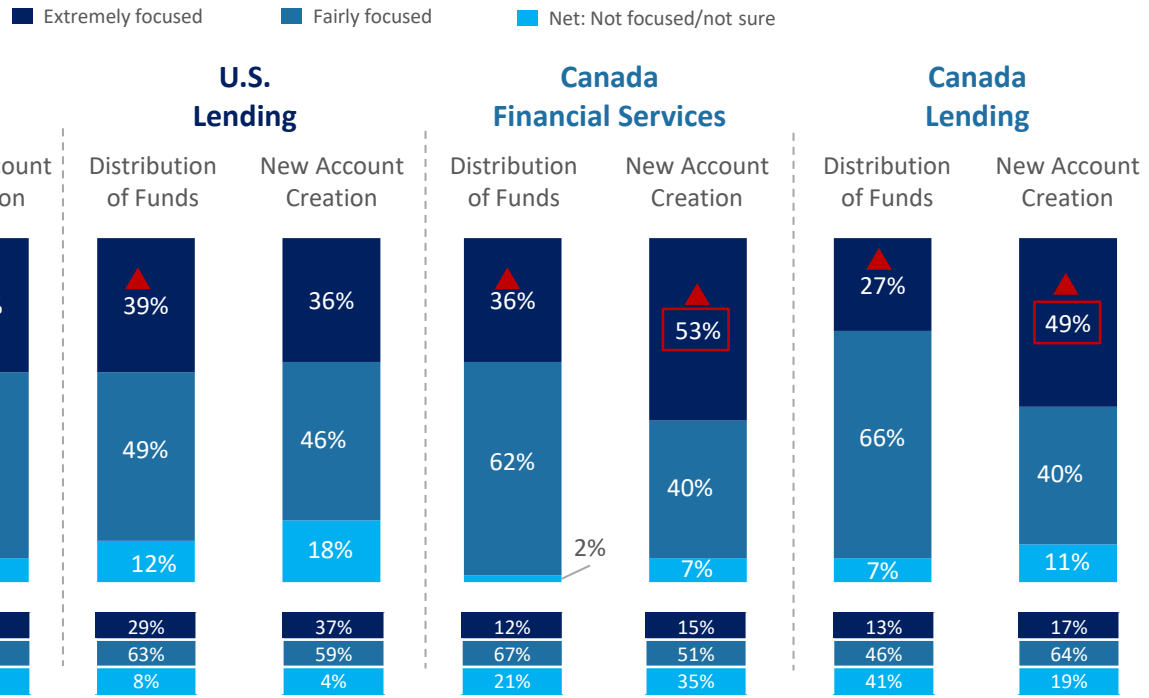
BEST PRACTICE

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.

Somewhat more U.S. and Canadian financial services and lending firms have become extremely focused on optimizing risk assessment with the customer experience, though many remain only somewhat focused.

Where this differs is with Canadian financial services and lending firms at new account creation.

Degree of Focus on Optimizing Risk Level to Appropriate Customer Friction Level



* Asked of those with online and/or mobile channel translations; first asked in 2020

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?

= significantly or directionally higher than same category in other industry segments

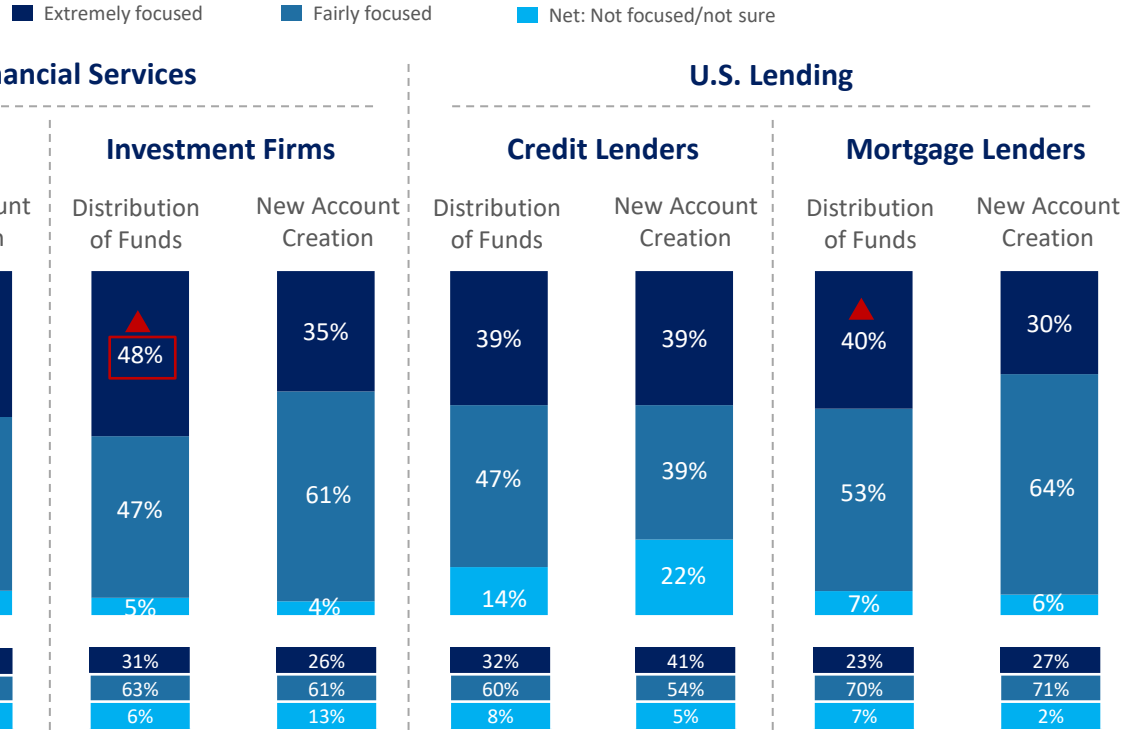
= significantly or directionally higher/lower than previous period

BEST PRACTICE

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.

The largest increase in U.S. firms being extremely focused on optimizing risk assessment-to-customer experience has come from investment firms and mortgage lenders.

Degree of Focus on Optimizing Risk Level to Appropriate Customer Friction Level



* Asked of those with online and/or mobile channel translations; first asked in 2020

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?

= significantly or directionally higher than same category in other industry segments

= significantly or directionally higher/lower than previous period

There is continued movement among financial services and lending firms toward integrating fraud prevention efforts with the digital/customer experience, though most remain at a partially integrated stage.

The increase among U.S. firms is from banks and mortgage lenders.

Firms 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.

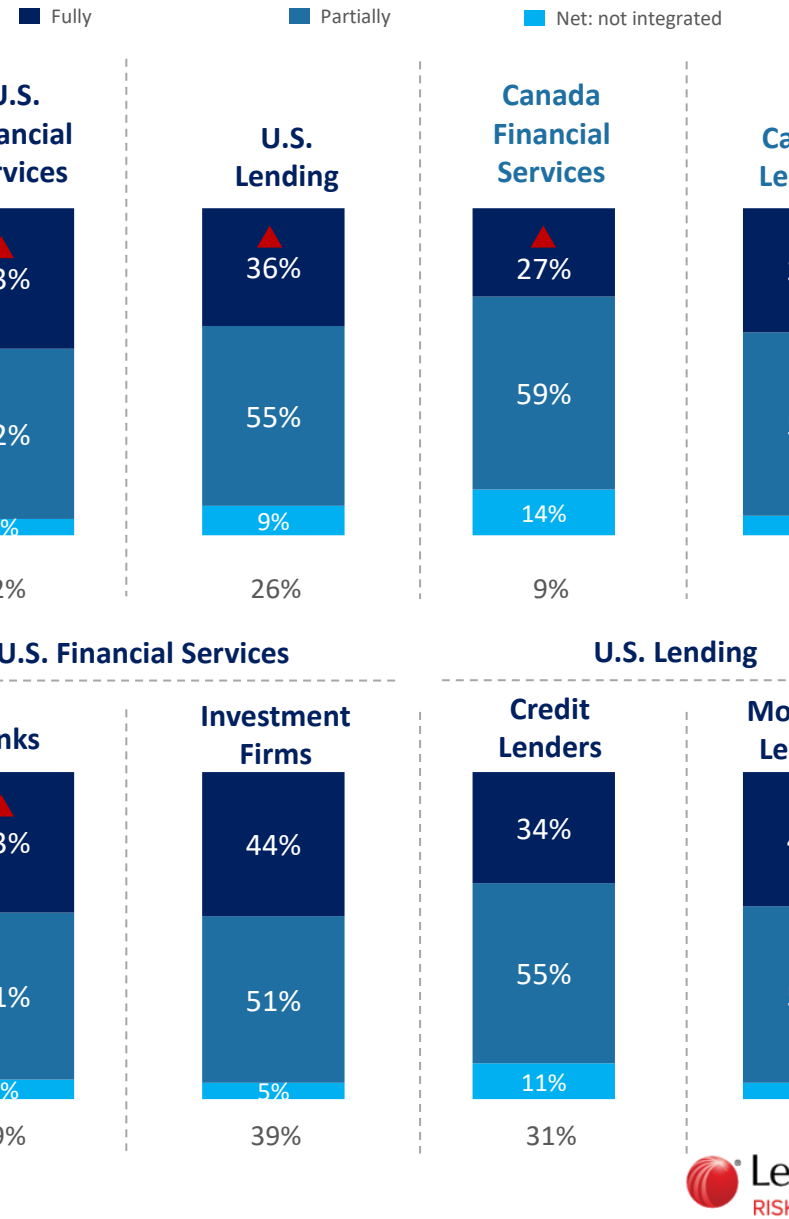
Survey Questions:
Q30b. To what degree has your company integrated its digital/customer experience operations with its fraud prevention efforts?

= significantly or directionally higher than same category in other industry segments

= significantly or directionally higher/lower than previous period

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

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



There is also some continued movement toward integrating fraud prevention efforts with cybersecurity operations, though most also remain at a partially integrated stage.

The increase among U.S. firms is from banks and mortgage lenders, which suggests that these firms may be integrating cybersecurity operations and the digital customer experience with fraud prevention at the same time.

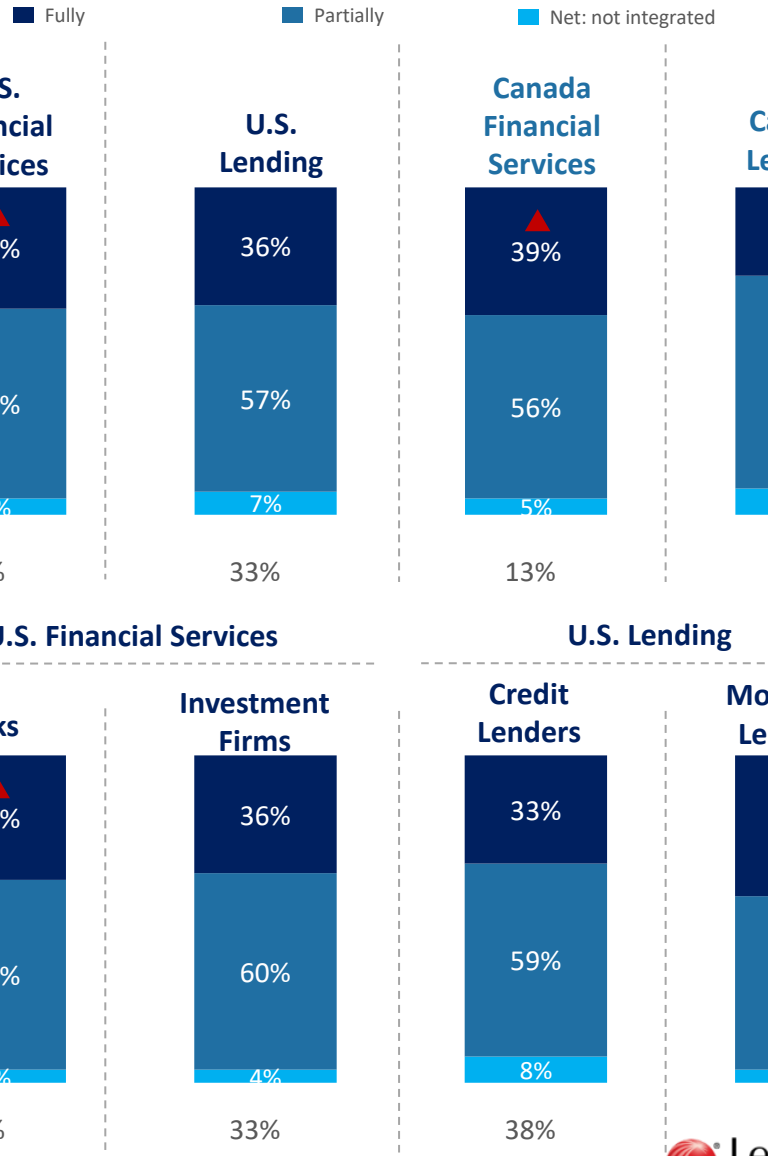
Survey Questions:
Q29. To what degree has your company integrated its cybersecurity operations with its fraud prevention efforts?

= significantly or directionally higher than same category in other industry segments

= significantly or directionally higher/lower than previous period

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

Integration of Cybersecurity Operations w/ Fraud Prevention*



More U.S. banks have embraced supportive capabilities around cybersecurity alerts, social media intelligence and AI/ML models in the battle against fraud.

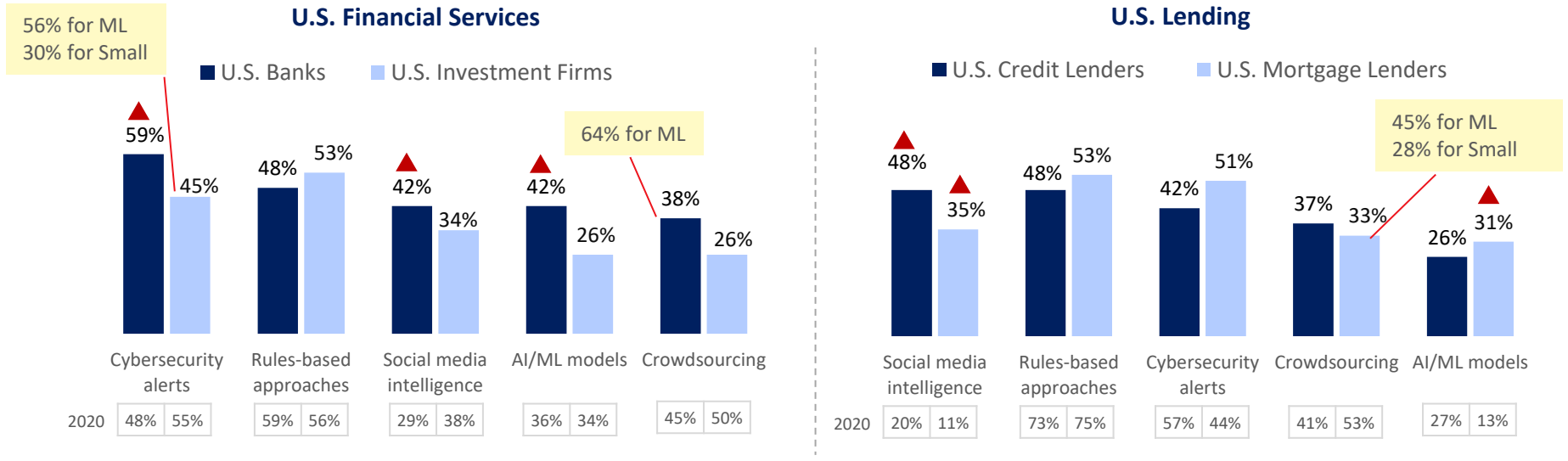
There is also an increase in the number of U.S. mortgage firms that are using social media intelligence and AI/ML models. In both cases, increased fraud volume and costs may be driving these organizations to expand their resources more so than others.

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

= significantly or directionally higher than same category in other industry segments

= significantly or directionally higher/lower than previous period

% Using Supportive Capabilities to Fight Fraud



Cybersecurity alerts are notifications that specifics attack have been directed at an organization's information systems.
Rules-based approaches use codes to drive if-then actions (if information or activity = risk, then an action is taken or alert if provided).
Social media intelligence refers to the collective tools and solutions that allow organizations to analyze conversations, respond to social signals and synthesize social data points into meaningful trends and analysis.
AI/ML models are mathematical algorithms that are "trained" using data and human expert input to replicate a decision an expert would make when provided that same information.
Crowdsourcing is the collection of information, opinions, or work from a group of people, usually sourced via the Internet.

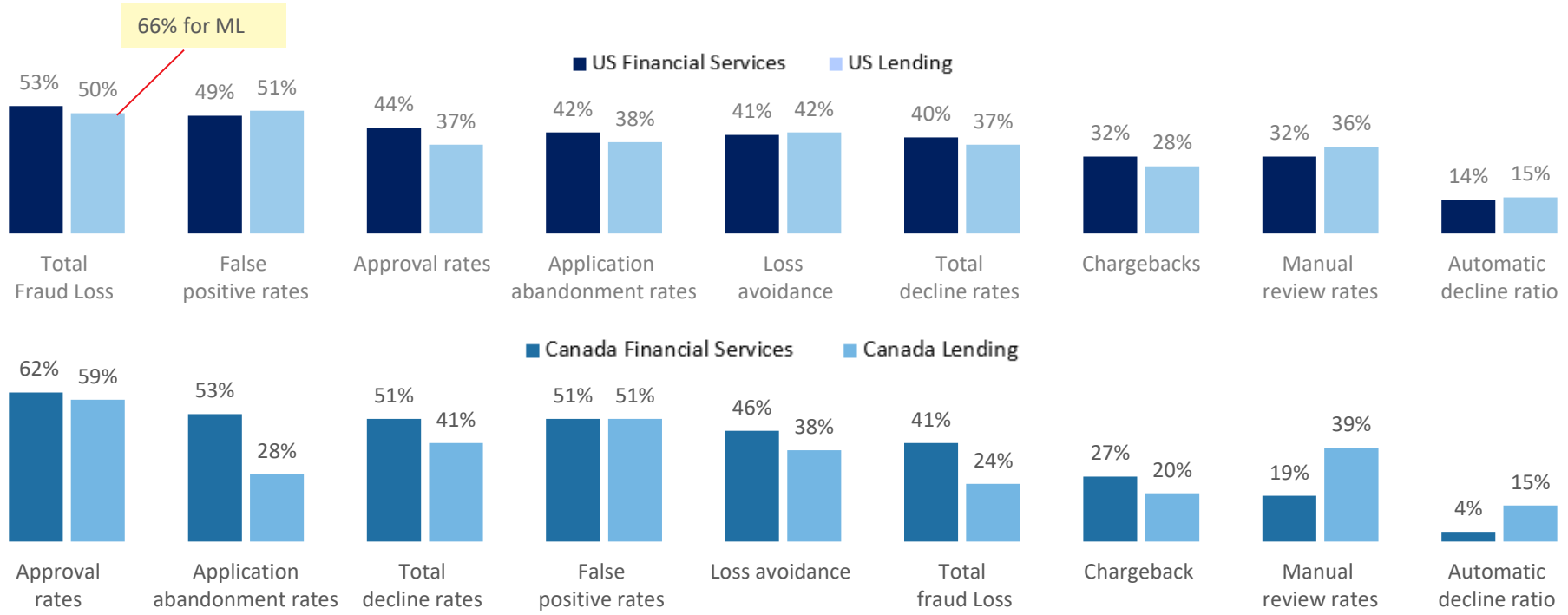
Fraud prevention performance metrics vary, with roughly half of U.S. firms using total fraud loss and false positives as key metrics.

There is a broader set of measures among Canadian financial services firms, also including approval and abandonment rates.

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

= significantly or directionally higher than other responses

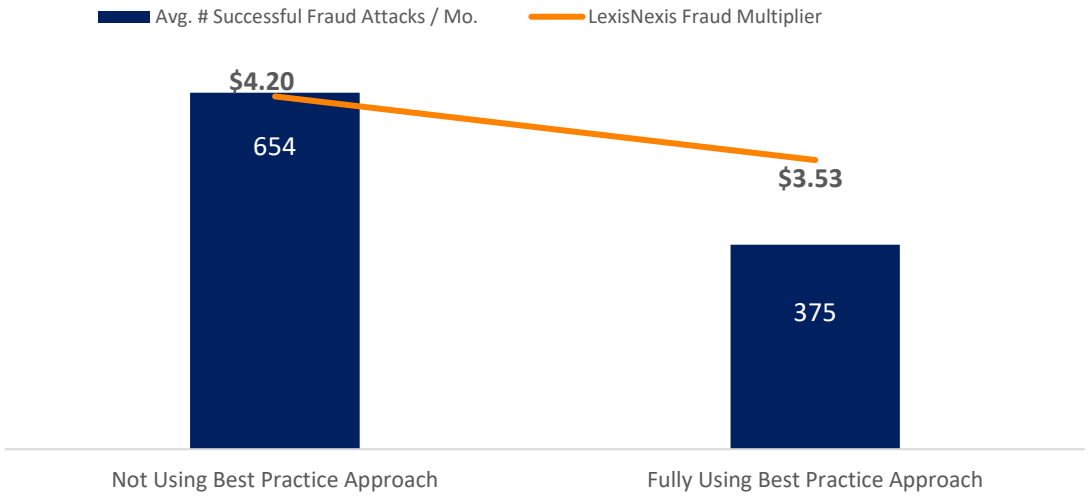
Measuring Fraud Prevention Performance



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

Using U.S. financial services and lending firms as an illustration, those which employ the best practice solutions and integration approach have a lower cost of fraud and level of successful fraud attacks.

For best practice followers, every $1 of fraud costs them less ($3.52) than those which do not follow this approach ($4.20), with nearly half the amount of successful fraud attacks per month compared to those not using this approach.



Integration of Cybersecurity, Digital Experience with Fraud Ops	No	Yes
Focus on Optimizing Fraud Risk-to-Friction Levels	No	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	✓
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.

RECOMMENDATIONS

Recommendation #1

IDENTITY PROOFING MUST INCLUDE ASSESSING DIGITAL IDENTITY ATTRIBUTES. TECHNOLOGY IS KEY TO THIS EFFORT OF DETECTING AND MITIGATING FRAUD WHILE MINIMIZING FRICTION.

- ☑ 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 it 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 frictionless experience for genuine customers.
- ☑ Deploying technologies which can recognize customers, pinpoint fraud and build the fraud knowledge base to streamline on-boarding can 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.

A MULTI-LAYERED SOLUTION APPROACH IS REQUIRED, CUSTOMIZED TO EACH PHASE OF THE CUSTOMER JOURNEY AND TRANSACTION CHANNEL.

- ☑ 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 needed. This includes a single authentication decision platform that incorporates real-time event data, third-party signals and global, cross-channel intelligence.

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 MINIMIZING FRICTION.

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

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 guards against attacks while minimizing friction.

Multi-layered Solutions Approach

Authenticate the Physical Person

Verify physical identity attributions. **Solution examples:** name/address/DOB verification

Authenticate the Digital Person

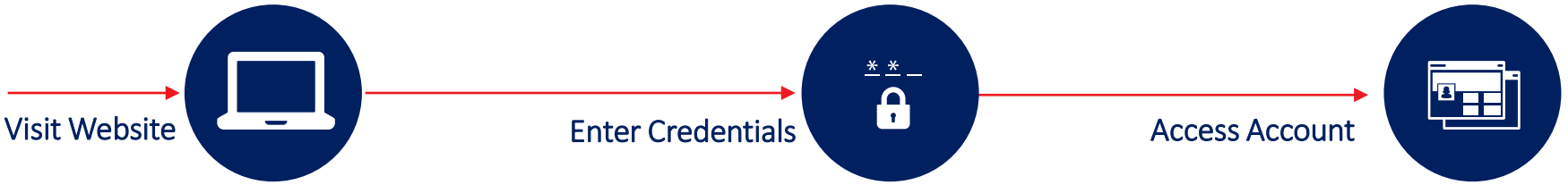
Analyze human-device interactions and behavioral patterns, such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognizing normal user and fraudster behavior. **Solution examples:** authentication by biometrics; email/phone risk assessment – seamless risk assessment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

Continue to Manage Risk Across All Endpoints

Use machine learning and an integration of systems/resources to manage risk across the business, the account and all endpoints.

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.

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 with minimal friction. 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.



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 guards against attacks while minimizing friction.

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

Multi-layered Solutions 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.

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.

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

Account Transaction/Distribution of Funds

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 Solutions Approach

Authenticate the Digital Person

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

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/insights-resources/research/us-ca-true-cost-of-fraud-study#financialservices


+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 and www.relx.com. Our solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.