LexisNexis®
RISK SOLUTIONS

6th Annual True Cost of Fraud™ Study: Financial Services and Lending Report

U.S. and Canada Edition 2022

Research Overview

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

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

The study included a 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 & Lending	Small (<$10M)	Mid/Large ($10M+)
# Completions	502	251	251	136	366

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 at least $10 million in annual revenues

Note:
S = small companies
M/L = mid/large companies

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

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

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 through online and mobile channels, and expanding internationally

Data Collection:

- Data collection occurred between May and July 2022
- Many of the survey questions reference the past 12 months

For the purposes of this study, we refer to fraud as:

- Fraudulent transactions due to identity fraud, which is the misuse of stolen payments methods (e.g., credit cards) or personal information
- Fraudulent requests for refunds/returns, bounced checks
- Fraudulent loan applications (i.e., 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.

Summary of Key Findings

1) **Trends**: Buy Now, Pay Later (BNPL) adoption, various scams, increased bots and increased fraudster targeting of the mobile channel are key trends for financial services and lending firms. The mobile channel generates a sizeable level of transaction volume and fraud costs. Banks and credit lenders are beginning to accept BNPL transactions, as digital payment methods represent one-third of overall average volume. Financial institutions are dealing with multiple scams, including those targeting digital payments.

2) **Attacks and Costs**: Fraud costs and attack volumes remain significantly higher compared to before the pandemic. Financial services firms' costs continue to rise above early 2020, with banks reporting the highest figure of $4.36 for every $1 of fraud loss. Mortgage firms also have a comparably higher cost of $4.20 for every $1 of fraud loss. While both credit and mortgage lending firms' costs remain above early 2020, they are trending down from the significant spikes they experienced at the start of the pandemic.

3) **Scams Impacting Customer Journey Risks:** Scams are contributing to increased fraud costs and particularly creating more risk at the new account creation stage of the customer journey. They are impacting fraud detection across the customer journey by heightening challenges with digital identity verification, distinguishing bots from legitimate customers and balancing fraud detection with customer friction. Those dealing with multiple types of scams have a higher cost of fraud based on more labor/investigation efforts.

4) **BNPL Impact on Fraud Detection:** Financial institutions' adoption of Buy Now, Pay Later (BNPL) is expected to grow within the next 12 – 18 months. With that comes fraud detection challenges for banks and credit lenders which can include the need for assessing the risk with more transactions, difficulty determining a transaction origination, ensuring that BNPL providers are compliant with financial regulations, lacking consistency across payment apps and dealing with false positives.

5) **Identity-related Fraud:** Identity verification is a top challenge that contributes to fraud losses across the customer journey. Identity-related fraud is occurring across the customer journey, with new account creation continuing its upward trend as a source for this type of fraud. U.S. banks that are dealing with multiple types of scams (>=3 scams) attribute more identity-related fraud to new account creation.

6) **Risk Mitigation Smart Practices:** Findings show that firms using a multi-layered solutions approach that is integrated with cybersecurity and digital customer experience operations can lower their cost and volume of successful fraud while improving identity verification and fraud detection effectiveness.

Summary of Recommendations

Overview

Key Findings

#1 Trends/Landscape

#2 Attacks & Costs

#3 Scams Impacting Customer Journey Risks

#4 BNPL Impact on Fraud Detection

#5 Identity-related Fraud

#6 Risk Mitigation Smart Practices

Recommendations

1) **Identity proofing should include assessing digital identity attributes. Technology is key to the effort of detecting and mitigating fraud while minimizing friction.**

2) **We recommend adopting a multi-layered solutions approach, which should be customized to each phase of the customer journey and transaction channel.**

3) **Financial services and lending organizations can mitigate 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.**

4) **Financial institutions should consider using technologies that recognize their customers, determine their point of access, and distinguish them from fraudsters and malicious bots. The use of layered solutions would allow firms to apply more or less fraud assessment in order to optimize this with the customer experience.**

5) **Financial services and lending organizations should consider adding transaction risk technology to the layering of the digital attributes, behavioral analytics and device assessment solutions during the transaction/ distribution of funds journey point.**

Key Finding 1

Some key trends for financial services and lending firms include Buy Now, Pay Later adoption, various scams, increased bots and increased fraud attacks targeting the mobile channel.

Mobile channel transaction volume continues to grow, matching or outpacing online channel volume. Notably, the share of mobile transactions grew by 57% for U.S. investment firms and 64% for U.S. credit lenders. That drives a sizeable portion of fraud costs as fraudsters continue to target this channel, including through bot attacks.

Banks and credit lenders are beginning to accept point-of-sale credit transactions through Buy Now, Pay Later (BNPL) apps, with about one-third doing so.

Digital payment methods represent one-third of transaction volume as consumer behavior has changed since the pandemic.

Many financial institutions are dealing with multiple scams, including phishing and those targeting digital payments. The most common scam is phishing, which is reported by 75% of U.S. lending firms and 88% of Canadian lending firms.

Key Finding 1

INCREASE IN SHARE OF MOBILE TRANSACTIONS

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Online and mobile channel transaction share is now on par with or exceeds in-person share, with U.S. credit lenders and investment firms seeing the largest growth.

The degree of in-person transactions in some segments is rebounding from early pandemic lows.

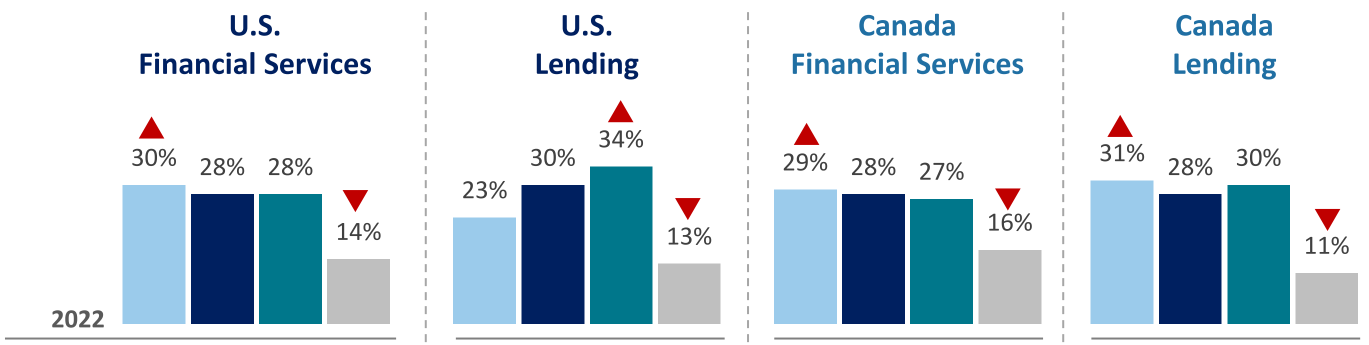
Note:
Above average mobile transaction volume = 25%+

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

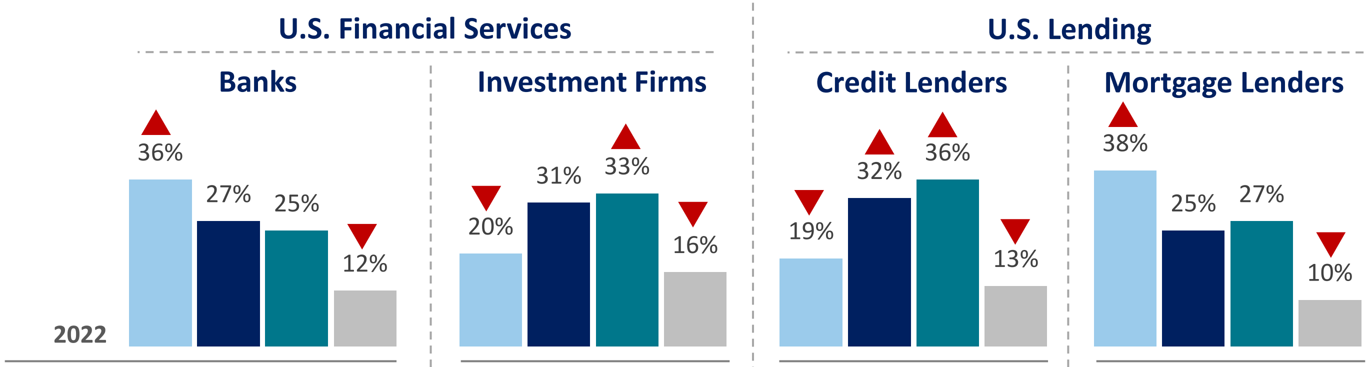
▼▲ = significantly or directionally higher/lower than previous period

% Transaction Volume by Channel

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



	U.S. Financial Services				U.S. Lending				Canada Financial Services				Canada Lending			
2021	24%	29%	25%	22%	25%	27%	24%	24%	21%	31%	24%	24%	25%	26%	26%	23%
2020	27%	21%	17%	35%	29%	21%	18%	32%	32%	17%	18%	33%	26%	18%	18%	38%
2019	35%	20%	14%	31%	27%	28%	13%	32%								



	Banks				Investment Firms				Credit Lenders				Mortgage Lenders			
2021	22%	31%	27%	20%	26%	26%	21%	27%	26%	25%	22%	27%	21%	30%	29%	20%
2020	30%	19%	16%	35%	22%	24%	21%	33%	30%	21%	19%	30%	26%	23%	16%	35%
2019	40%	18%	12%	30%	30%	22%	16%	32%	27%	28%	13%	31%	26%	27%	12%	35%

Key Finding 1

FRAUD TARGETING MOBILE CHANNEL TRANSACTIONS

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Fraud continues to target mobile channel transactions, with larger increases among U.S. financial services and lending firms that have higher transaction volume through this channel.

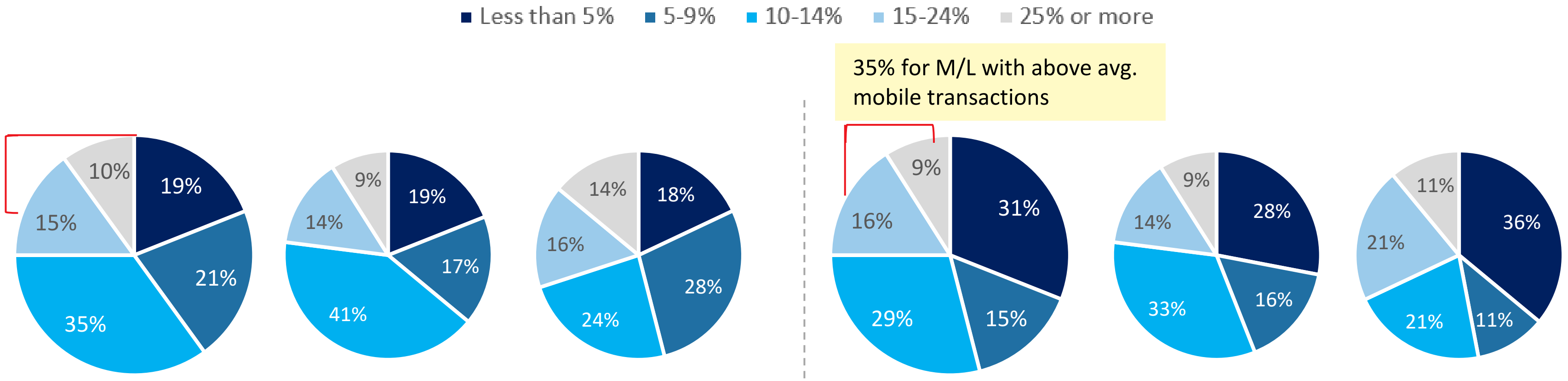
Fraud Targeting Mobile Channel Transactions

U.S. Financial Services vs. Lending

% Saying Fraud Targeting Mobile Has Increased	Financial Services (Overall)	Banks	Investment Firms	Lending (Overall)	Credit Lenders	Mortgage Lenders
2022	95%	96%	93%	96%	99%	88% ▼
2021	98%	92%	98%	96%	96%	98%

% Increase

32% for M/L with above avg. mobile transactions



35% for M/L with above avg. mobile transactions

Survey Question:
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

Canadian financial services and lending firms also report increased targeting of the mobile channel by fraudsters.

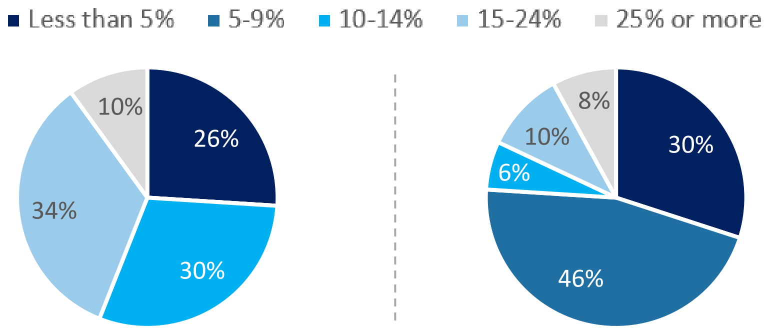
However, in terms of the magnitude of increase, financial services firms are more likely than lending firms to report more significant increases in mobile channel fraud.

Fraud Targeting Mobile Channel Transactions

Canada Financial Services vs. Lending

	Financial Services (Overall)	Lending (Overall)
% Saying Fraud Targeting Mobile Has Increased		
2022	84% ▼	94%
2021	95%	89%

% Increase



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

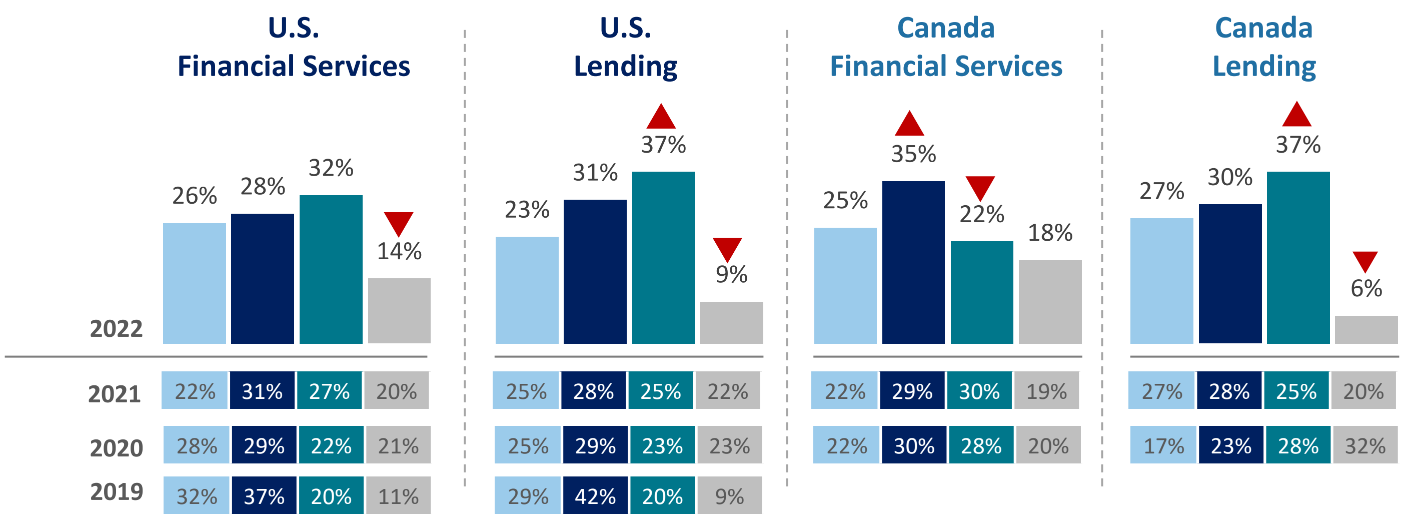
▼▲ = significantly or directionally higher/lower than previous period

In line with expectations, the mobile channel continues to increase as a driver of fraud costs, particularly for U.S. and Canadian lending firms.

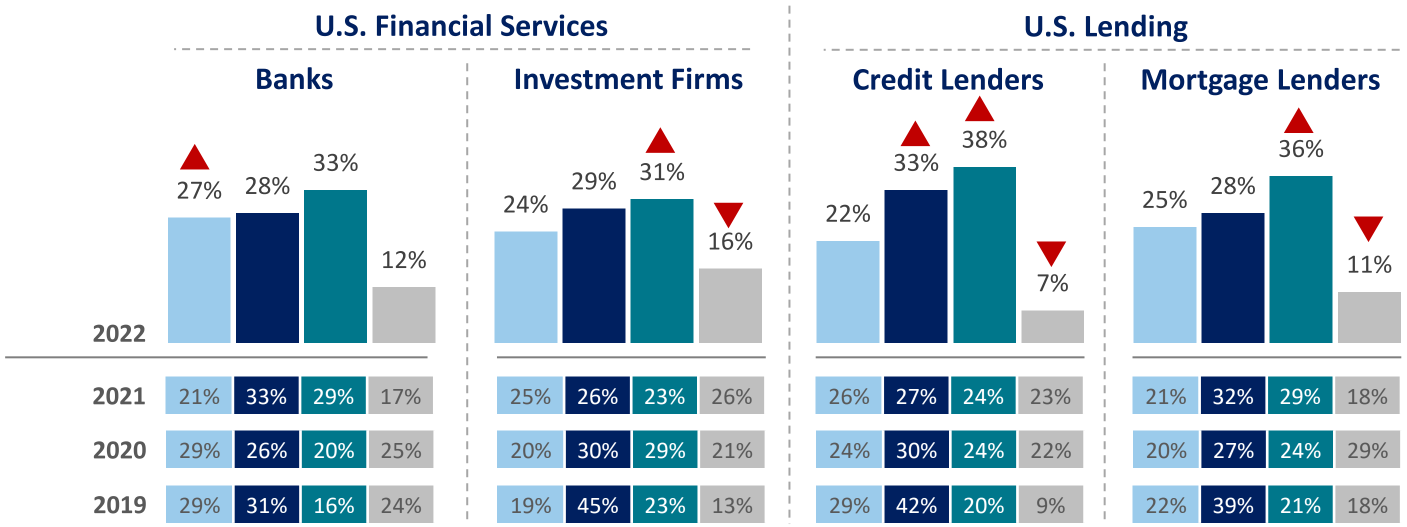
U.S. financial services and lending firms with more mobile transaction volume attribute a higher percentage of fraud costs to that channel compared to firms with less mobile transaction volume.

% Fraud Costs by Channel

🟦 In-Person
🟩 Mobile
■ Online
▨ Other (Phone, Mail, Kiosk)



	U.S. Financial Services				U.S. Lending				Canada Financial Services				Canada Lending			
2022	26%	28%	32%	▼14%	23%	31%	▲37%	▼9%	25%	▲35%	▼22%	18%	27%	30%	▲37%	▼6%
2021	22%	31%	27%	20%	25%	28%	25%	22%	22%	29%	30%	19%	27%	28%	25%	20%
2020	28%	29%	22%	21%	25%	29%	23%	23%	22%	30%	28%	20%	17%	23%	28%	32%
2019	32%	37%	20%	11%	29%	42%	20%	9%								



	Banks				Investment Firms				Credit Lenders				Mortgage Lenders			
2022	▲27%	28%	33%	12%	24%	29%	▲31%	▼16%	22%	▲33%	▲38%	▼7%	25%	28%	▲36%	▼11%
2021	21%	33%	29%	17%	25%	26%	23%	26%	26%	27%	24%	23%	21%	32%	29%	18%
2020	29%	26%	20%	25%	20%	30%	29%	21%	24%	30%	24%	22%	20%	27%	24%	29%
2019	29%	31%	16%	24%	19%	45%	23%	13%	29%	42%	20%	9%	22%	39%	21%	18%

Survey Question:
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

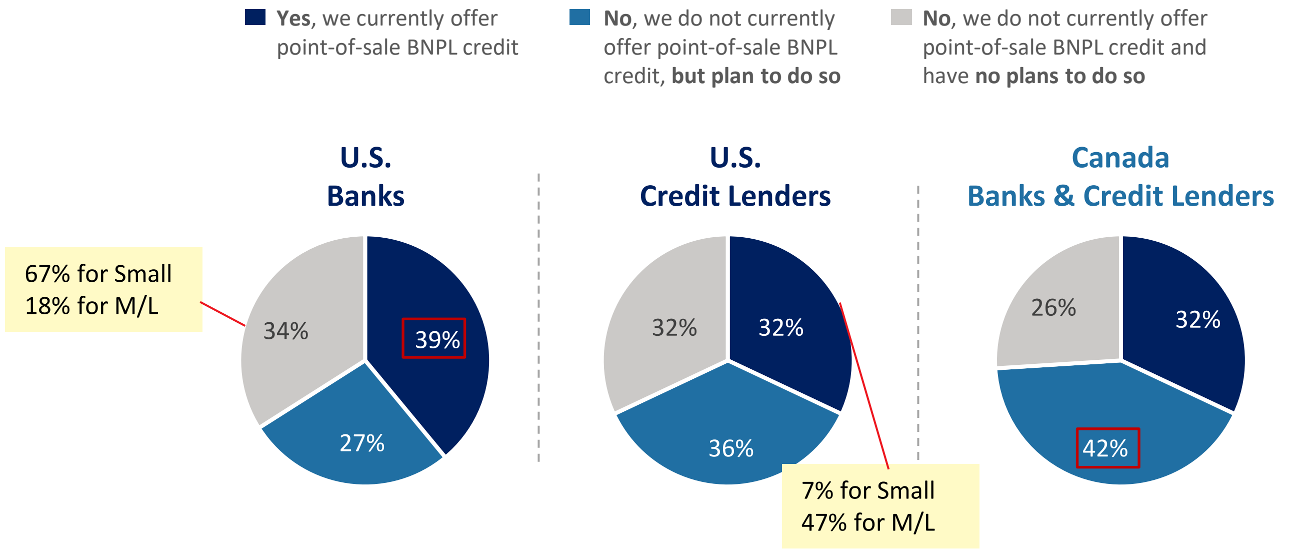
Key Finding 1

POINT-OF-SALE ACCESS TO BUY NOW, PAY LATER CREDIT

The acceptance of Buy Now, Pay Later (BNPL) credit is becoming more prevalent among many North American banks and credit lenders, either currently or in the near-term. Larger U.S. credit lenders are leading the way.

Specifically, Mastercard is a driving force with the launch of its BNPL product (Mastercard Installments), which includes building out a large partner network of leading retailers and banks.[1]

Point-of-Sale Access to Buy Now, Pay Later Credit



67% for Small
18% for M/L

7% for Small
47% for M/L

Survey Question:
Q3n1: Does your financial institution provide point-of-sale access to Buy Now, Pay Later credit?

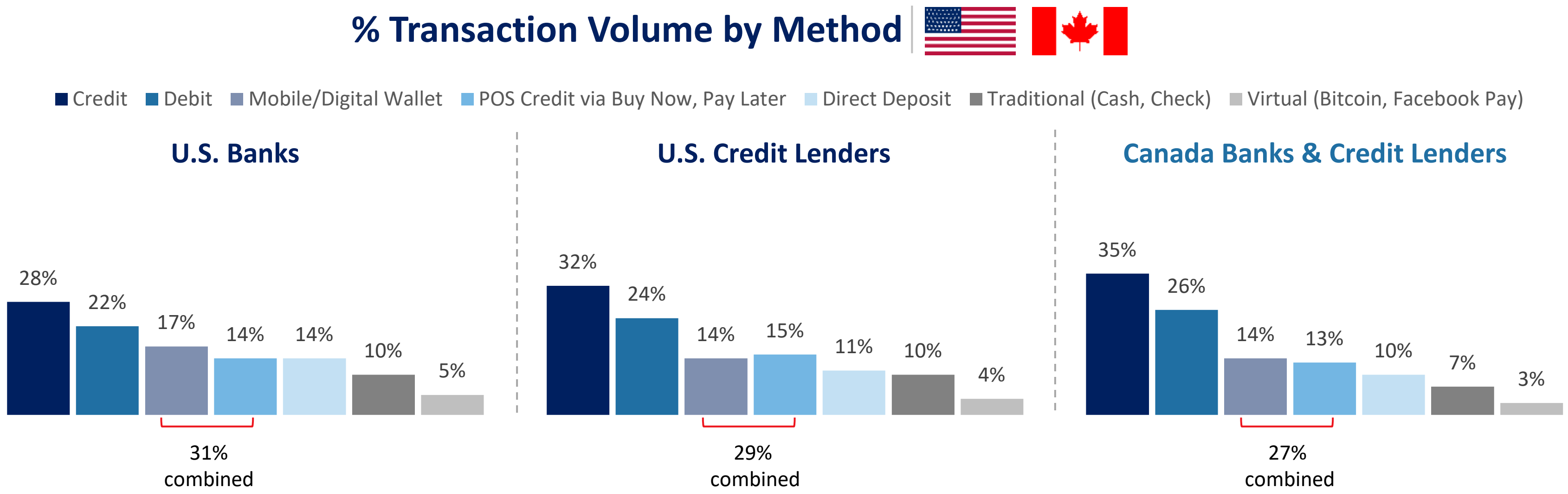
□ = significantly or directionally higher than same response in other segment

[1] https://www.americanbanker.com/news/how-mastercard-is-linking-banks-to-bnpl

Digital payment methods, including mobile wallets and point-of-sale credit via Buy Now, Pay Later (BNPL), represent nearly one-third of transaction volume through financial services and lending firms.

Credit and debit transactions combined continue to represent the majority of transaction volume, though mobile/digital wallets and debit cards have similar volumes among U.S. banks.

% Transaction Volume by Method

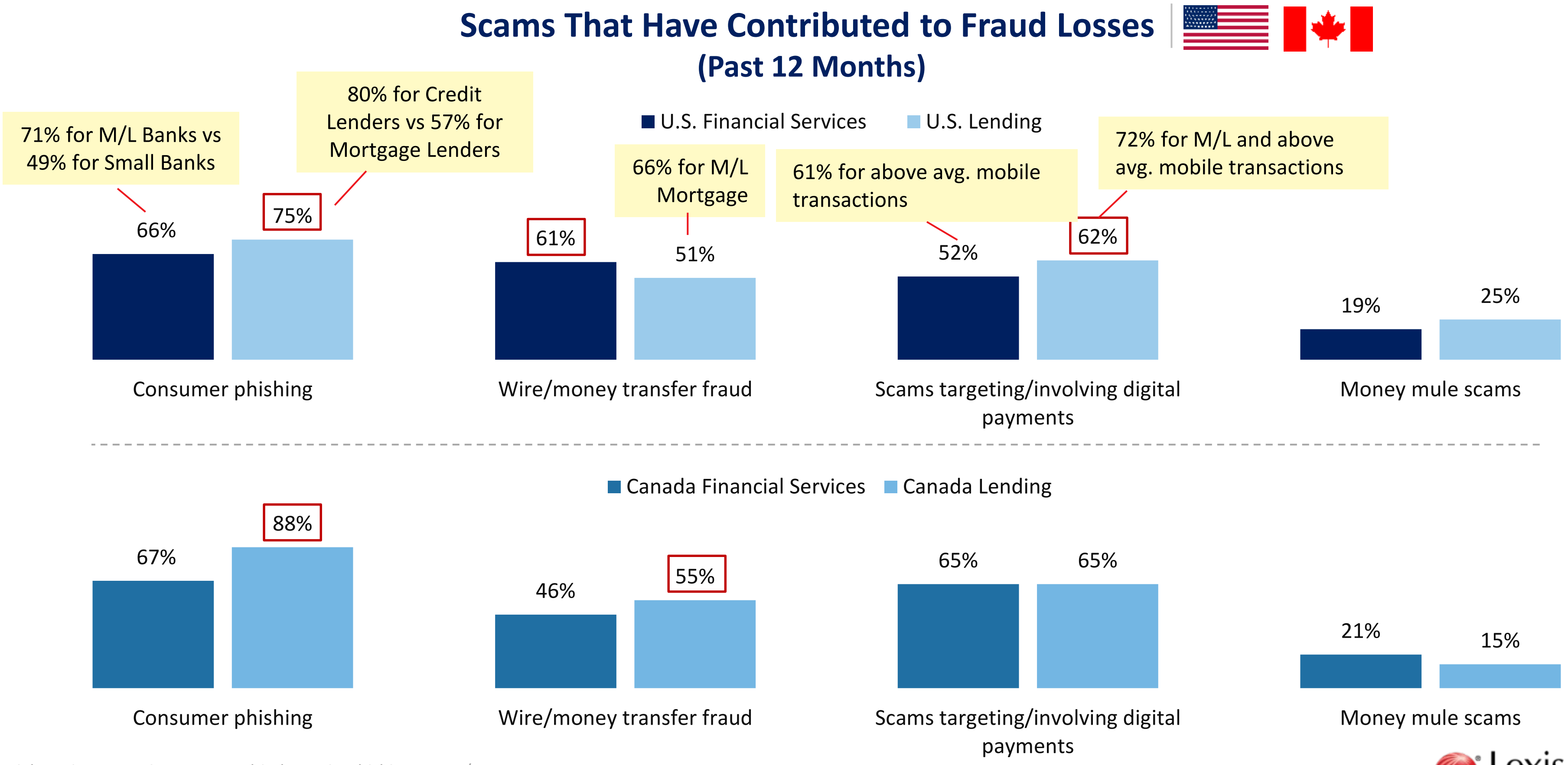


Survey Question:
Q2: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following channels used by your company.

Phishing and scams targeting digital payments are contributing to fraud losses among many U.S. and Canadian financial institutions.

Recent American Bankers Association research found that financial services is a prime target for phishing, accounting for 35% of all tracked phishing attempts.[2] The ABA also recently reported that scammers can purchase phishing software aimed at banks for $50 which involves code, graphics and configuration files to imitate login pages.[3] Wire transfer fraud is a common mortgage-related scam where fraudsters impersonate escrow officers, real estate agents or the lender to get the homeowner to wire funds into an illegitimate account for financial gain during the closing process.

Scams That Have Contributed to Fraud Losses (Past 12 Months)



	U.S. Financial Services	U.S. Lending	Canada Financial Services	Canada Lending
Consumer phishing	66%	75%	67%	88%
Wire/money transfer fraud	61%	51%	46%	55%
Scams targeting/involving digital payments	52%	62%	65%	65%
Money mule scams	19%	25%	21%	15%

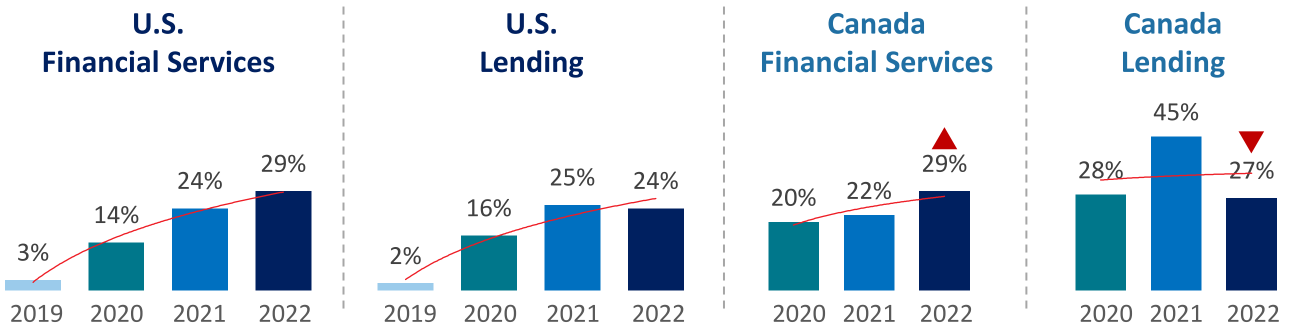
Survey Question:
Q12e: Which types of the following scams have contributed to your fraud losses during the past 12 months?

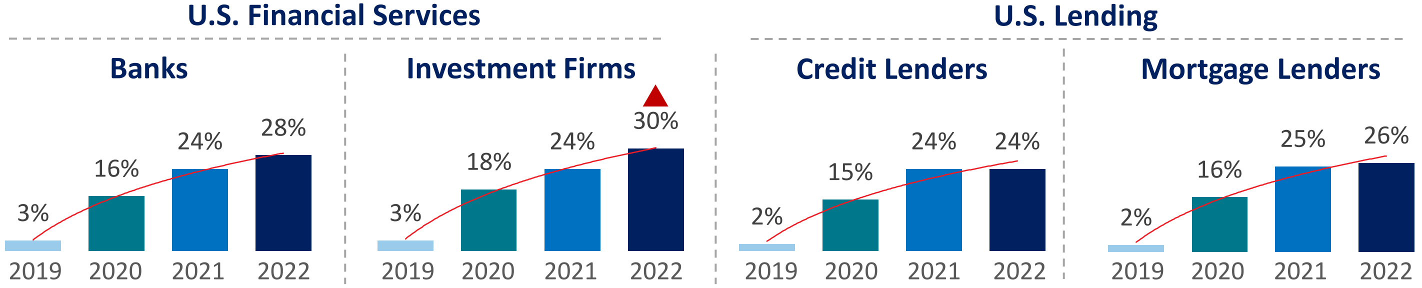
□ = significantly or directionally higher than same category in other industry segments

[2] https://bankingjournal.aba.com/2022/07/report-financial-services-most-impersonated-industry-in-phishing-scams/
[3] https://www.americanbanker.com/news/phishing-group-targeting-large-banks-offers-its-services-for-50-a-month

Malicious botnet attacks continue to increase for U.S. and Canadian financial services firms, particularly for larger banks and investment firms. The degree of increase has leveled off compared to early pandemic periods but remains significantly higher than before the pandemic.

Average % of Transactions Determined as Malicious Bot Attacks





SEGMENT HIGHLIGHTS

U.S. Financial Services

- Bot Attacks: S = 18%; M/L = 35%

SEGMENT HIGHLIGHTS

U.S. Banks

- Bot Attacks: S = 15%; M/L = 35%

U.S. Investment Firms

- Bot Attacks: S = 23%; M/L = 35%

Survey Question:
B1: In a typical month, what percent of your transactions are determined to be malicious automated bot attacks?

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

Key Finding 2

Fraud costs and attack volumes remain significantly higher compared to before the pandemic.

U.S. and Canadian financial services firms' fraud costs continue to rise and are up 19.6% - 22.4% since early 2020. The cost of fraud is highest among U.S. banks, where every $1 of fraud loss actually costs $4.36.

Mortgage firms also have a high cost of fraud compared to other segments, with every $1 of fraud loss costing $4.20. Fraud attack volume continues to rise for these firms, particularly with application fraud through direct-to-consumer transactions.

However, while mortgage and credit lending firms experienced the highest spike in fraud cost at the beginning of the pandemic and continue to report costs at levels above early 2020, these figures are trending down from those highs to be more in line with other segments.

Key Finding 2

INCREASED FRAUD COSTS

Overview

Key Findings

#1 Trends/Landscape

#2 Attacks & Costs

#3 Scams Impacting Customer Journey Risks

#4 BNPL Impact on Fraud Detection

#5 Identity-related Fraud

#6 Risk Mitigation Smart Practices

Recommendations

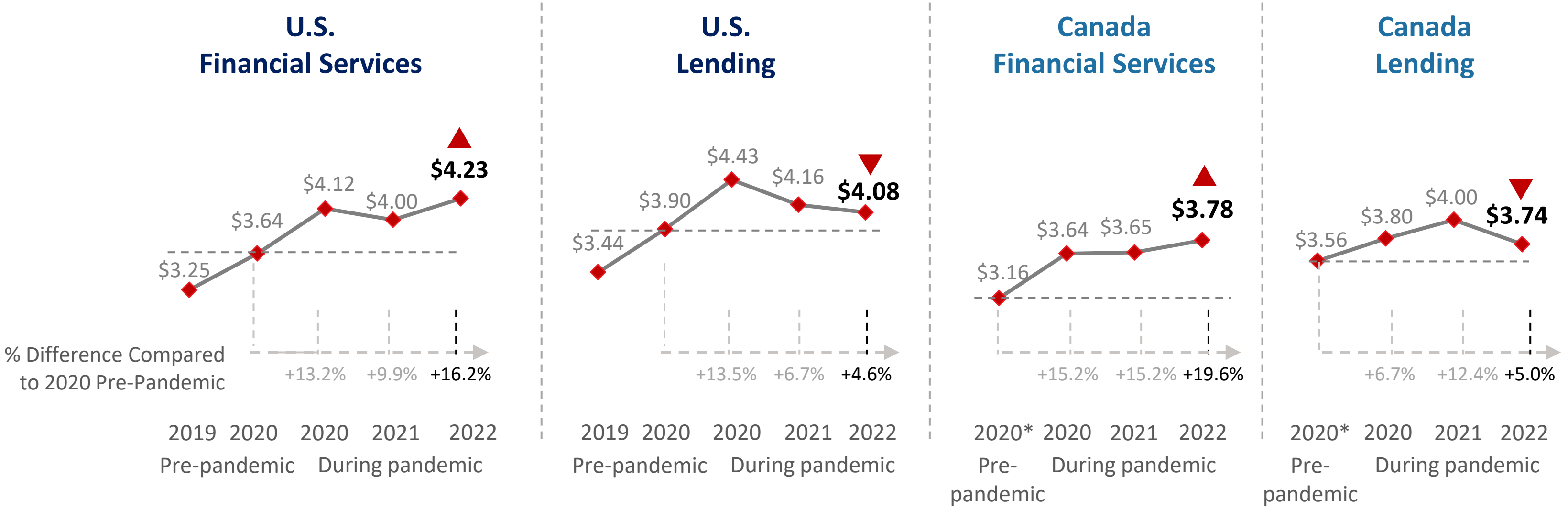
The cost of fraud continues to increase and be significantly higher than before the pandemic.

For every $1 of fraud loss, it costs U.S. financial services firms $4.23 compared to $3.64 in 2020 (pre-pandemic). For Canadian financial services firms, every $1 of fraud loss costs $3.78 compared to $3.16 in 2020 (pre-pandemic). These firms continue to see double-digit percentage increases over the pre-pandemic period.

U.S. and Canadian lending firm fraud costs are trending down towards their pre-pandemic levels.

Fraud costs involve losses related to the transaction face value for which firms are liable, plus fees/interest incurred during applications/underwriting/processing stages, fines/legal fees, labor/investigation and external recovery expenses.

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-pandemic

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

Overview

Key Findings

#1 Trends/Landscape

#2 Attacks & Costs

#3 Scams Impacting Customer Journey Risks

#4 BNPL Impact on Fraud Detection

#5 Identity-related Fraud

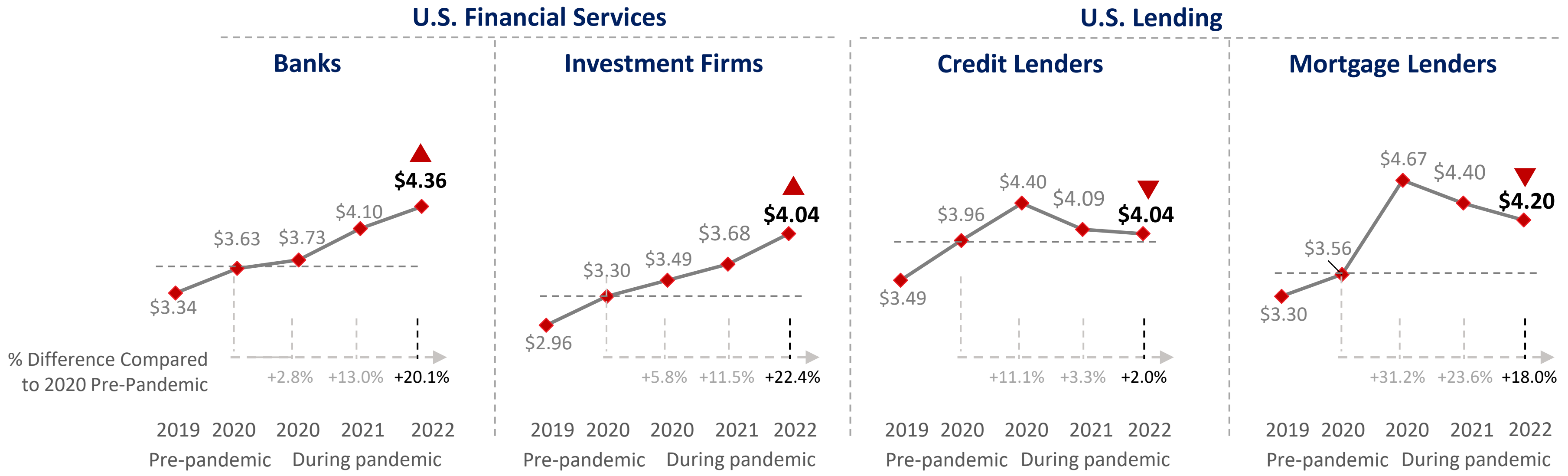
#6 Risk Mitigation Smart Practices

Recommendations

Banks and investment firms are both contributing to the continued upward trend in U.S. financial services fraud costs.

U.S. credit lending fraud costs are trending towards their 2020 pre-pandemic levels after significant spikes at the start of the pandemic. A similar trend is occurring with U.S. mortgage firms, though at a level which is still significantly higher than early 2020 and is second only to U.S. banks.

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-pandemic

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

Key Finding 2

INCREASED FRAUD ATTACKS

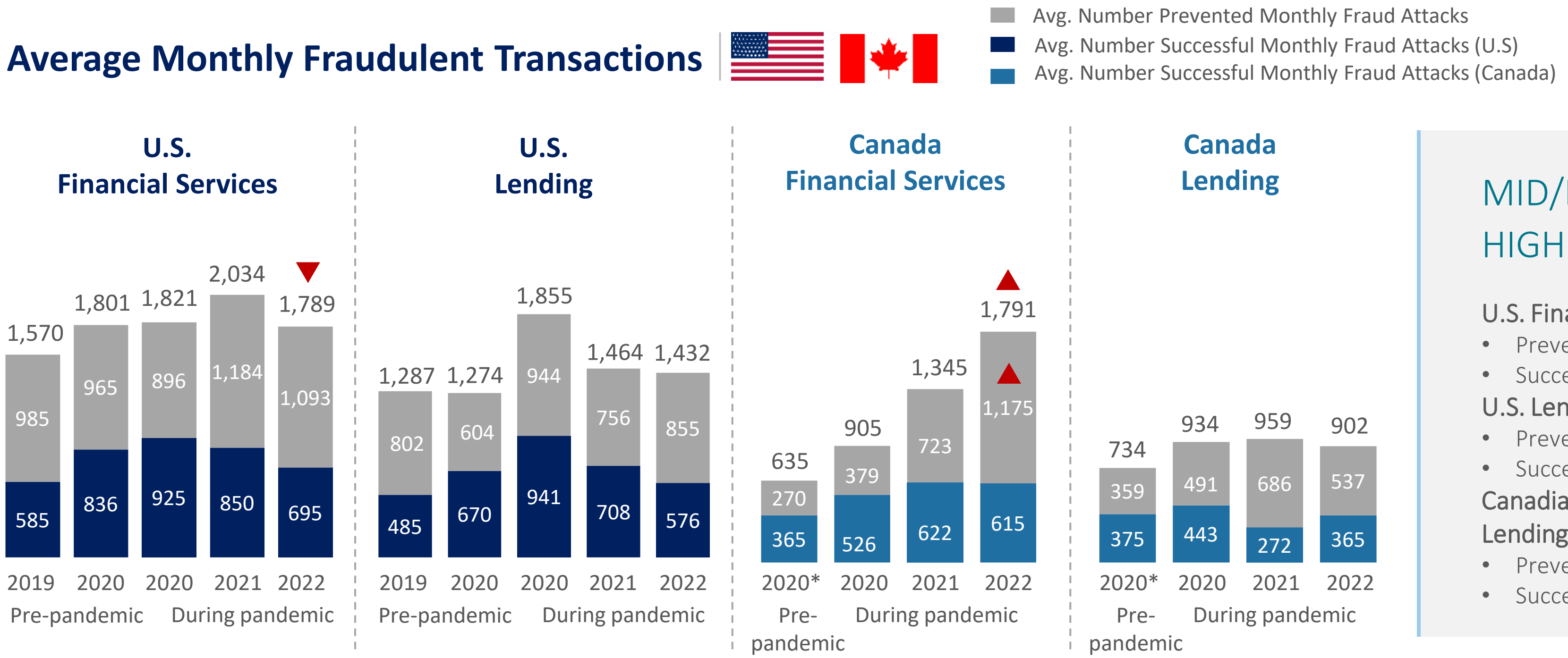
Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

The average number of successful fraudulent transactions per month remains above 2019 pre-pandemic levels for financial services and lending firms.

This is driven by larger firms.

Canadian financial services firms have experienced a significant increase in average monthly attack volume, which coincides with a spike in reported botnet attacks over the past 12 months.

Average Monthly Fraudulent Transactions



MID/LARGE SEGMENT HIGHLIGHTS

U.S. Financial Services
- Prevented Attacks: 1,144
- Successful Attacks: 756

U.S. Lending
- Prevented Attacks: 1022
- Successful Attacks: 712

Canadian Financial Services & Lending
- Prevented Attacks: 1,129
- Successful Attacks: 873

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-pandemic

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

Successful fraudulent transactions continue to rise particularly for U.S. mortgage firms.

This reflects increased application fraud across channels, including online and mobile involving direct-to-consumer transactions.[4]

Across segments, mid/large firms experience a higher volume of fraudulent transactions per month.

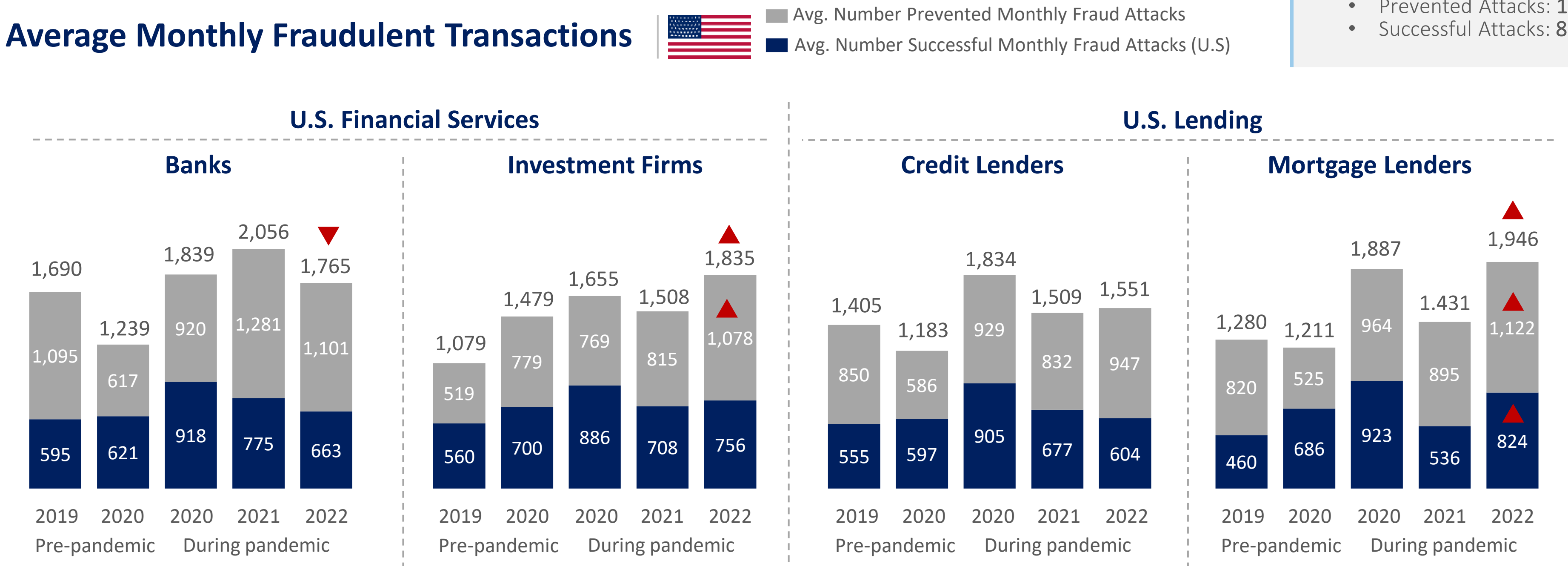
MID/LARGE SEGMENT HIGHLIGHTS

U.S. Banks (Overall 1,875)
- Prevented Attacks: 1,161
- Successful Attacks: 714

U.S. Investment (Overall 1,952)
- Prevented Attacks: 1,109
- Successful Attacks: 843

U.S. Credit (Overall 1,841)
- Prevented Attacks: 1,106
- Successful Attacks: 735

U.S. Mortgage (Overall 2,056)
- Prevented Attacks: 1,174
- Successful Attacks: 882



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-pandemic

[4] LexisNexis Risk Solutions True Cost of Fraud™ Study for Real Estate

Key Finding 2

DOMESTIC/INTERNATIONAL FRAUD COSTS

Overview

Key Findings

#1 Trends/Landscape

#2 Attacks & Costs

#3 Scams Impacting Customer Journey Risks

#4 BNPL Impact on Fraud Detection

#5 Identity-related Fraud

#6 Risk Mitigation Smart Practices

Recommendations

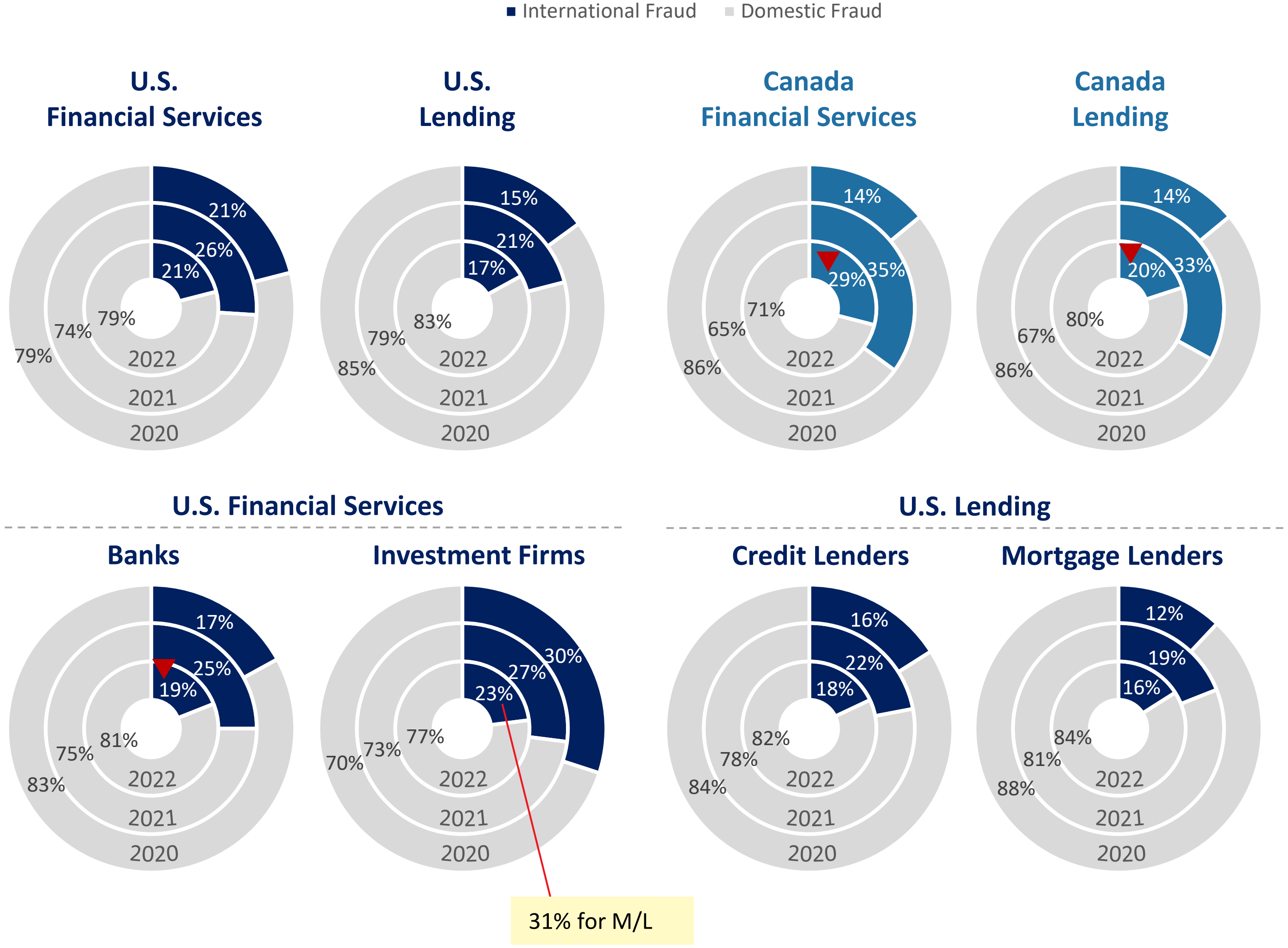
Financial services and lending firms are now experiencing a relatively smaller share of international fraud. However, the percent of international fraud still meets or exceeds pre-pandemic levels.

Compared to other segments, larger U.S. investment firms are seeing a larger share of fraud from international transactions.

Survey Question:
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



Key Finding 3

Scams are contributing to increased fraud costs and particularly creating more risk at the new account creation stage of the customer journey.

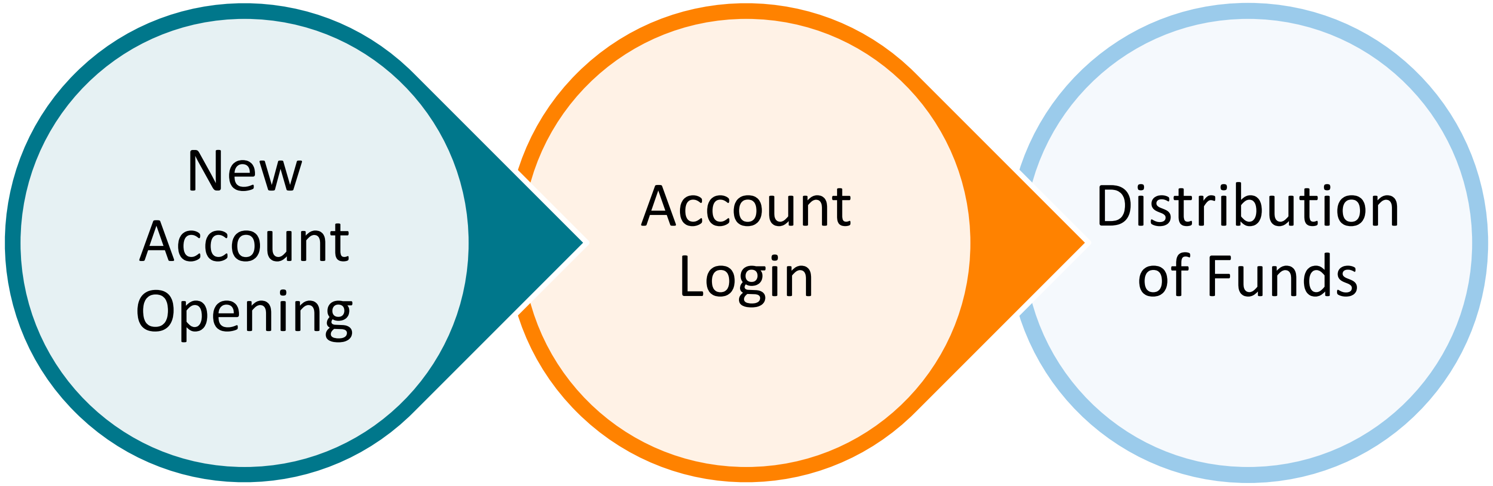
Criminals are using stolen or fake identities to open new accounts, particularly with banks and credit lenders. The new account creation stage is considered to be the most susceptible to fraud by more than 50% of U.S. banks and credit lenders as well as more than 40% of U.S. investment firms and mortgage lenders.

Scams are impacting fraud detection across the customer journey by heightening challenges with verifying digital identity, distinguishing bots from legitimate customers and balancing fraud detection efforts with customer friction.

Firms facing multiple types of scams have a significantly higher cost of fraud than others, involving more time dedicated to labor and investigation efforts.

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

In the True Cost of Fraud™ Report, we define the customer journey as follows:



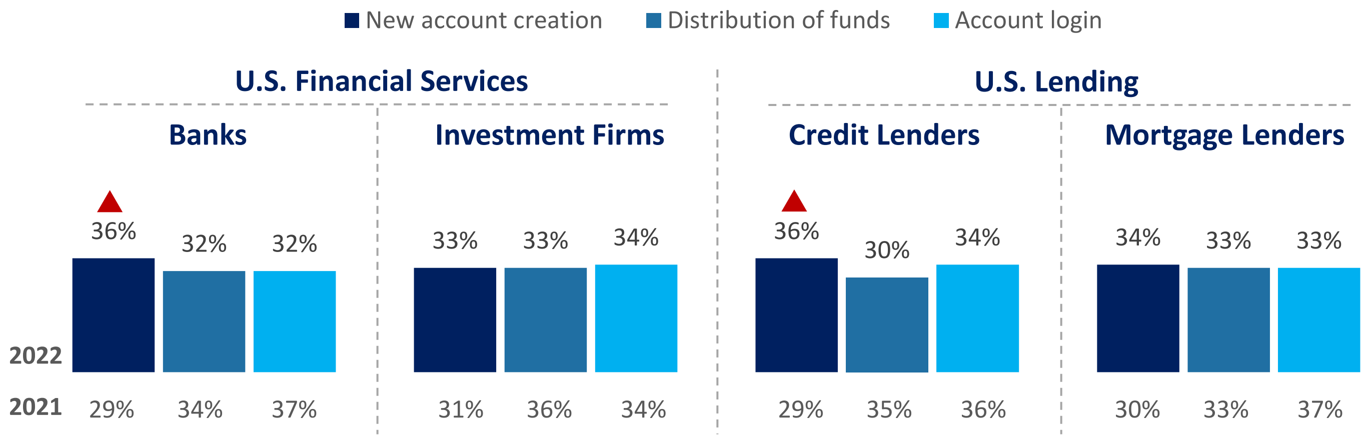
New Account Opening	Account Login	Distribution of Funds
On-boarding a new customer Establishing a new account	Accessing an account	Disbursing funds from a bank or investment account Disbursing funds for a loan
Verifying new identity, credentials	Verifying identity before allowing access to the account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

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

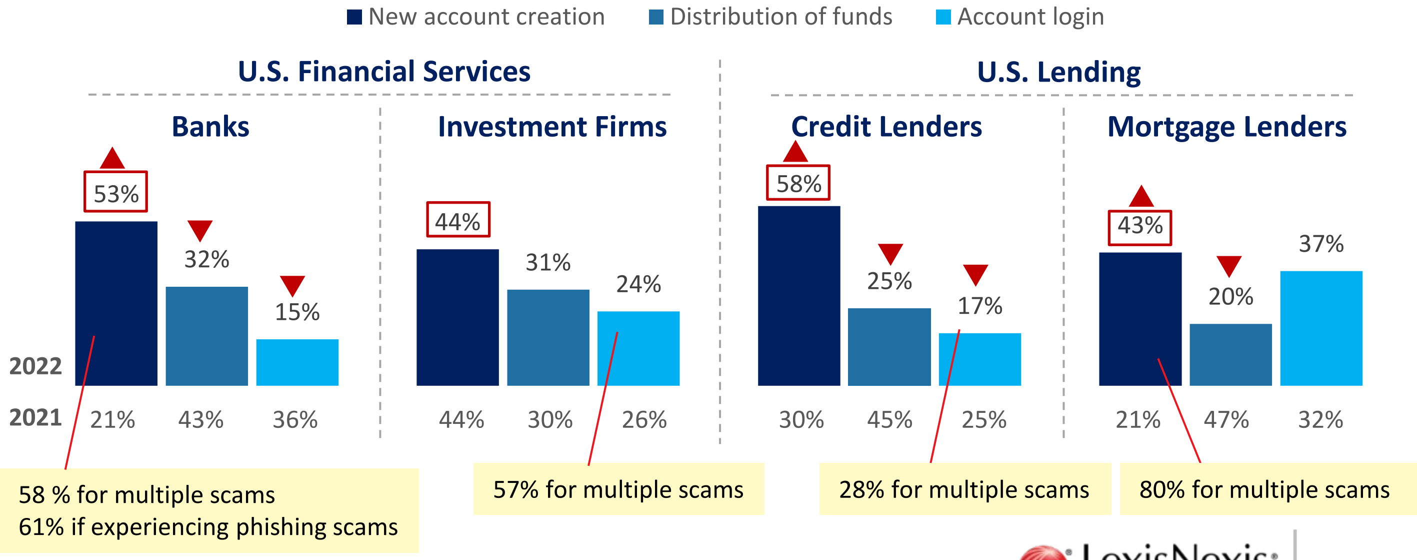
New account creation is becoming a significant fraud vector among U.S. financial services and lending firms, particularly those dealing with multiple types of scams.

With online and mobile banking becoming more pervasive, criminals can use fake or stolen IDs to open new bank accounts or to obtain a loan.[6]

% Distribution of Fraud Losses by Customer Journey Stages



Customer Journey Stage MOST Susceptible to Fraud



58 % for multiple scams
61% if experiencing phishing scams

57% for multiple scams

28% for multiple scams

80% for multiple scams

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/lower than previous period

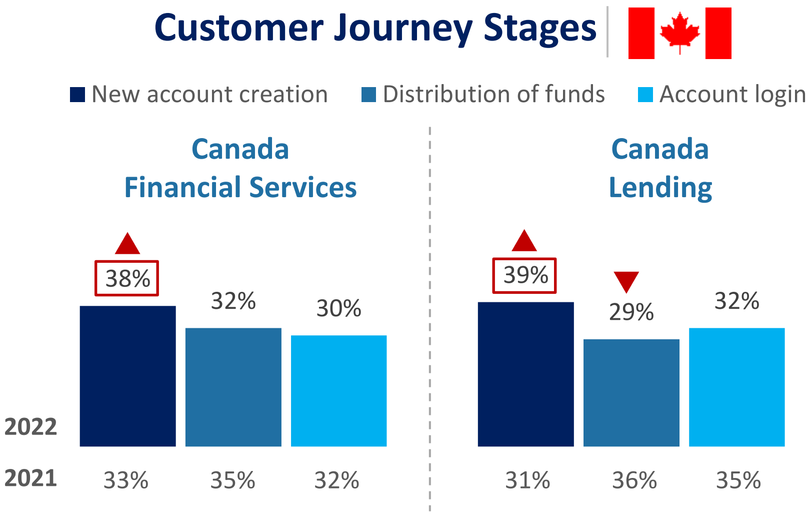
□ = significantly or directionally higher than same response in other segment within the same industry

[6] https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/04/07/thieves-hit-on-a-new-scam-synthetic-identity-fraud

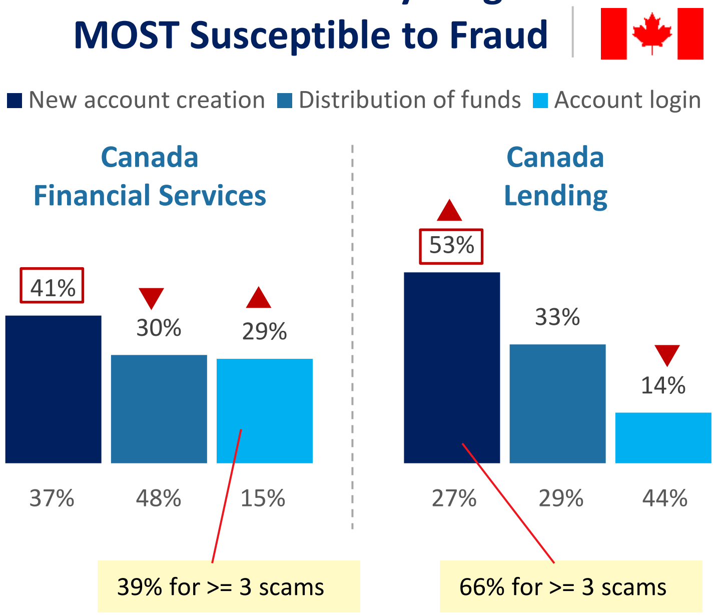
New account creation has also become a significantly larger threat for Canadian lending firms, while account login has become more of a fraud risk for Canadian financial services firms.

Even more firms indicate these as high risk among those dealing with more types of scams.

% 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

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

Key Finding 3

TOP ONLINE/MOBILE CHANNEL CHALLENGES ACROSS THE CUSTOMER JOURNEY

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Digital identity verification has become more challenging for U.S. financial institutions across the customer journey.

Challenges such as new transaction methods, determining origination source and country risk, identifying bots and balancing fraud detection with friction have all increased with account login and distribution of funds.

Top Online/Mobile Challenges: Notable Increases Since 2021

2021 - - -> 2022

	Account Opening		Account Login		Distribution of Funds	
	Online	**Mobile**	**Online**	**Mobile**	**Online**	**Mobile**
U.S. Banks	**Verification** Phone # (23% -> 33%) Email/device (23% -> 42%)	**Verification** Email/device (31% -> 41%)	Assessing risk by country (23% -> 31%)	**Verification** Address (27% -> 34%)	Balancing fraud prevention friction (24% -> 38%) Lack of specialized tools (23% -> 35%)	Balancing fraud prevention friction (24% -> 37%)
U.S. Investment Firms			Manual reviews (25% -> 36%) **Verification** Phone (23% -> 31%)	Knowing origination source (23% -> 34%) **Verification** Identity (25% -> 33%)	Malicious bot transactions (23% -> 45%)	Balancing fraud prevention friction (25% -> 36%) Manual reviews (22% -> 34%) Malicious bot transactions (21% -> 30%)
U.S. Credit Lenders	**Verification** Email/device (27% -> 36%)	**Verification** Email/device (27% -> 36%)		Knowing origination source (26% -> 36%)	New transaction methods (27% -> 34%) Balancing fraud prevention friction (21% -> 31%)	New transaction methods (29% -> 38%) Manual reviews (18% -> 30%) **Verification** Email/device (23% -> 32%)
U.S. Mortgage Firms	Assessing risk by country (27% -> 41%) **Verification** Phone # (27% -> 46%)	**Verification** Phone (41% -> 48%) Email/device (28% -> 45%)	Assessing risk by country (17% -> 38%) Balancing fraud prevention friction (22% -> 34%) **Verification** Address (31% -> 47%)	Balancing fraud prevention friction (22% -> 36%) Assessing risk by country (17% -> 38%) **Verification** Address (22% -> 30%) Email/device (30% -> 38%)	Lack of specialized tools (25% -> 39%) **Verification** Phone (25% -> 39%) Identity (30% -> 38%)	New transaction methods (26% -> 55%) Manual reviews (29% -> 37%) Knowing origination source (25% -> 35%)

Survey Questions:
Q20A/B: 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.

Key Finding 3

TOP ONLINE/MOBILE CHANNEL CHALLENGES ACROSS THE CUSTOMER JOURNEY

Canadian financial institutions have seen a greater number of challenges, such as customer verification, malicious bot transactions, manual order reviews, assessing fraud risk and balancing fraud prevention friction with customer experience.

Top Online/Mobile Challenges: Notable Increases Since 2021

2021 - - ▶ 2022

	Account Opening		Account Login		Distribution of Funds	
	Online	**Mobile**	**Online**	**Mobile**	**Online**	**Mobile**
Canada Financial Services	**Verification** Address (24% -> 52%)	Assessing risk by country (16% -> 33%) Manual reviews (24% -> 31%)	Malicious bot transactions (20% -> 36%) Knowing origination source (24% -> 34%)	**Verification** Email/device (21% -> 37%) Identity (23% -> 37%)	**Verification** Email/device (23% -> 34%) Identity (31% -> 49%)	New transaction methods (17% -> 31%)
Canada Lending	Assessing risk by country (19% -> 37%) **Verification** Identity (26% -> 36%)	Manual reviews (23% -> 31%) **Verification** Address (27% -> 46%) Email/device (24% -> 48%)	Lack of specialized tools (19% -> 30%) **Verification** Address (27% -> 36%) Phone (30% -> 39%) Identity (32% -> 43%)	Balancing fraud prevention friction (28% -> 41%) **Verification** Address (21% -> 52%)	Balancing fraud prevention friction (27% -> 45%) Malicious bot transactions (17% -> 44%) Manual reviews (23% -> 32%)	**Verification** Phone (23% -> 38%) Identity (19% -> 39%)

Survey Questions:
Q20A/B: 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.

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Scams involving phishing, money mules and wire transfers are driving the increase in digital identity verification challenges at the new account creation stage.

For both online and mobile channel transactions at the account creation stage of the customer journey, firms that are experiencing more types of scams are significantly more likely to rank email and phone number verification among their top three fraud detection challenges than those who are dealing with few or no scams. As noted on slides 23 and 24, these are the challenges that have increased most at this stage.

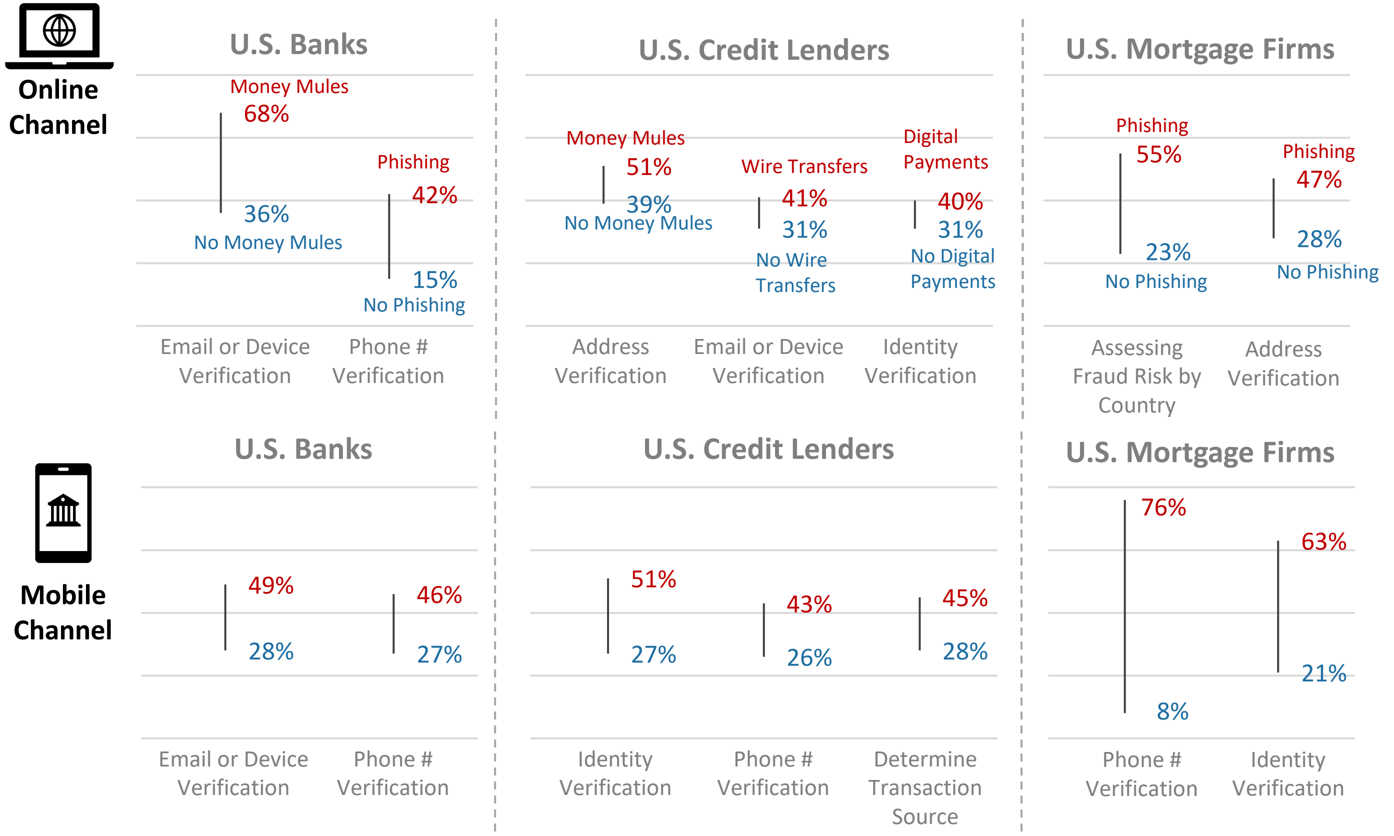
When comparing the difference between those dealing with money mule and phishing scams, the impact at this stage is most acute with U.S. banks and mortgage firms regarding email device verification (banks/online), assessing risk of non-domestic transactions (mortgage/online) and phone number verification (mortgage/mobile).

Survey Question:
Q20A/B: 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.

Fraud Detection Challenges by Variety of Scams: New Account Creation

Experiencing Multiple Types of Scams Overall (or experiencing a specifically noted scam)

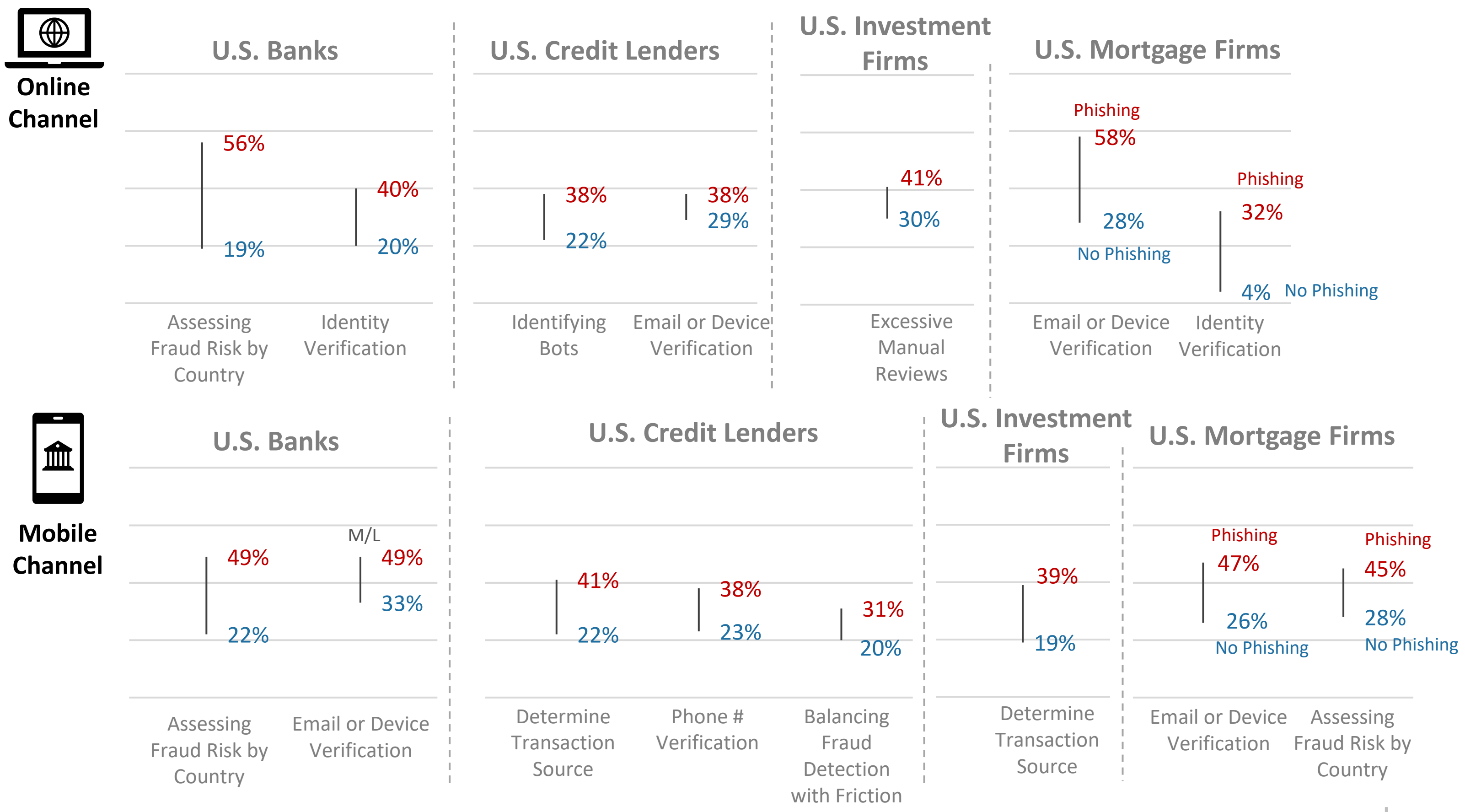
Experiencing One or No Types of Scams Overall (or not experiencing a specifically noted scam)



Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Along with email/device verification, challenges assessing non-domestic access risks and sources are heightened by scams during the account login stage.

Phishing attempts are impacting U.S. mortgage firms, while banks and lenders are challenged by multiple types of scams at this stage.



Fraud Detection Challenges by Level of Scams: Account Login

Experiencing Multiple Types of Scams Overall (or experiencing a specifically noted scam)

Experiencing 1 or No Types of Scams Overall (or not experiencing a specifically noted scam)

Survey Question:
Q20A/B: 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.

Financial institutions experiencing a variety of scams overall are more likely to indicate challenges with assessing non-domestic fraud risks and minimizing friction during the distribution of funds stage.

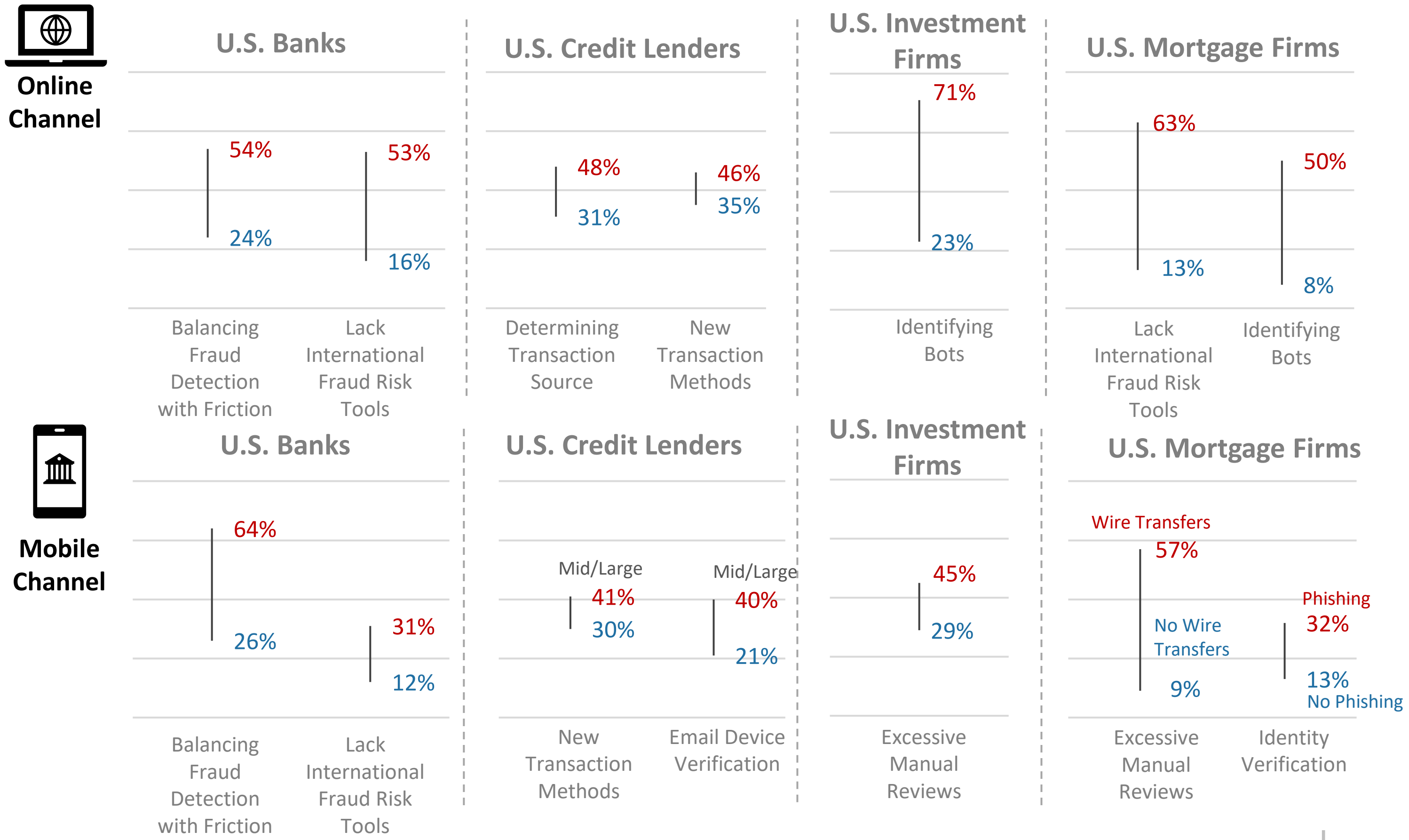
U.S. banks and mortgage firms are particularly impacted by these scams and challenges.

As noted earlier, wire transfer fraud is a common mortgage-related scam where fraudsters impersonate escrow officers, real estate agents or the lender to get the homeowner to wire funds into an illegitimate account for financial gain during the closing process. This is creating excessive manual reviews at this stage for many firms.

Fraud Detection Challenges by Level of Scams: Distribution of Funds

Experiencing Multiple Types of Scams Overall (or experiencing a specifically noted scam)

Experiencing 1 or No Types of Scams Overall (or not experiencing a specifically noted scam)



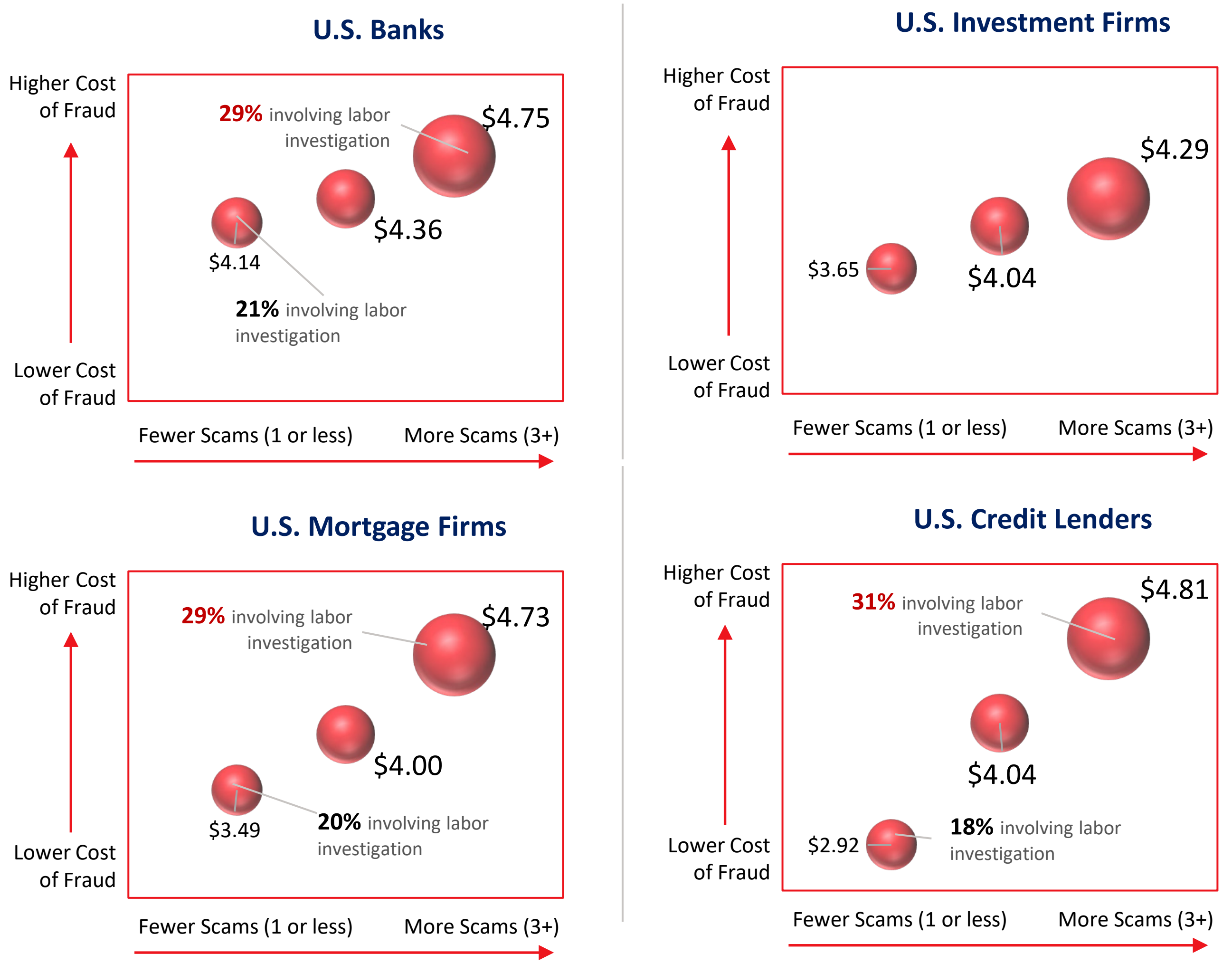
Survey Question:
Q20A/B: Please rank the top 3 challenges for each customer journey stage related to fraud faced by your company when serving customers using the ONLINE/MOBILE channel.

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Scams are negatively impacting financial services and lending fraud costs.

Banks, mortgage firms and credit lenders are particularly impacted. Those firms that experience more types of scams have significantly higher fraud costs that involve a sizeable portion of labor investigation compared to those which are not dealing with scams.

Cost of Fraud: LexisNexis Fraud Multiplier™



Survey Questions:
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. Q12e: Which types of the following scams have contributed to your fraud losses during the past 12 months?

▼▲ = significantly or directionally higher/lower than pre-pandemic

● Size equals relative comparison based on costs and level of scams; larger size equals more types of scams and higher fraud cost

Key Finding 4

Financial institutions’ adoption of Buy Now, Pay Later is expected to grow within the next 12 – 18 months. With that comes fraud detection challenges for banks and credit lenders.

While BNPL adoption is still in an early phase for banks and credit lenders, there are fraud detection challenges.

These challenges are based on the need for assessing risk with difficulty determining a transaction origination, ensuring that BNPL providers are compliant with financial regulations, lacking consistency across payment apps and dealing with false positives.

Ensuring BNPL provider compliance is important since, for many financial institutions, the business model for offering this point-of-sale credit will be through partnering with a BNPL provider or other credit institution.

Key Finding 4

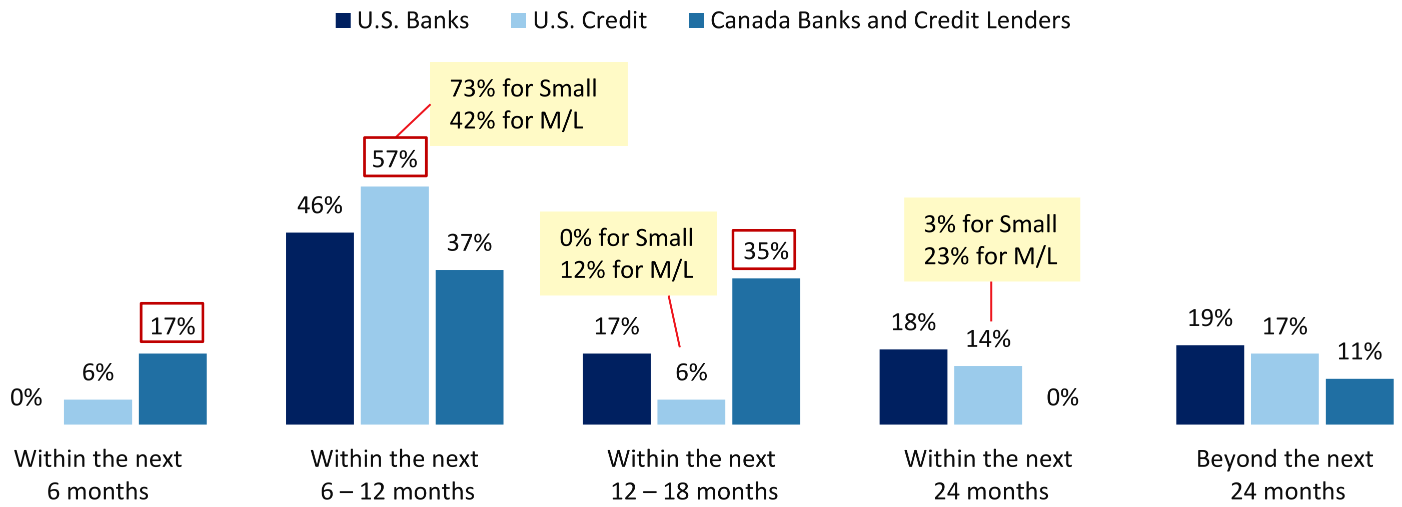
TIMELINE TO ROLL OUT BUY NOW, PAY LATER CREDIT

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Among U.S. and Canadian financial institutions expecting to offer point-of-sale BNPL credit in the future, a majority plan to do so within the next 18 months, particularly Canadian banks and credit lenders.

Larger U.S. credit lenders are more likely than smaller ones to make the rollout less of a priority.

Expected Rollout of Point-of-Sale Buy Now, Pay Later Credit*



73% for Small
42% for M/L

0% for Small
12% for M/L

3% for Small
23% for M/L

Survey Question:
Q3n2: When does your financial institution plan to offer point-of-sale Buy Now, Pay Later credit?

* Asked of those who currently offer point-of-sale BNPL credit.

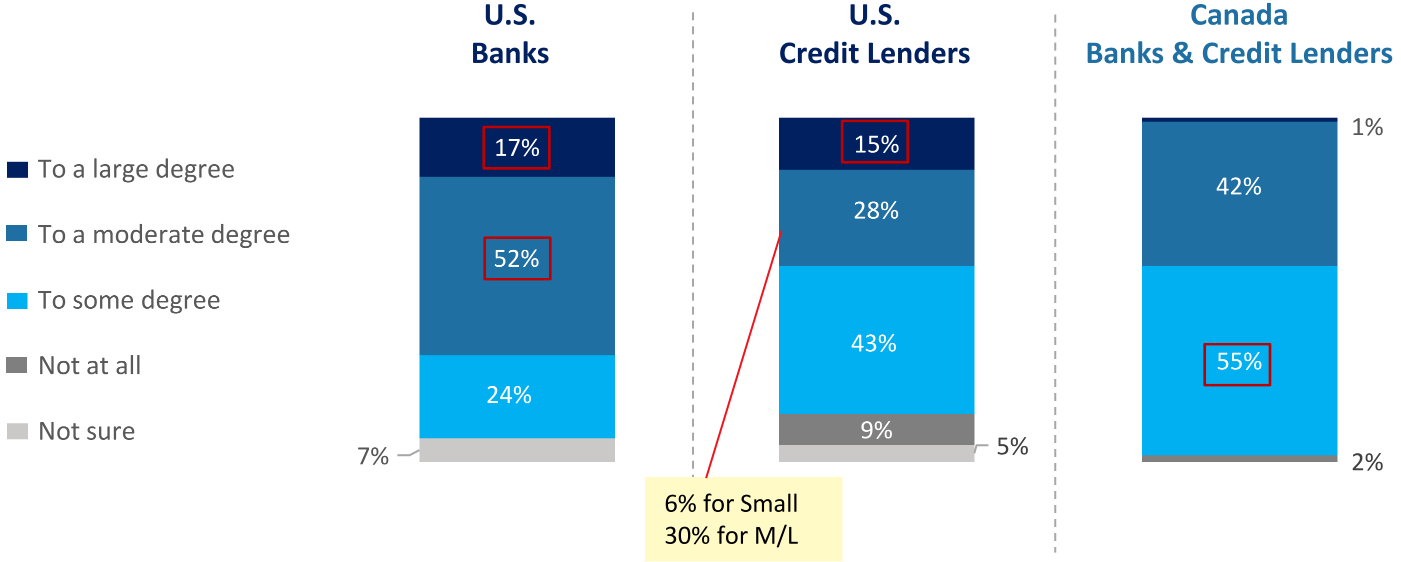
□ = significantly or directionally higher than same response in other segment

BNPL can create challenges with fraud detection.

U.S. banks that provide this type of credit are particularly likely to say that it has had at a moderate/large impact on their fraud detection efforts.

Degree That Providing Point-of-Sale Credit Via Buy Now, Pay Later* Creates Challenges for Fraud Detection

(Past 12 Months)



6% for Small
30% for M/L

Survey Question:
Q20e. To what degree has providing point-of-sale credit via Buy Now, Pay Later created challenges to your fraud detection and prevention processes/operations during the past year?

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

* Asked of those who currently offer point-of-sale BNPL credit.

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

U.S. and Canadian banks and credit lenders have different perceived fraud detection challenges with BNPL.

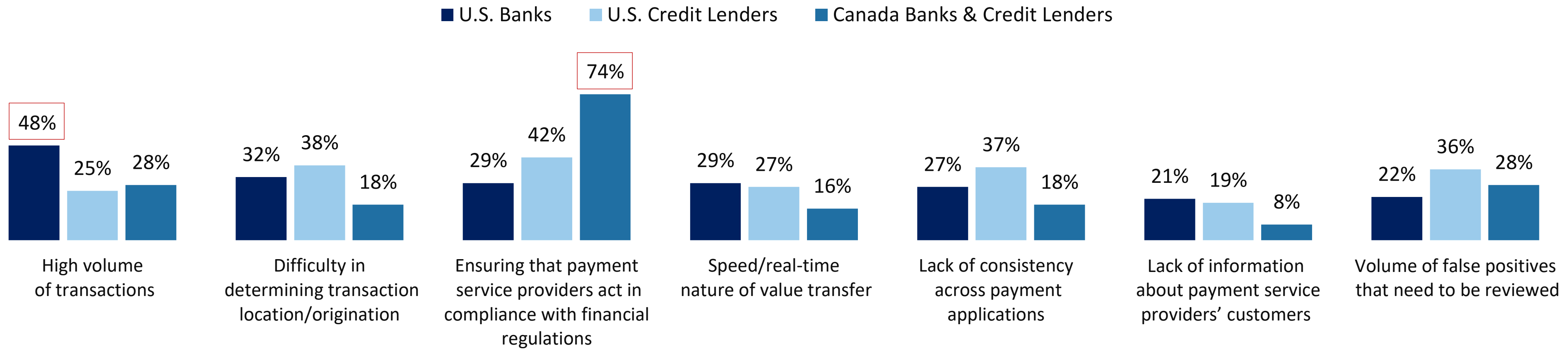
For U.S. banks, the high volume of transactions presents a challenge.

For U.S. credit lenders, key challenges include difficulty determining transaction origination, ensuring that BNPL providers are regulatory compliant, a lack of consistency across payment applications and false positives.

Ensuring provider compliance is the top challenge for Canadian banks and credit lenders.

Challenges to Fraud Detection and Prevention Processes/Operations With Transactions Made Through POS Credit via BNPL Apps*

(large degree)



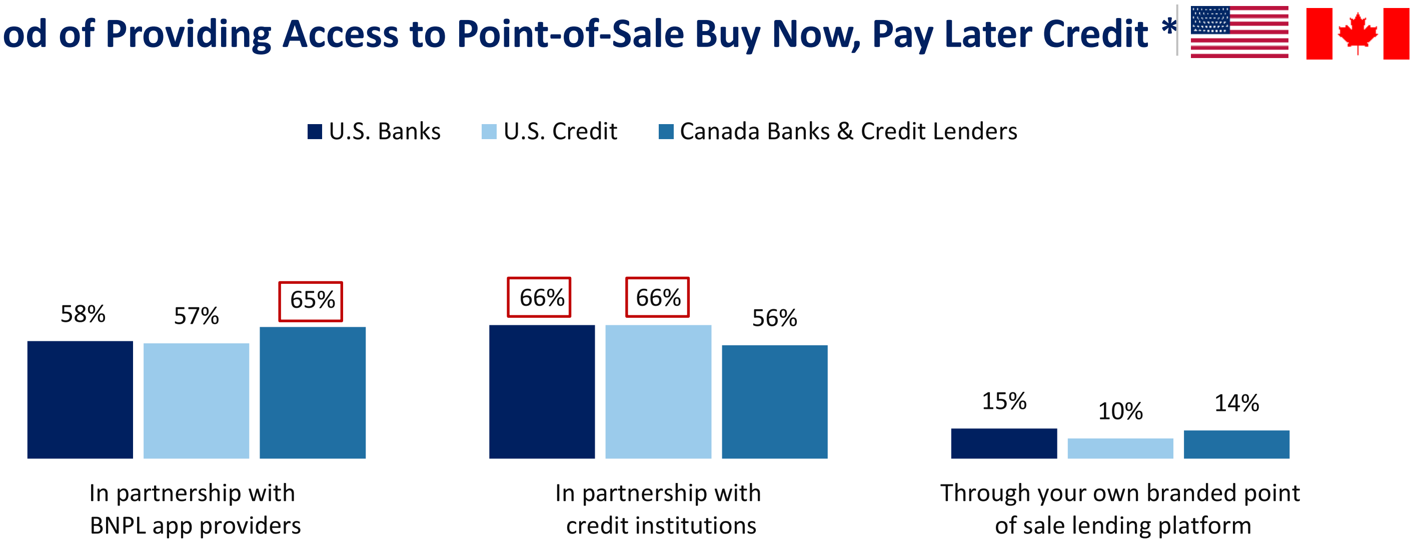
Survey Question:
Q20f: Over the past year, to what degree have the following been challenging to your fraud detection and prevention processes/operations with transactions made through point-of-sale credit via Buy Now, Pay Later apps?

* Asked of those who experience a moderate or large degree of challenge to fraud detection and prevention processes/operations providing point-of-sale credit via Buy Now, Pay Later.

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

Ensuring BNPL provider compliance is important since, for many financial institutions, the business model for offering this point-of-sale credit will be through partnering with a BNPL provider or other credit institution.

Method of Providing Access to Point-of-Sale Buy Now, Pay Later Credit *



Survey Question:
Q3n3: Through institution provide access to point-of-sale Buy which method does (or will) your Now, Pay Later credit?

* Asked of those currently offer point-of-sale BNPL credit, or are planning to.

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

Key Finding 5

Identity verification is a top challenge that contributes to fraud losses across the customer journey.

Identity-related fraud is occurring across the customer journey, with new account creation continuing an upward trend as a source for this type of fraud.

U.S. banks that are dealing with multiple types of scams attribute more identity-related fraud to new account creation.

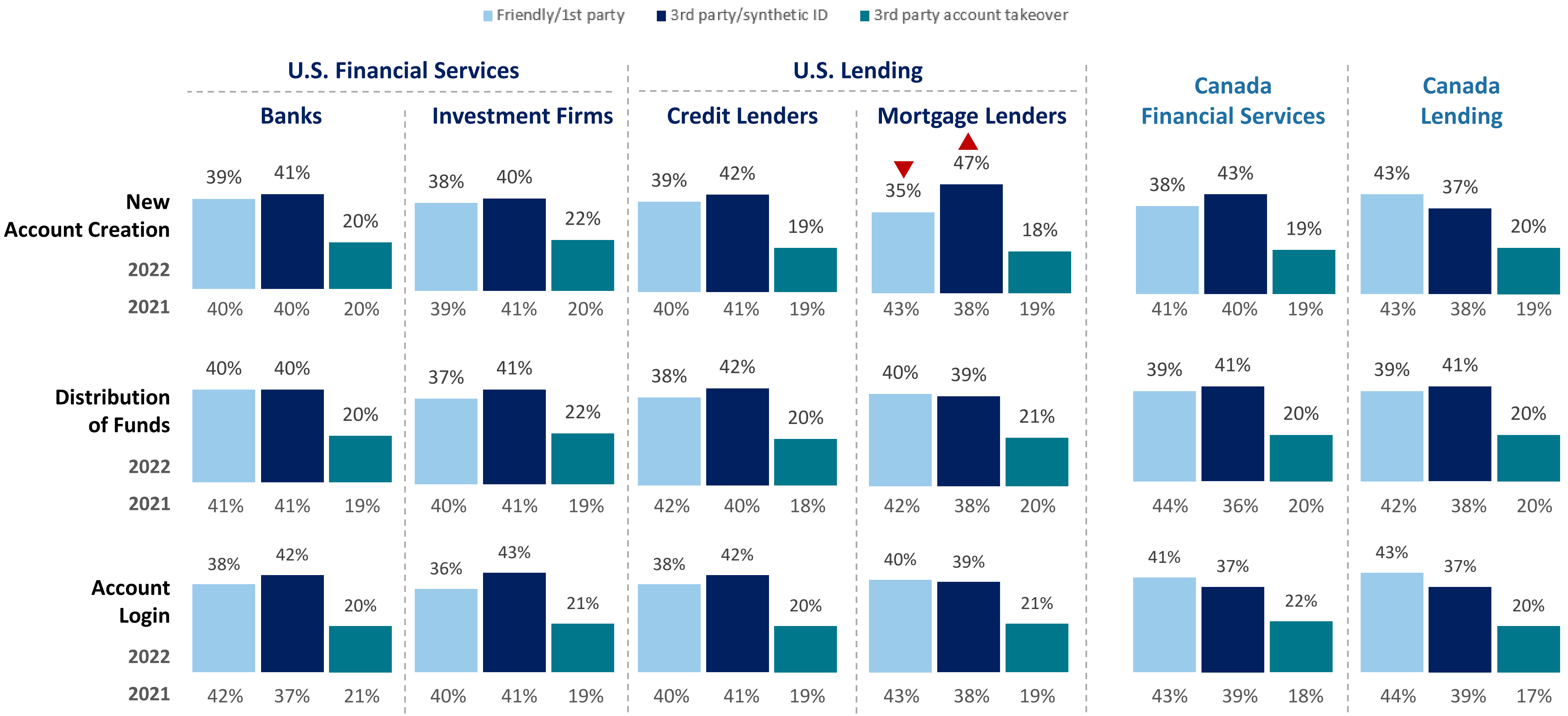
Key Finding 5

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

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Friendly/first-party and third-party/synthetic identity fraud continue to drive fraud losses for financial institutions 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.

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

LexisNexis® RISK SOLUTIONS

Key Finding 5

INCREASED LOSSES DUE TO IDENTITY- AND ACCOUNT-RELATED FRAUD

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

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

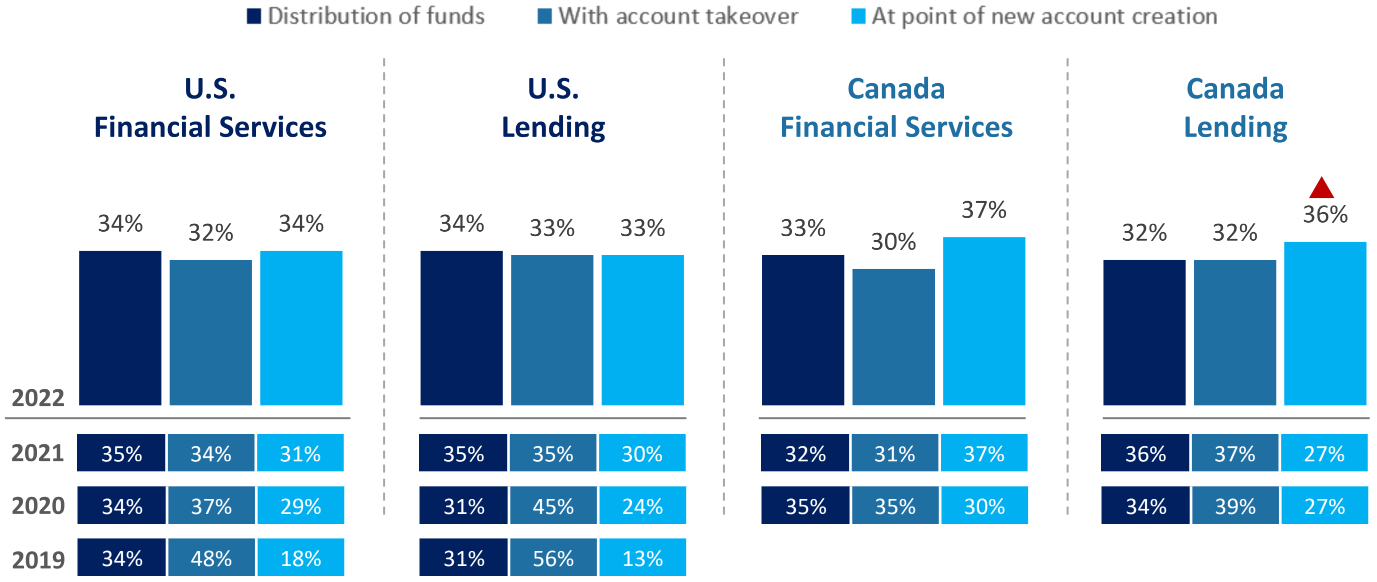
The growth in share of new account creation activities in identity-related fraud is not unexpected since new account creation is viewed as being the riskier customer journey point.

U.S. banks that are facing multiple types of scams attribute more identity-related fraud to new account creation.

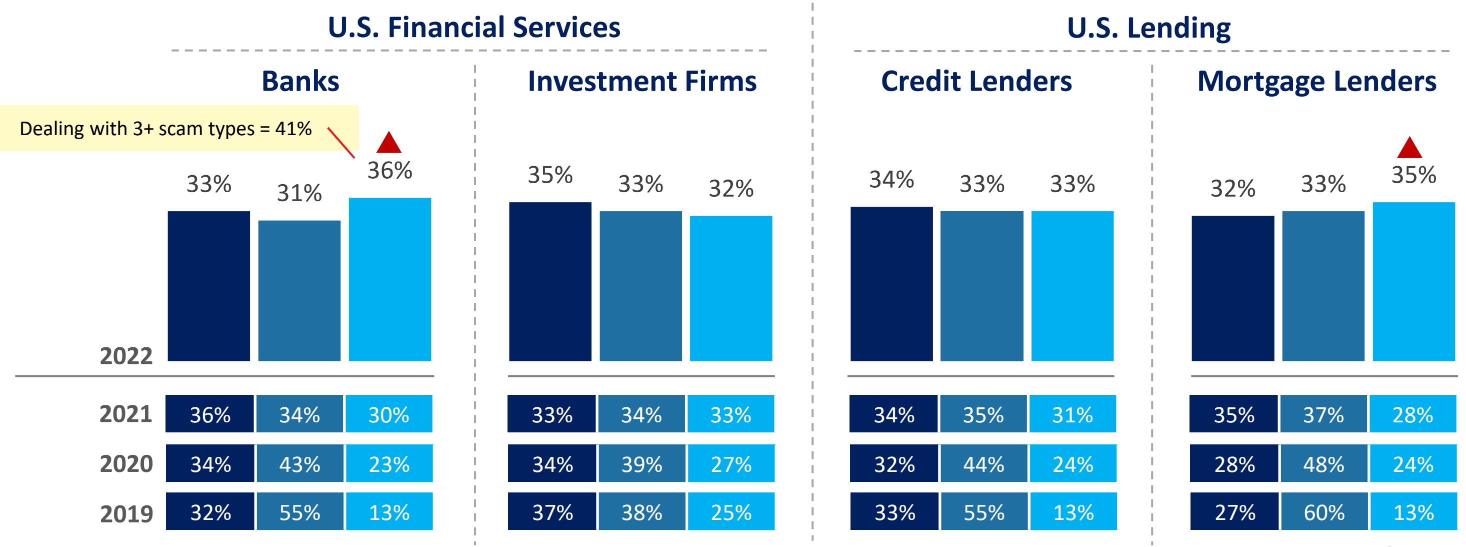
Survey Question:
Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?

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

Identity-Related Fraud: % Distribution by Activity



	U.S. Financial Services			U.S. Lending			Canada Financial Services			Canada Lending		
2021	35%	34%	31%	35%	35%	30%	32%	31%	37%	36%	37%	27%
2020	34%	37%	29%	31%	45%	24%	35%	35%	30%	34%	39%	27%
2019	34%	48%	18%	31%	56%	13%						



	Banks			Investment Firms			Credit Lenders			Mortgage Lenders		
2021	36%	34%	30%	33%	34%	33%	34%	35%	31%	35%	37%	28%
2020	34%	43%	23%	34%	39%	27%	32%	44%	24%	28%	48%	24%
2019	32%	55%	13%	37%	38%	25%	33%	55%	13%	27%	60%	13%

LexisNexis® RISK SOLUTIONS

Key Finding 6

Smart 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 remote digital channels.

There has been increased investment in risk mitigation solutions, particularly digital identity verification (email and phone number risk assessment and verification) and two-factor authentication (e.g. OTP). There are also some financial services and lending firms that have fully integrated cybersecurity operations, the digital customer experience and fraud prevention. However, fewer financial services and lending firms are using a multi-layered solutions approach in combination with risk mitigation solutions and integration of cybersecurity operations and digital CX with fraud prevention.

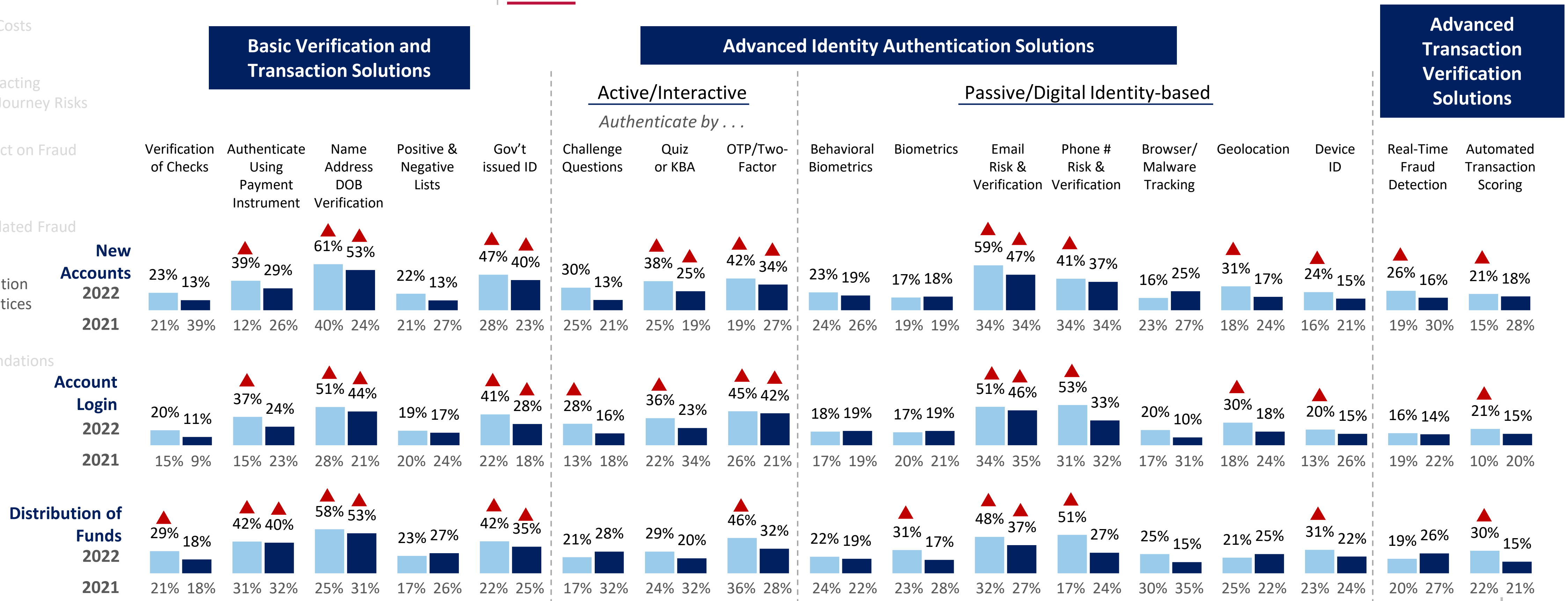
Firms that are using a multi-layered solutions approach tend to have a lower cost of fraud and fewer challenges across each customer journey stage. For example, firms with multi-layered digital solutions involving biometrics are very unlikely to experience mobile challenges in the distribution of funds stage, such as manual reviews (6%) and balancing fraud detection with friction (2%).

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Across the customer journey, there has been an increase in adoption of some advanced identity authentication solutions among U.S. financial services firms, with more banks particularly adopting email and phone number risk and verification solutions.

There is, however, a sizeable majority that is not using these solutions.

Fraud Mitigation Solutions Use | U.S. Financial Services



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

▲ = significantly or directionally higher than previous period

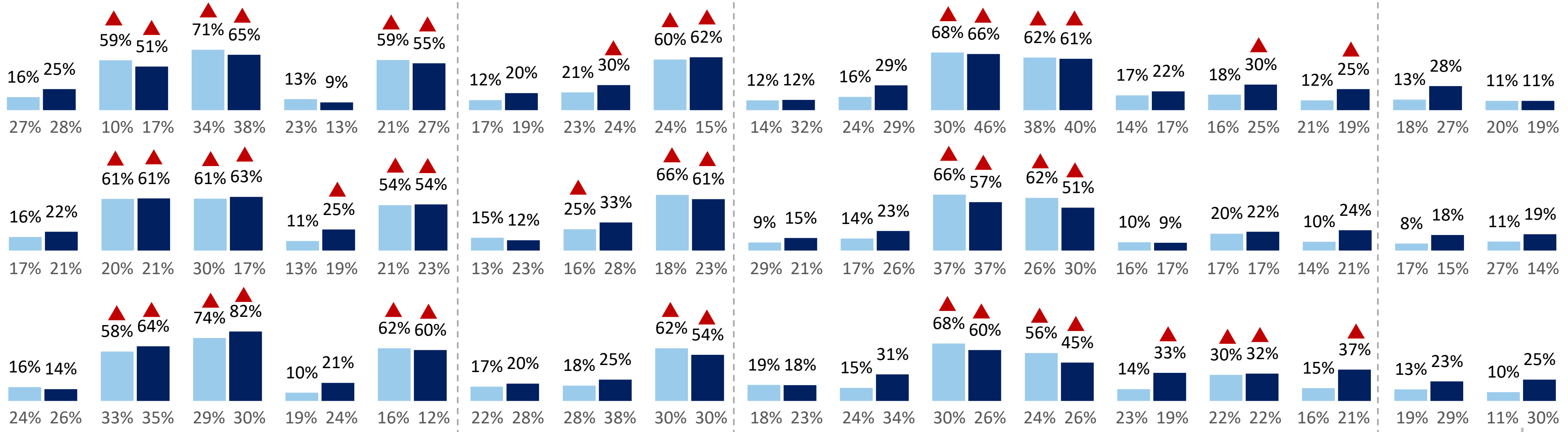
Key Finding 6

FRAUD MITIGATION SOLUTIONS USE ACROSS THE CUSTOMER JOURNEY

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

The number of U.S. lenders adopting fraud mitigation solutions have significantly increased, particularly two-factor authentication and email/phone number risk and verification. There is, however, still limited use of other digital identity-based solutions.

Fraud Mitigation Solutions Use | U.S. Lending ■ US Credit Lenders ■ US Mortgage Lenders



	Basic Verification and Transaction Solutions					Advanced Identity Authentication Solutions										Advanced Transaction Verification Solutions	
						Active/Interactive *Authenticate by . . .*			Passive/Digital Identity-based								
	Verification of Checks	Authenticate Using Payment Instrument	Name Address DOB Verification	Positive & Negative Lists	Gov't issued ID	Challenge Questions	Quiz or KBA	OTP/Two-Factor	Authenticate Using Behavioral Biometrics	Authenticate Using Biometrics	Email Risk & Verification	Phone # Risk & Verification	Browser/ Malware Tracking	Geolocation	Device ID	Real-Time Fraud Detection	Automated Transaction Scoring
New Accounts 2022	16% 25%	▲59% ▲51%	▲71% ▲65%	13% 9%	▲59% ▲55%	12% 20%	21% ▲30%	▲60% ▲62%	12% 12%	16% 29%	▲68% ▲66%	▲62% ▲61%	17% 22%	18% ▲30%	12% ▲25%	13% 28%	11% 11%
2021	27% 28%	10% 17%	34% 38%	23% 13%	21% 27%	17% 19%	23% 24%	24% 15%	14% 32%	24% 29%	30% 46%	38% 40%	14% 17%	16% 25%	21% 19%	18% 27%	20% 19%
Account Login 2022	16% 22%	▲61% ▲61%	▲61% ▲63%	11% ▲25%	▲54% ▲54%	15% 12%	▲25% 33%	▲66% ▲61%	9% 15%	14% 23%	▲66% ▲57%	▲62% ▲51%	10% 9%	20% 22%	10% 24%	8% 18%	11% 19%
2021	17% 21%	20% 21%	30% 17%	13% 19%	21% 23%	13% 23%	16% 28%	18% 23%	29% 21%	17% 26%	37% 37%	26% 30%	16% 17%	17% 17%	14% 21%	17% 15%	27% 14%
Distribution of Funds 2022	16% 14%	▲58% ▲64%	▲74% ▲82%	10% 21%	▲62% ▲60%	17% 20%	18% 25%	▲62% ▲54%	19% 18%	15% 31%	▲68% ▲60%	▲56% ▲45%	14% ▲33%	▲30% ▲32%	15% ▲37%	13% 23%	10% 25%
2021	24% 26%	33% 35%	29% 30%	19% 24%	16% 12%	22% 28%	28% 38%	30% 30%	18% 23%	24% 34%	30% 26%	24% 26%	23% 19%	22% 22%	16% 21%	19% 29%	11% 30%

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

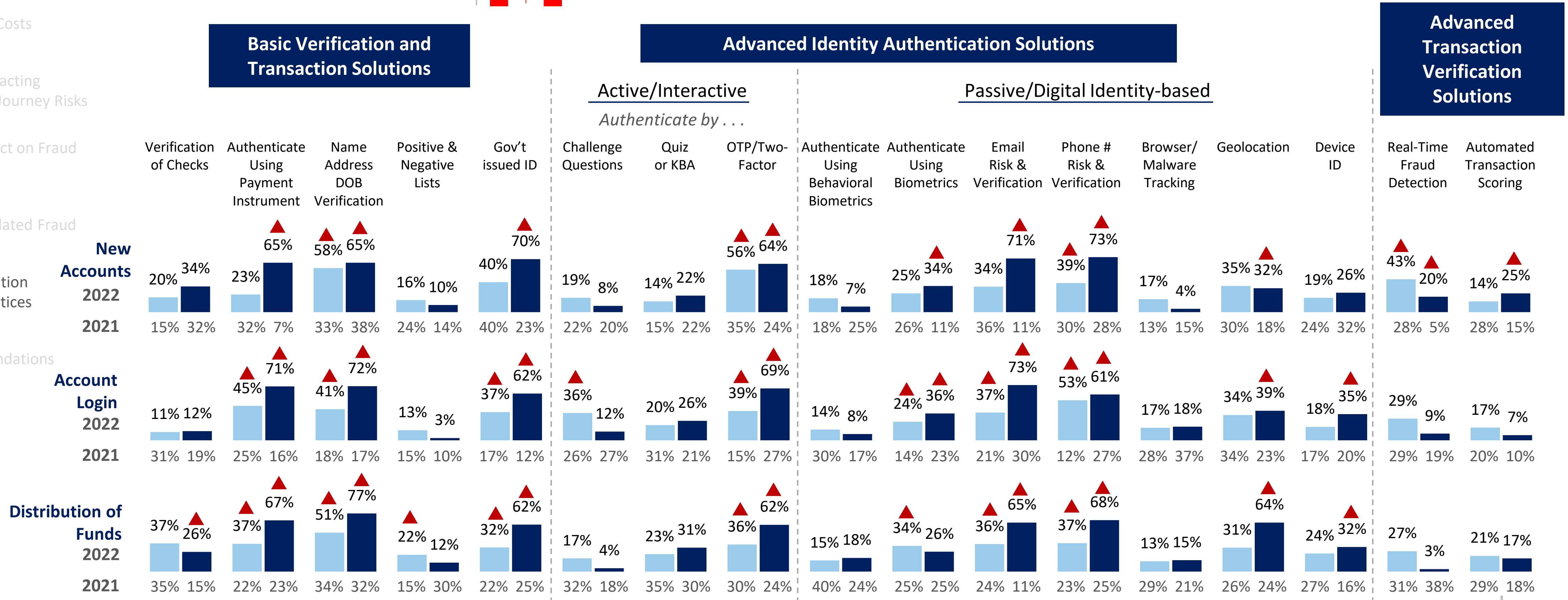
▲ = significantly or directionally higher than previous period

LexisNexis RISK SOLUTIONS

The number of Canadian institutions, particularly lending firms, adopting email/phone risk and verification solutions have significantly increased. However, there is still limited inclusion of other digital identity and transaction solutions.

Verification and authentication solutions seeing the greatest increase in adoption from 2021 include verification of name, address, DOB, email and phone, government-issued ID, as well as authentication using payment instrument and two-factor authentication.

Fraud Mitigation Solutions Use | Canada Financial Services & Lending



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

▲ = significantly or directionally higher than previous period

Key Finding 6

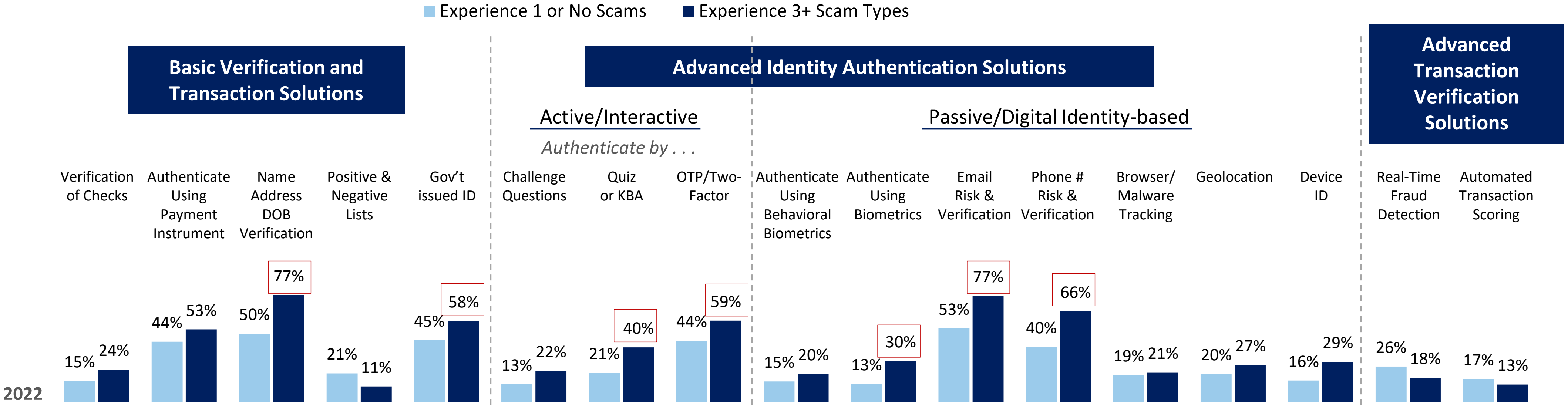
FRAUD MITIGATION SOLUTIONS USE AT NEW ACCOUNT CREATION

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

With the new account creation stage being a higher risk for scams, financial services and lending firms that are dealing with multiple types of scams are significantly more likely to have invested in fraud mitigation solutions, particularly digital identity email/phone risk and verification.

This indicates that, given higher fraud costs and challenges, they recognize the need for technology to detect and mitigate increasingly sophisticated digital-related scams.

Fraud Mitigation Solutions Use: New Account Creation | U.S. & Canadian Financial Services & Lending



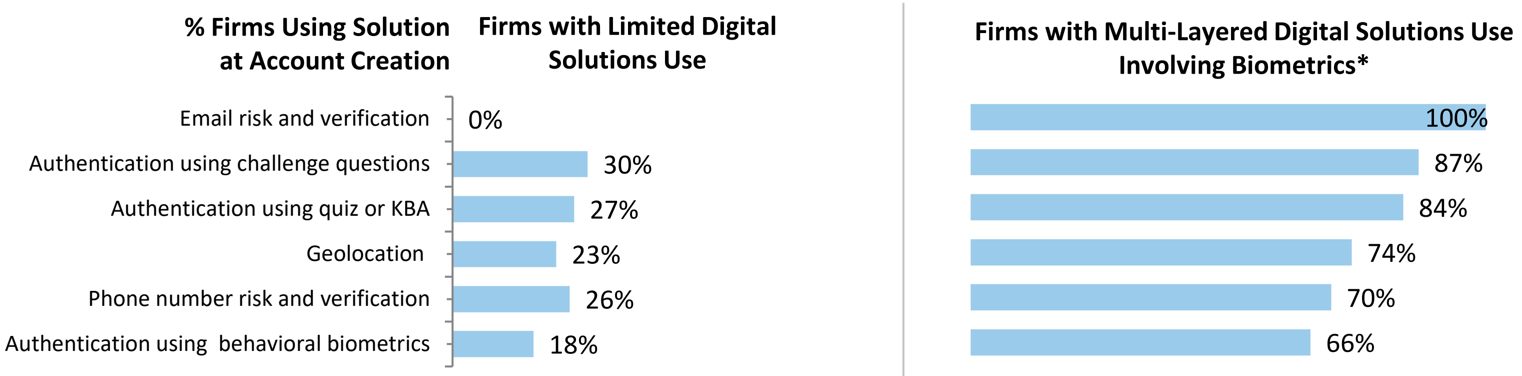
Survey Question: Q27: Which fraud detection/mitigation solutions does your company currently use for the following transaction or customer journey points?

= significantly or directionally higher than same solution in other segment

USE CASE: SOLUTIONS LAYERING FOR EFFECTIVE FRAUD DETECTION/MITIGATION DURING NEW ACCOUNT OPENING

A multi-layered digital identity solutions approach, including behavioral biometrics and email/device verification, for new account openings is significantly more effective at verifying identities and mitigating fraud costs.

U.S. Financial Services and Lending Solutions/Challenges/Cost Comparison: New Account Creation



	Firms with Limited Digital Solutions Use	Firms with Multi-Layered Digital Solutions Use Involving Biometrics*
% Indicating Top Online Channel Challenge	• Email/device verification (34%) • Assessing fraud by country (37%) • Address verification (39%)	• Email/device verification (22%) • Assessing fraud by country (23%) • Address verification (22%)
% Indicating Top Mobile Channel Challenge	• Email/device verification (37%) • Address verification (38%) • Phone # verification (55%)	• Email/device verification (19%) • Address verification (15%) • Phone # verification (33%)
Every $1 of fraud loss at Account Creation actually costs	**$4.28**	**$3.69**

Survey Question:
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.

* 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

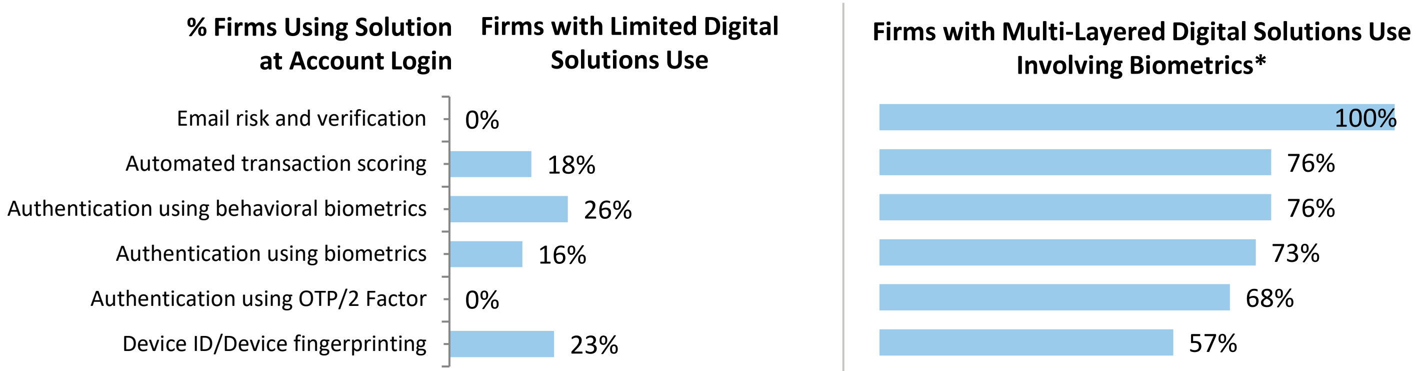
Key Finding 6

USE CASE: SOLUTIONS LAYERING FOR EFFECTIVE FRAUD DETECTION/MITIGATION DURING ACCOUNT LOGIN

Survey Question:
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.

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

U.S. Financial Services and Lending Solutions/Challenges/Cost Comparison: Account Login



	Firms with Limited Digital Solutions Use	Firms with Multi-Layered Digital Solutions Use Involving Biometrics*
% Indicating Top Online Channel Challenge	• Manual reviews (35%) • Balancing fraud detection with friction (31%)	• Manual reviews (20%) • Balancing fraud detection with friction (18%)
% Indicating Top Mobile Channel Challenge	• Email/device verification (36%) • Determining origination (37%) • Balancing fraud detection with friction (31%)	• Email/device verification (23%) • Determining origination (22%) • Balancing fraud detection with friction (20%)
Every $1 of fraud loss at Account Login actually costs	**$4.10**	**$3.38**

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

Overview

Key Findings

#1 Trends/Landscape

#2 Attacks & Costs

#3 Scams Impacting Customer Journey Risks

#4 BNPL Impact on Fraud Detection

#5 Identity-related Fraud

#6 Risk Mitigation Smart Practices

Recommendations

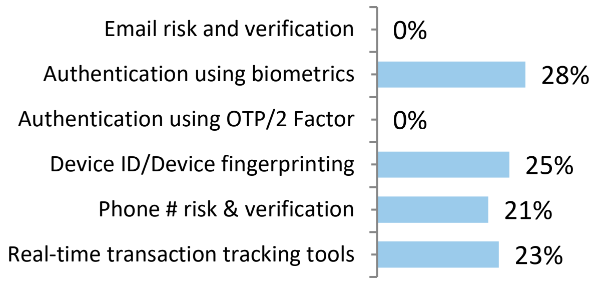
Survey Question:
Q20: Please rank the top 3 challenges for each customer journey stage related to fraud faced by your company when serving customers using the ONLINE/MOBILE channel.

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

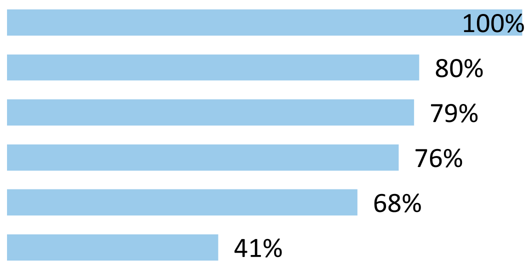
U.S. Financial Services and Lending Solutions/Challenges/Cost Comparison: Distribution of Funds

% Firms Using Solution at Distribution of Funds

Firms with Limited Digital Solutions Use



Firms with Multi-Layered Digital Solutions Use Involving Biometrics*



	Firms with Limited Digital Solutions Use	Firms with Multi-Layered Digital Solutions Use Involving Biometrics*
% Indicating Top Online Channel Challenge	• Identifying bots from humans (35%) • Phone # verification (34%)	• Identifying bots from humans (21%) • Phone # verification (24%)
% Indicating Top Mobile Channel Challenge	• Manual reviews (30%) • Determining origination (36%) • Balancing fraud detection with friction (29%)	• Manual reviews (6%) • Determining origination (8%) • Balancing fraud detection with friction (2%)
Every $1 of fraud loss at Distribution of Funds actually costs	**$4.50**	**$3.51**

* 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

Fraud tools need to authenticate both digital and physical criteria, as well as both identity and transaction risk.

FRAUD ISSUES

DIGITAL SERVICES

Fast transactions lead to easy synthetic identity and botnet targets. There is a **need for 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

There is a **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 occur often to test cards, passwords/credentials or infect devices.

MOBILE CHANNEL

Source origination and infected devices add risk. Mobile bots and malware increase risk of identity fraud. There is a **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 payment 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; two- factor authentication.

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 behavioral 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.

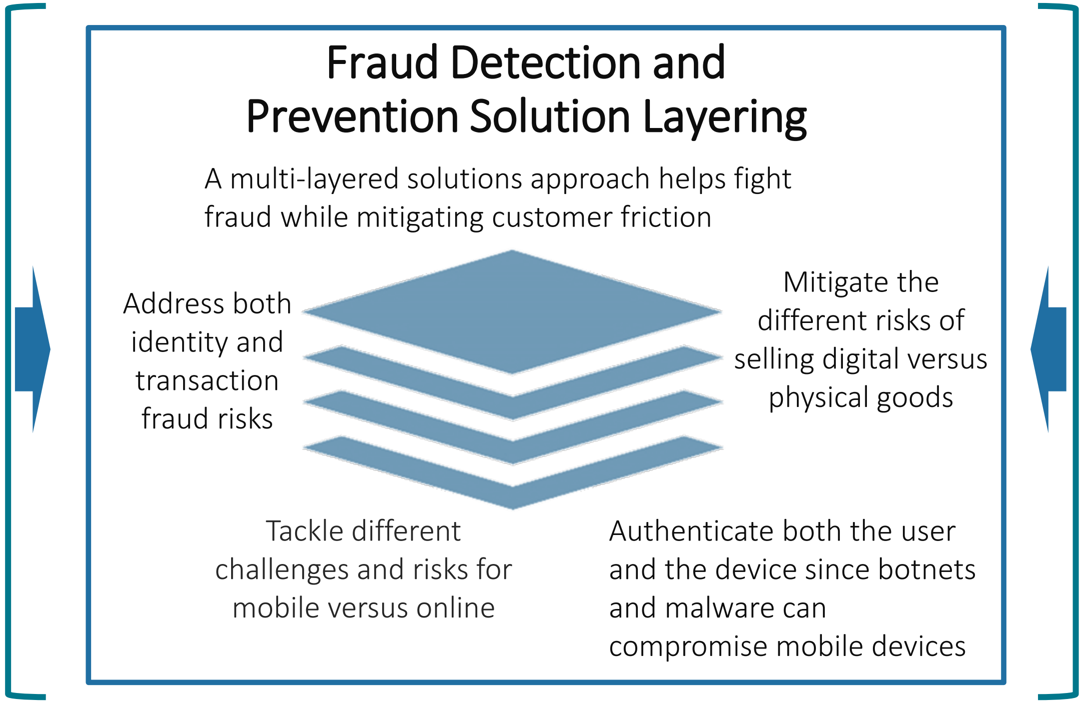
Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Smart practice approaches call for a layering of different solutions to address unique risks from different channels, payment methods and products. Additionally, firms should consider 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 solutions approach helps fight fraud while mitigating customer friction

Address both identity and transaction fraud risks

Mitigate the different risks of selling digital versus physical goods

Tackle different challenges and risks for mobile versus online

Authenticate both the user and the device since botnets and malware can compromise mobile devices

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

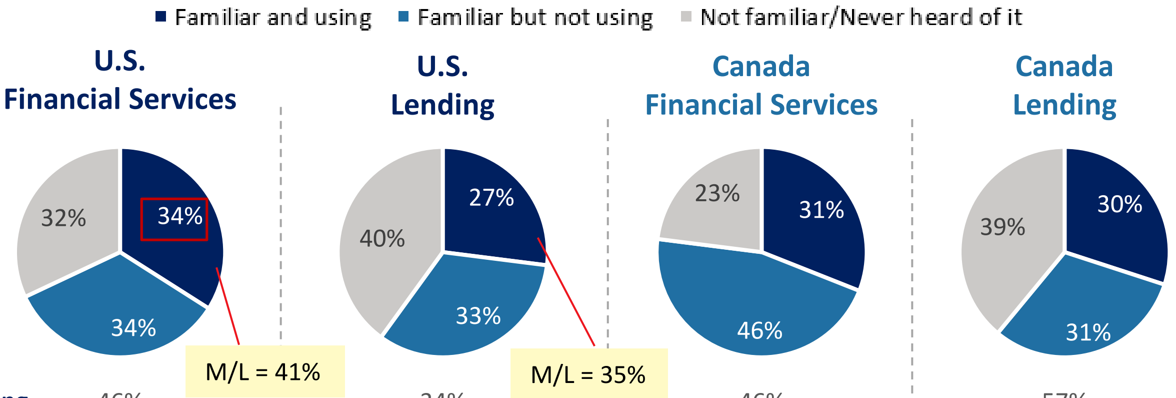
← Integration of Cybersecurity and Digital Customer Experience Operations with Fraud Prevention Approach →

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Larger U.S. financial services firms are more likely than other segments to be familiar with and using the FraudClassifier℠ Model, with a significant majority of those that have not yet adopted the model planning to do so within the next 6-12 months.

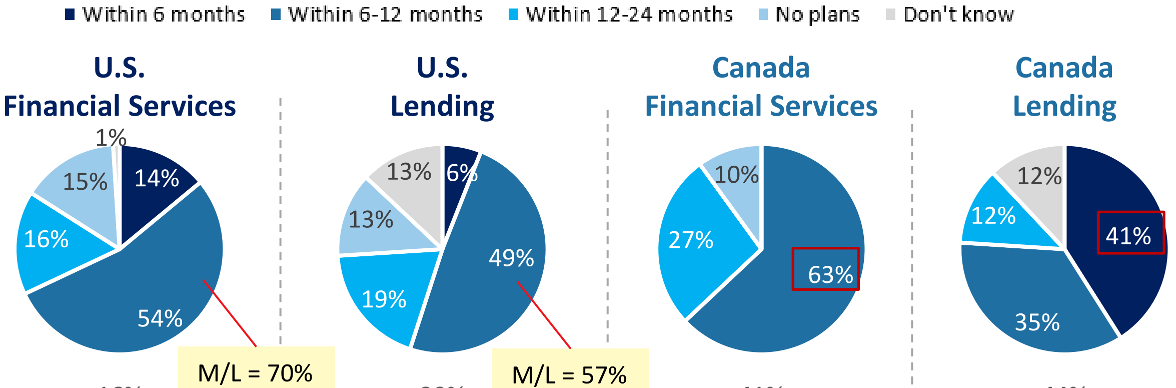
Survey Question:
Q14e: To what degree is your organization familiar with the FraudClassifier℠ model, published by the Federal Research in June 2020, to classify fraud related to payments?

Degree of Familiarity with FraudClassifier℠ Model



2021	U.S. Financial Services	U.S. Lending	Canada Financial Services	Canada Lending
% Familiar, using	46%	34%	46%	57%
% Familiar, not using	37%	49%	48%	41%
Not familiar	17%	17%	6%	2%

Plans to Use FraudClassifier℠ Model*



2021	U.S. Financial Services	U.S. Lending	Canada Financial Services	Canada Lending
6 months	16%	20%	41%	44%
6-12 months	30%	40%	19%	42%
12-24 months	29%	30%	32%	14%

□ = 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

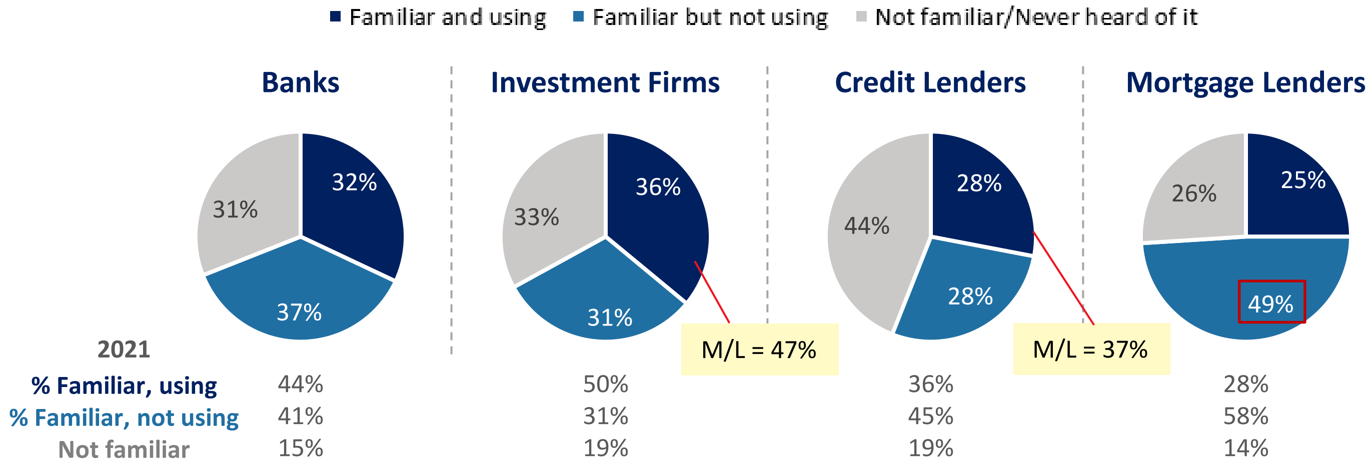
Key Finding 6
FRAUD DETECTION AND PREVENTION APPROACHES

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Mid/large U.S. investment firms and credit lenders are particularly likely to use the FraudClassifer℠ Model.

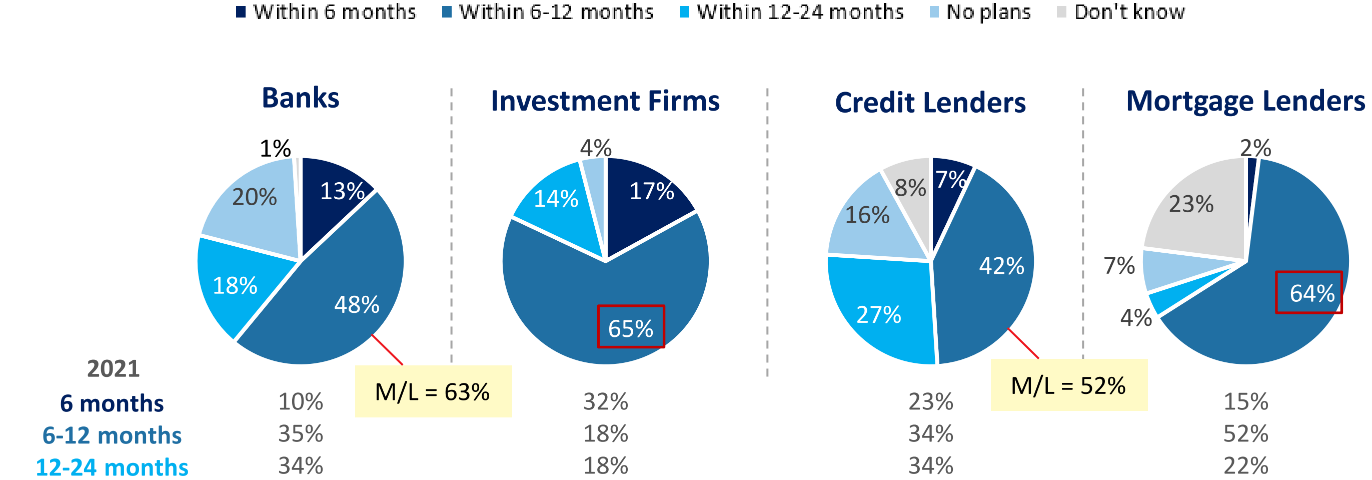
Among those that are familiar with the model but not yet using it, a significant majority expect to do so within the next 12 months.

Degree of Familiarity with FraudClassifier℠ Model



2021	Banks	Investment Firms	Credit Lenders	Mortgage Lenders
% Familiar, using	44%	50%	36%	28%
% Familiar, not using	41%	31%	45%	58%
Not familiar	15%	19%	19%	14%

Plans to Use FraudClassifier℠ Model*



2021	Banks	Investment Firms	Credit Lenders	Mortgage Lenders
6 months	10%	32%	23%	15%
6-12 months	35%	18%	34%	52%
12-24 months	34%	18%	34%	22%

Survey Question:
Q14e: To what degree is your organization familiar with the FraudClassifier℠ model, published by the Federal Research 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

Key Finding 6

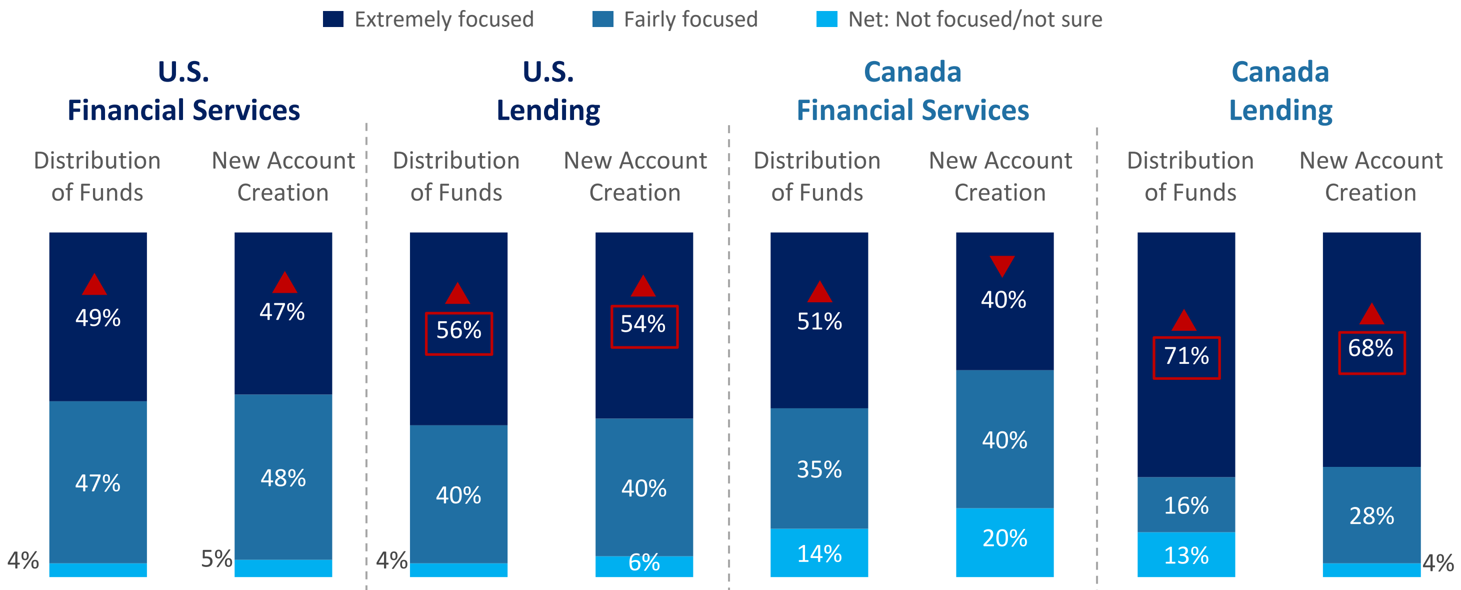
FRAUD DETECTION AND PREVENTION APPROACHES

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

U.S. and Canadian financial institutions are becoming more focused on optimizing risk assessment with the customer experience.

Across segments, significantly more firms indicate being extremely focused on optimizing risk to appropriate customer friction levels at both the distribution of funds and new account creation stages.

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



U.S. Financial Services				U.S. Lending				Canada Financial Services				Canada Lending			
Distribution of Funds		New Account Creation		Distribution of Funds		New Account Creation		Distribution of Funds		New Account Creation		Distribution of Funds		New Account Creation	
2020	2021	2020	2021	2020	2021	2020	2021	2020	2021	2020	2021	2020	2021	2020	2021
31%	41%	31%	39%	29%	39%	37%	36%	12%	36%	15%	53%	13%	27%	17%	49%
57%	51%	52%	54%	63%	49%	59%	46%	67%	62%	51%	40%	46%	66%	64%	40%
11%	8%	16%	7%	8%	12%	4%	18%	21%	2%	35%	7%	41%	7%	19%	11%

SMART PRACTICE

Minimize friction 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.

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

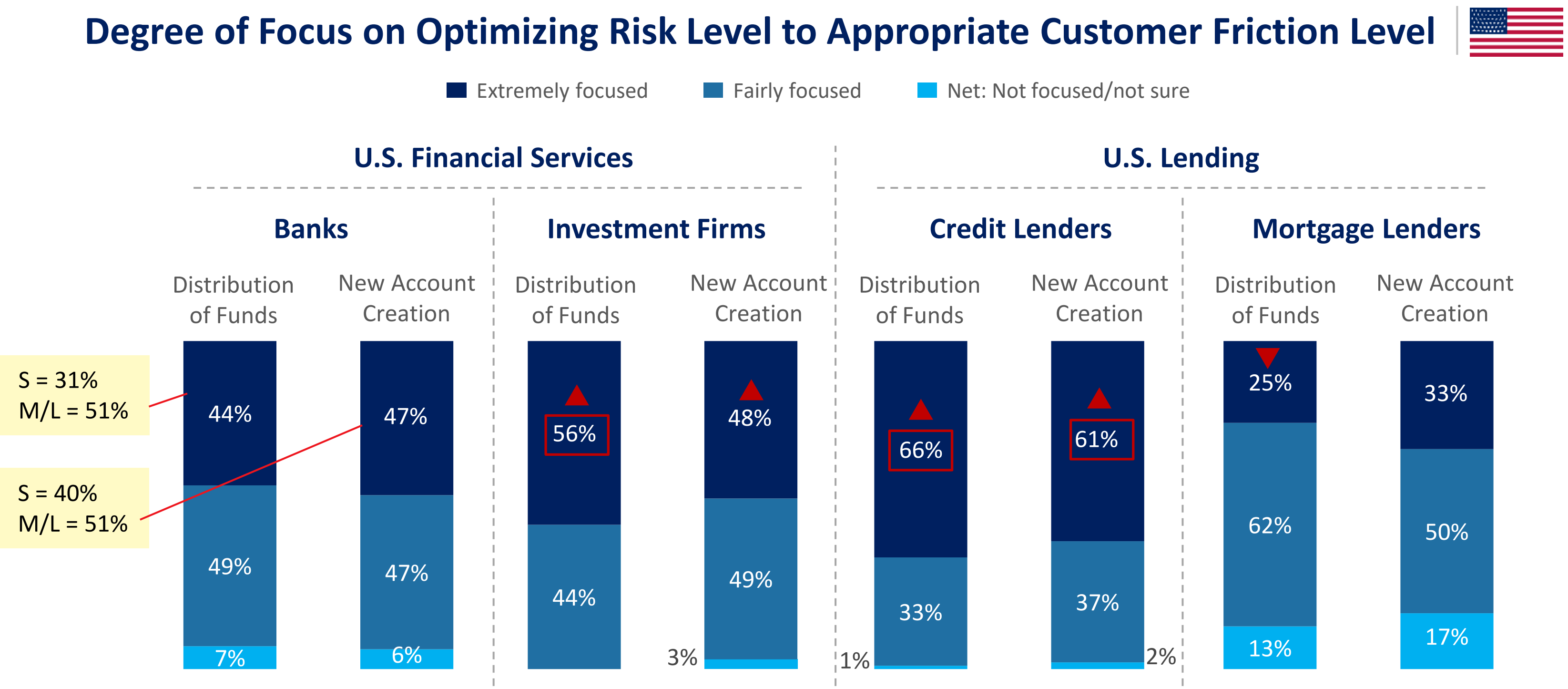
* Asked of those with online and/or mobile channel translations; first asked in 2020

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

Credit lenders in the U.S. tend to be extremely focused on optimizing risk assessment with the customer experience across distribution of funds and new account creation stages.

Larger banks are more likely than smaller banks to be extremely focused on such optimization.

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



		Extremely focused	Fairly focused	Net: Not focused/not sure
Banks – Distribution of Funds	2020	32%	54%	14%
	2021	38%	53%	9%
Banks – New Account Creation	2020	34%	48%	18%
	2021	42%	50%	7%
Investment Firms – Distribution of Funds	2020	31%	63%	6%
	2021	48%	47%	5%
Investment Firms – New Account Creation	2020	26%	61%	13%
	2021	35%	61%	4%
Credit Lenders – Distribution of Funds	2020	32%	60%	8%
	2021	39%	47%	14%
Credit Lenders – New Account Creation	2020	41%	54%	5%
	2021	39%	39%	22%
Mortgage Lenders – Distribution of Funds	2020	23%	70%	7%
	2021	40%	53%	7%
Mortgage Lenders – New Account Creation	2020	27%	71%	2%
	2021	30%	64%	6%

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

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

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

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

Key Finding 6

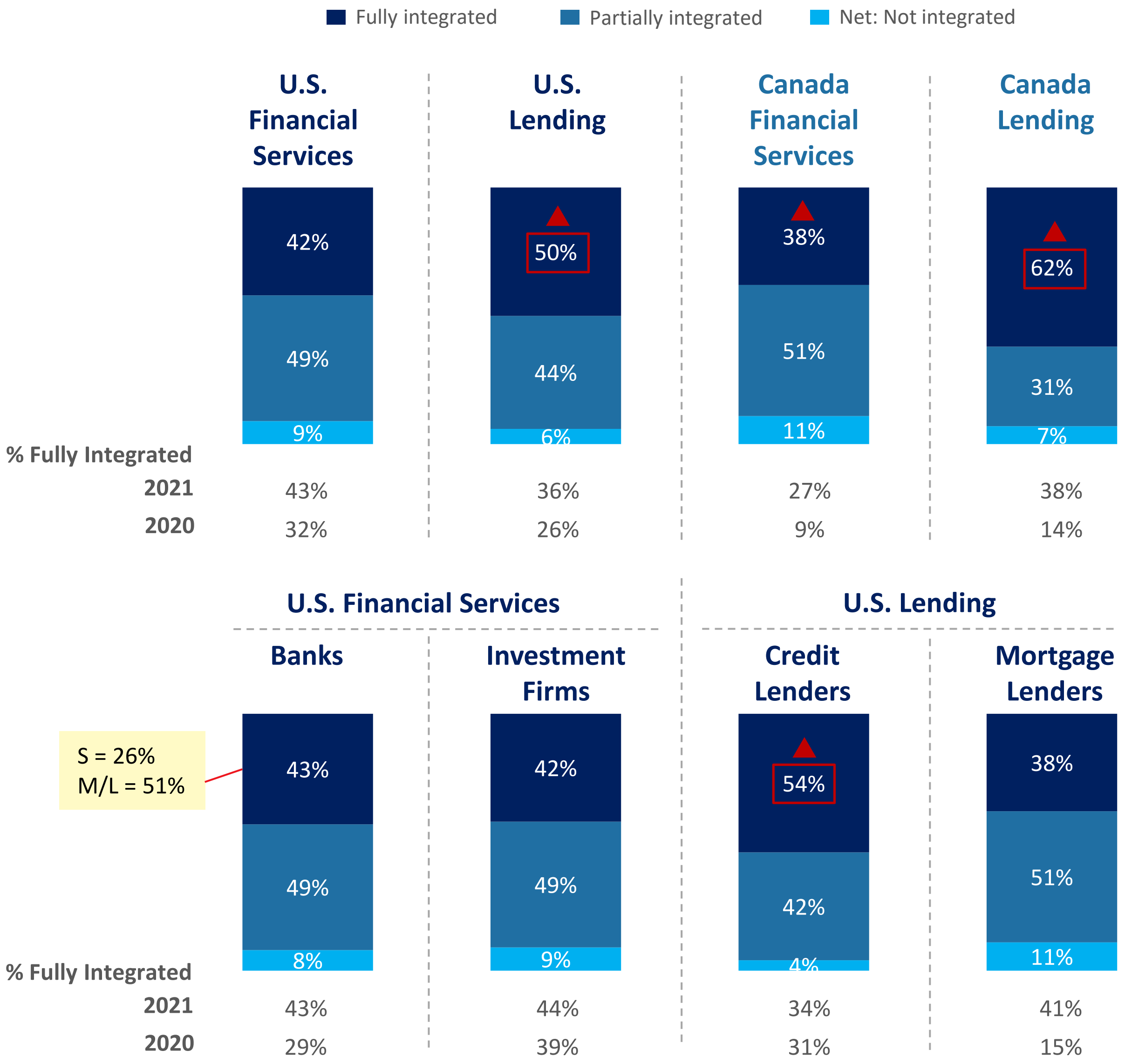
FRAUD DETECTION AND PREVENTION APPROACHES

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

There is a strong growth toward full integration of the digital/ customer experience with fraud prevention efforts, particularly among lending firms.

The increase among U.S. firms is primarily from larger banks and credit lenders.

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



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

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

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

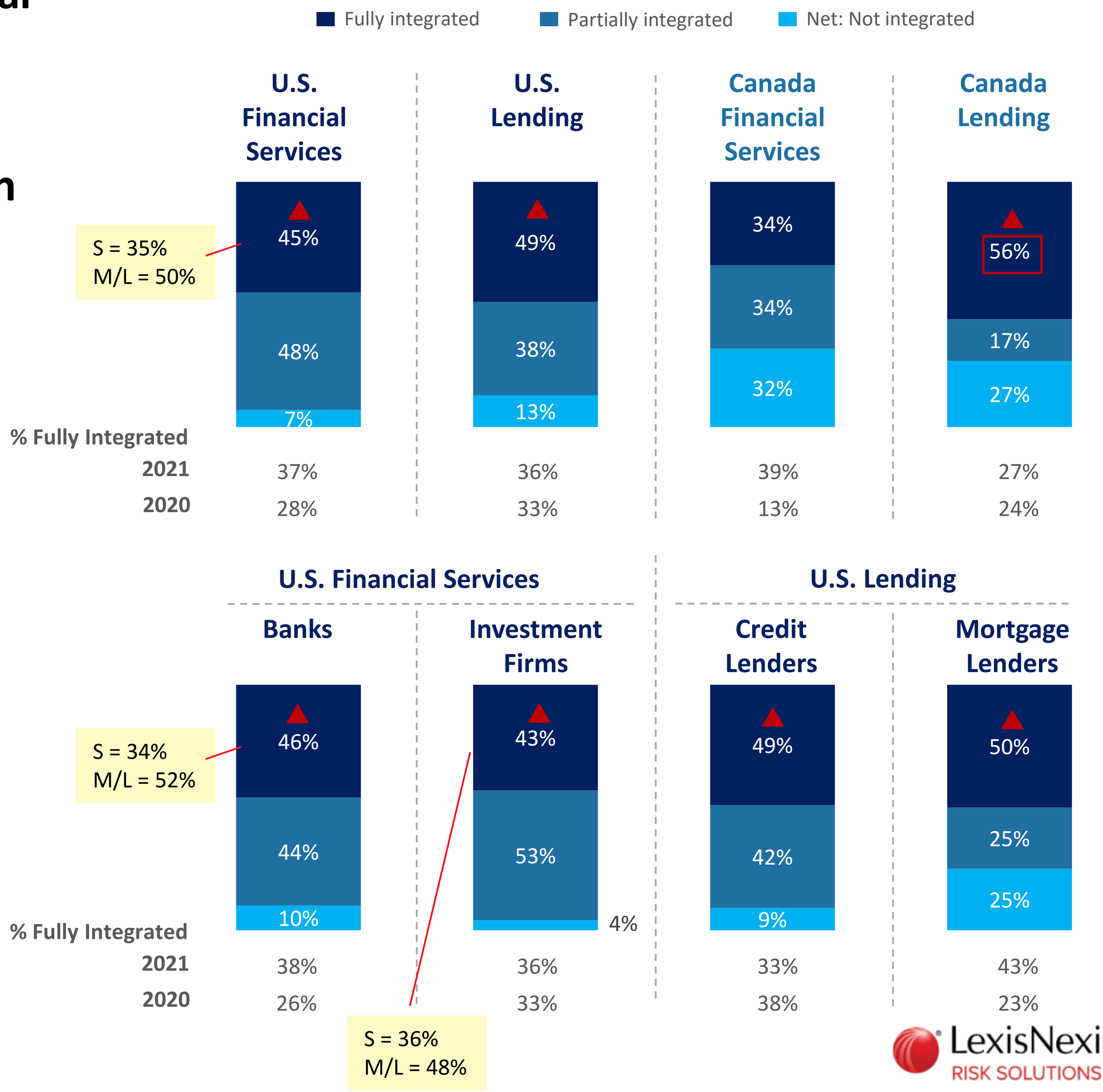
* Asked of those with online and/or mobile channel transactions

Key Finding 6

FRAUD DETECTION AND PREVENTION APPROACHES

Compared to 2021, more financial institutions have achieved full integration of cybersecurity operations with fraud prevention efforts.

Integration of Cybersecurity Operations w/ Fraud Prevention*



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

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

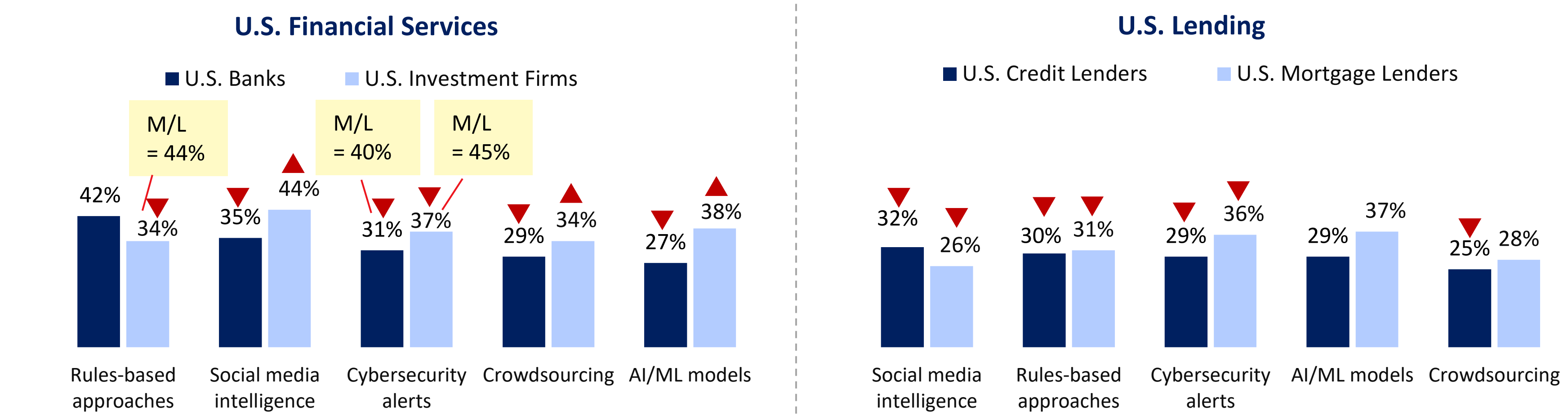
▼▲ = significantly or directionally higher/lower than previous period

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

U.S. financial institutions use a variety of supportive capabilities to fight fraud, with social media intelligence, crowdsourcing and AI/ML model use increasing among financial services firms.

Larger financial services firms are particularly likely to adopt rules-based approaches and cybersecurity alerts to tackle fraud.

% Using Supportive Capabilities to Fight Fraud



	Rules-based approaches		Social media intelligence		Cybersecurity alerts		Crowdsourcing		AI/ML models	
2021	48%	53%	42%	34%	59%	45%	38%	26%	42%	26%
2020	59%	56%	29%	38%	48%	55%	45%	50%	36%	34%

	Social media intelligence		Rules-based approaches		Cybersecurity alerts		AI/ML models		Crowdsourcing	
2021	48%	35%	48%	53%	42%	51%	26%	31%	37%	33%
2020	20%	11%	73%	75%	57%	44%	27%	13%	41%	53%

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

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

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

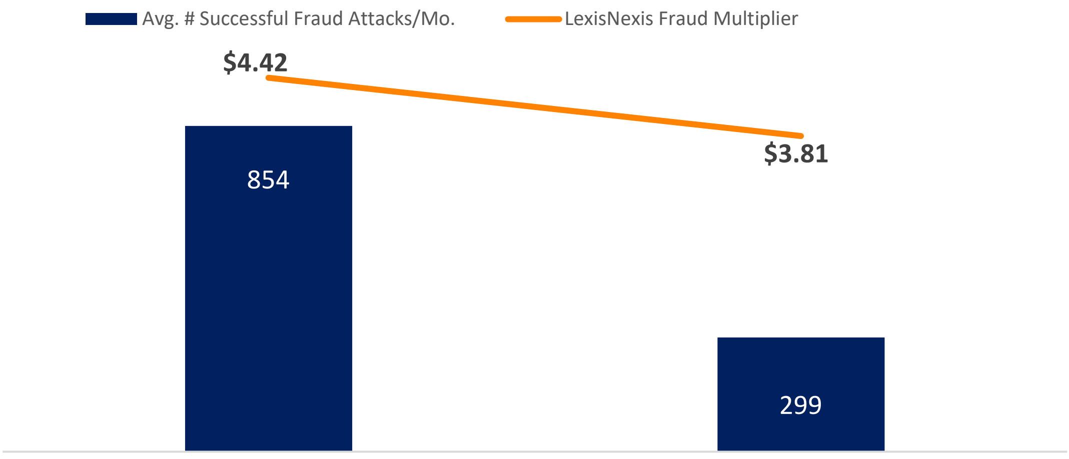
Cybersecurity alerts are notifications that specific attacks have been directed at an organization's information systems.
Rules-based approaches use codes to drive if-then actions (if information or activity = risk, then an action is taken or alert is provided).
Social media intelligence refers to the 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.

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

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

For example, U.S. financial services and lending firms which employ the smart practice solutions and integration approach* have a lower cost of fraud and level of successful fraud attacks.

Every $1 of fraud costs smart practice followers less ($3.81) than those firms which do not follow this approach ($4.42). Furthermore, there are nearly two-thirds less the amount of successful fraud attacks per month compared to those not using this approach.



	Not Using Smart Practice Approach	Fully Using Smart Practice 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., Email, 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	✓

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

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations

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

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

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

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

☑ Deploying technologies that are able to recognize legitimate customers, mitigate 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' logins from multiple devices, locations and channels is essential for identifying risks.

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

Recommendation #2

A MULTI-LAYERED SOLUTIONS APPROACH IS RECOMMENDED, CUSTOMIZED TO EACH PHASE OF THE CUSTOMER JOURNEY AND TRANSACTION CHANNEL

Overview

Key Findings

#1 Trends/Landscape

#2 Attacks & Costs

#3 Scams Impacting Customer Journey Risks

#4 BNPL Impact on Fraud Detection

#5 Identity-related Fraud

#6 Risk Mitigation Smart Practices

Recommendations

Account Creation → Account Login → Account Transaction

☑ Single point protection is inadequate 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.

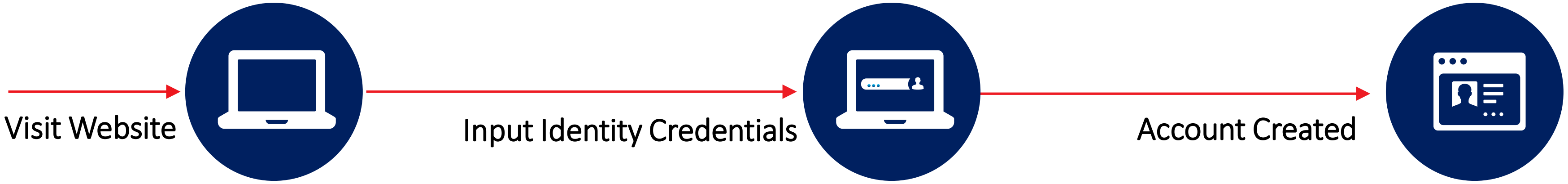
☑ We recommend adopting a multi-layered, strong authentication defense approach. This includes a single authentication decision platform that incorporates real-time event data, third-party signals and global, cross-channel intelligence.

Recommendation #3 Account Creation

MITIGATE 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 later stages. It is also the first point of contact for many legitimate customers; too much friction and they may abandon the effort.

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Scams Impacting Customer Journey Risks
#4 BNPL Impact on Fraud Detection
#5 Identity-related Fraud
#6 Risk Mitigation Smart Practices
Recommendations



Protect Entry Points

Implement strong customer identity and access management (CIAM) controls by starting with integrating cybersecurity and digital experience operations with fraud detection technology. This 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.

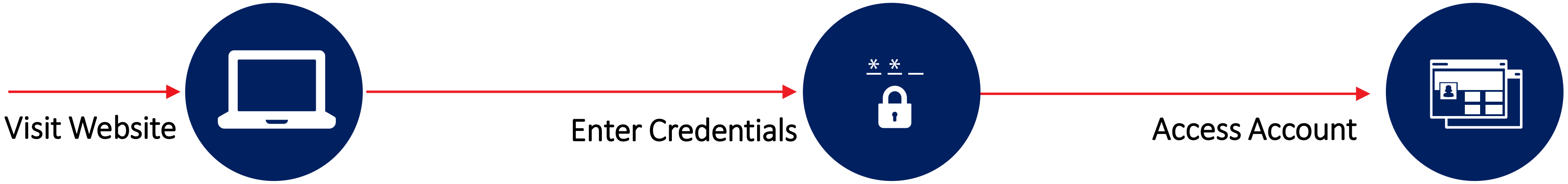
Continue to Manage Risk Across All Endpoints

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

Recommendation #4 **Account Login**

USE TECHNOLOGIES THAT RECOGNIZE YOUR CUSTOMERS, DETERMINE THEIR POINT OF ACCESS AND DISTINGUISH THEM FROM FRAUDSTERS AND MALICIOUS BOTS. LAYERED SOLUTIONS EMPOWER YOUR ORGANIZATION TO 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; this also provides a more secure means of identification that speeds the process with minimal friction. 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.


Visit Website → Enter Credentials → Access Account

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 distinguishing a 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; two-factor authentication (e.g., OTP).

Recommendation #5 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.

Overview

Key Findings

#1 Trends/Landscape

#2 Attacks & Costs

#3 Scams Impacting Customer Journey Risks

#4 BNPL Impact on Fraud Detection

#5 Identity-related Fraud

#6 Risk Mitigation Smart Practices

Recommendations

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; two- factor authentication.

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/corporations-and-non-profits/fraud-and-identity-management

📱 +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.

This document is for informational purposes only. LexisNexis Risk Solutions does not represent nor warrant that this document is complete or error free.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. True Cost of Fraud is a trademark of LexisNexis Risk Solutions Inc. LexisNexis Fraud Multiplier is a trademark of RELX Inc. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2022 LexisNexis Risk Solutions Group. All rights reserved. NXR15741-00-1022-EN-US

Glossary

Term	Definition
AI/ML models	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	Collection of information, opinions or work from a group of people, usually sourced via the internet
Cybersecurity alerts	Notifications that specific attacks have been directed at an organization’s information systems
Integrated	Various parts or aspects linked or coordinated (e.g. integrating digital/CX operations with fraud prevention)
Mid/Large (M/L)	Mid/large companies earning at least $10 million in annual revenues
Rules-based approaches	The use of codes to drive if-then actions (if information or activity is deemed a risk, then an action is taken or alert is provided)
Scams	Fraudulent or deceptive act or operation typically to make money; multiple scams in this report are referred to as facing three or more types of scams
Smart practice multi-layered solutions approach	Using some combination of passive/digital identity-based solutions and those which assess physical identity attributes and transaction risk
Social media intelligence	Collective tools and solutions that allow organizations to analyze conversations, respond to social signals and synthesize social data points into meaningful trends and analysis

APPENDIX

TOP ONLINE/MOBILE CHANNEL CHALLENGES ACROSS THE CUSTOMER JOURNEY

Identity verification and assessment of fraud risk by country are top online and mobile challenges for U.S. banks and investment firms at account opening and login stages. However, malicious bot transactions and balancing fraud prevention friction with the customer experience pose a greater challenge at the point of fund distribution.

U.S. Financial Services

	Account Opening		Account Login		Distribution of Funds	
	Banks ⚠	Investment Firms ⚠	Banks	Investment Firms	Banks	Investment Firms
Top Online Channel Challenges	• Assessing risk by country (33%) • **Verification** – Address (34%) – Phone (33%) – Email or device (42%)	• **Verification** – Address (34%) – Phone (43%) – Identity (38%)	• Assessing risk by country (31%) • **Verification** – Address (35%)	Manual reviews (36%) **Verification** – Address (38%) – Phone (31%) – Identity (30%)	• Balancing fraud prevention friction (38%) • Lack of specialized tools (35%) • New transaction methods (33%) • Manual reviews (32%) • Phone **verification** (31%)	• Malicious bot transactions (45%) • New transaction methods (35%) • Lack of specialized tools (30%) • Knowing origination source (30%)
Top Mobile Channel Challenges	• Assessing risk by country (30%) • **Verification** – Address (34%) – Phone (32%) – Email or device (41%)	• Assessing risk by country (30%) • **Verification** – Address (40%) – Phone (37%)	• Assessing risk by country (32%) • **Verification** – Address (34%) – Phone (30%) – Email or device (31%) – Identity (30%)	Knowing origination source (34%) Assessing risk by country (31%) **Verification** – Address (32%) – Phone (33%) – Identity (33%)	• Balancing fraud prevention friction (37%) • Assessing risk by country (32%) • New transaction methods (31%) • Manual reviews (30%)	• Balancing fraud prevention friction (36%) • Manual reviews (34%) • Lack of specialized tools (31%) • Malicious bot transactions (30%)

Survey Question:
Q20A/B: 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.

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

Key Finding 3

TOP ONLINE/MOBILE CHANNEL CHALLENGES ACROSS THE CUSTOMER JOURNEY

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Customer Journey Risks
#4 Smart Practices
Recommendations

U.S. lending firms differ from financial services firms in terms of challenges faced in the fund distribution stage. Specifically, determining origination source, the emergence of new transaction methods, manual reviews and the lack of specialized tools are the top challenges in that stage.

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 (42%) – Email or device (36%) – Identity (36%)	• Assessing risk by country (41%) • **Verification** – Address (38%) – Phone (46%) – Email or device (35%)	• Assessing risk by country (29%) • Address **verification** (33%)	• Assessing risk by country (38%) • Balancing fraud prevention friction (34%) • **Verification** – Address (47%) – Email or device (45%)	• Knowing origination source (35%) • New transaction methods (34%) • Balancing fraud prevention friction (31%) • Malicious bot transactions (30%)	• Lack of specialized tools (39%) • Manual reviews (38%) • Knowing origination source (37%) • **Verification** – Phone (39%) – Identity (38%)
Top Mobile Channel Challenges	• **Verification** – Address (32%) – Phone (32%) – Email or device (36%) – Identity (33%)	• **Verification** – Phone (48%) – Email or device (45%) – Identity (31%)	• Knowing origination source (36%) • **Verification** – Address (33%) – Identity (34%)	• Balancing fraud prevention friction (36%) • Assessing risk by country (38%) • **Verification** – Address (30%) – Email or device (38%)	• New transaction methods (38%) • Manual reviews (30%) • **Verification** – Address (32%) – Email or device (32%)	• New transaction methods (55%) • Manual reviews (37%) • Knowing origination source (35%) • Address **verification** (35%)

Survey Question:
Q20A/B: 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.

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

TOP ONLINE/MOBILE CHANNEL CHALLENGES ACROSS THE CUSTOMER JOURNEY

Overview
Key Findings
#1 Trends/Landscape
#2 Attacks & Costs
#3 Customer Journey Risks
#4 Smart Practices
Recommendations

Identity verification, assessment of fraud risk by country, malicious bot transactions, the lack of specialized tools and balancing fraud prevention friction with the customer experience are top online and mobile challenges for Canadian financial institutions.

Canadian Financial Services & Lending

Account Opening

Account Login

Distribution of Funds

	Account Opening: Financial Services ⚠	Account Opening: Lending ⚠	Account Login: Financial Services	Account Login: Lending	Distribution of Funds: Financial Services	Distribution of Funds: Lending
Top Online Channel Challenges	• **Verification** – Address (52%) – Email or device (33%) – Identity (36%)	• Assessing risk by country (37%) • **Verification** – Address (42%) – Phone (43%) – Email or device (30%) – Identity (36%)	• Malicious bot transactions (36%) • Knowing origination source (34%) • **Verification** – Address (34%) – Identity (39%)	• Lack of specialized tools (30%) • **Verification** – Address (36%) – Phone (39%) – Email or device (37%) – Identity (43%)	• Knowing origination source (32%) • Malicious bot transactions (31%) • **Verification** – Email or device (34%) – Identity (49%)	• Balancing fraud prevention friction (45%) • Malicious bot transactions (44%) • Knowing origination source (35%) • Manual reviews (32%) • Identity **verification** (30%)
Top Mobile Channel Challenges	• Assessing risk by country (33%) • Manual reviews (31%) • **Verification** – Address (31%) – Phone (39%)	• Malicious bot transactions (34%) • Manual reviews (31%) • **Verification** – Address (46%) – Phone (36%) – Email or device (48%)	• Assessing risk by country (44%) • Malicious bot transactions (30%) • Balancing fraud prevention friction (30%) • **Verification** – Email or device (37%) – Identity (37%)	• Balancing fraud prevention friction (41%) • **Verification** – Address (52%) – Phone (40%)	• Malicious bot transactions (43%) • Knowing origination source (36%) • New transaction methods (31%) • Phone **verification** (30%)	• Lack of specialized tools (37%) • New transaction methods (30%) • **Verification** – Phone (38%) – Identity (39%)

Survey Question:
Q20A/B: 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.

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