7th Annual LexisNexis® True Cost of Fraud™ Study: Financial Services and Lending Report

U.S. and Canada Edition 2023

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

The study included a survey of 346 risk and fraud executives in financial services and lending companies in the U.S. (272) and Canada (74).

LEXISNEXIS® TRUE COST OF FRAUD™ STUDY				
Total	Company Type		Size	
# of Completions	Financial Services	Credit & Lending	Small (<$10M)	Mid/Large ($10M+)
346	174	172	103	243

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 (S)
Earns less than $10 million in annual revenues

Mid/Large (M/L)
Earns at least $10 million in annual revenues

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 app or “bill to mobile phone”

The LexisNexis® True Cost of Fraud™ study helps companies grow their business more 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 July and August 2023 as part of a larger commissioned global study conducted by Forrester® Consulting
- 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:

- It does not include insider fraud or employee fraud

The LexisNexis Fraud Multiplier™ variable:

- 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.

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

New Account Opening

On-boarding a new customer

Establishing a new account

Verifying new identity credentials

Account Login

Accessing an account

Verifying identity before allowing access to the account

Distribution of Funds

Disbursing funds from a bank or investment account

Disbursing funds for a loan

Verifying identity before distribution of funds

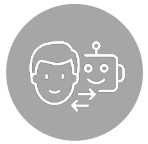
Summary of Key Findings

Trends

Physical branches generate the most revenue of any single channel, though two-thirds of revenue comes through remote channels. Traditional transaction methods, such as cash, checks and gifts cards, rebound. Digital wallets and payment apps hold ground while crypto softens. Credit and debit transactions combined continue to represent the majority of transaction volume, especially at U.S. Banks. U.S. firms report needing to allocate more resources toward fraud management while Canadian firms report greater impact due to direct revenue losses.

Attacks

Nearly two-thirds (63%) of financial firms report overall fraud increasing at least 6% in the prior 12 months. Canadian firms were nearly twice as likely as U.S. counterparts to report an overall increase of 21% or more. Synthetic Identity Fraud afflicts the entire Customer Journey, causing the greatest impact at distribution of funds for U.S. firms and Canadian financial services. Scams stand out for U.S. financial services at that customer journey stage, but rank highly for other groups at new account creation.



Challenges

Challenges discerning legitimate humans from malicious bot transactions, and the emergence of new/varied transaction methods, complicate the mandate to provide customers with a positive experience across touchpoints. Widespread expectations for increased budgets align with progress in conveying the commercial impact of fraud prevention to the business overall.

Summary of Key Findings (cont.)

Scams

Scams are still a major contributor to fraud losses, despite efforts to educate consumers. Over half of financial institutions report scams increasing 6% or more, with 21% of firms reporting at least a 21% increase. About 35% of fraud losses in the region are now attributed to scams. Almost half (48%) of financial institutions report undertaking efforts to educate customers about how to protect themselves. Over 40% have nudged customers to take actions with personalized or contextual recommendations.

Losses

The LexisNexis® Fraud Multiplier™ variable rose for all financial services segments, more so in Canada than in the U.S. - For every $1 of fraud loss, it costs Canadian firms $1 more compared to last year: $4.45 in 2023 versus $3.49 in 2022, a 28% increase on average. U.S. investment firms and credit lenders reported a 9% increase year-over-year, noticeably higher than U.S. banks and mortgage lenders. Fraud losses in the phone channel spike across the industry, in line with widespread increases in scam attacks and losses due to scams.

Risk Mitigation Smart Practices

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. Organizations who build a more robust posture against fraud throughout customer journey stages report 41% lower fraud losses compared to the least mature organizations.

Summary of Recommendations

1. Respond faster to emerging fraud trends and rising consumer expectations by taking a dynamic, agile and simplified approach to risk assessment. Promote safe and convenient interactions and transactions across the customer journey via capabilities integrated into risk-based workflows, and supported by deep troves of identity intelligence and robust linking technology.

2. Consolidate vendors where possible to reduce complexity, message latency and costs, and increase the effectiveness of custom solutions and responsiveness to changing risks.

3. Risk-based workflows respond effectively to the risk level of the present interaction or transaction, correctly blocking fraudulent actions while promoting positive experiences for legitimate consumers.

4. Call an appropriate combination of risk-assessment capabilities for the present interaction or transaction, customer journey stage, channel and risk-level, by leveraging multiple interoperable capabilities on a unifying platform for rapid identity verification, user authentication and transaction scoring.

5. Detect the risk level of the present interaction or transaction via signal from diverse sources of intelligence, including device, behavior, email, phone and physical consumer data, and assess the signal with insights from thousands of public record and proprietary sources, industry peers (“crowd sourcing”) and user-device behavior.

Key Finding 1

Increased digitalization affords fraudsters more opportunities to exploit both consumer identities and accounts. However, strong in-branch transaction volume and value, and prioritization of customer experience, indicate the need for robust omnichannel fraud prevention capabilities.

Although approximately two-thirds of revenue comes through remote channels, physical branches generate the most revenue of any channel.

Use of traditional transaction methods, such as cash, checks and gifts cards, rebounded, doubling for U.S. firms and more than tripling in Canada. The increase reinforces the importance of omnichannel identity verification and fraud risk assessment strategies.

Among business functions impacted by fraud, customer experience tops the list of concerns for most financial firms, though slightly less so for U.S. financial services. Widespread difficulty establishing trust with customers and concerns over customer churn point to potential long-term challenges.

Key Finding 1

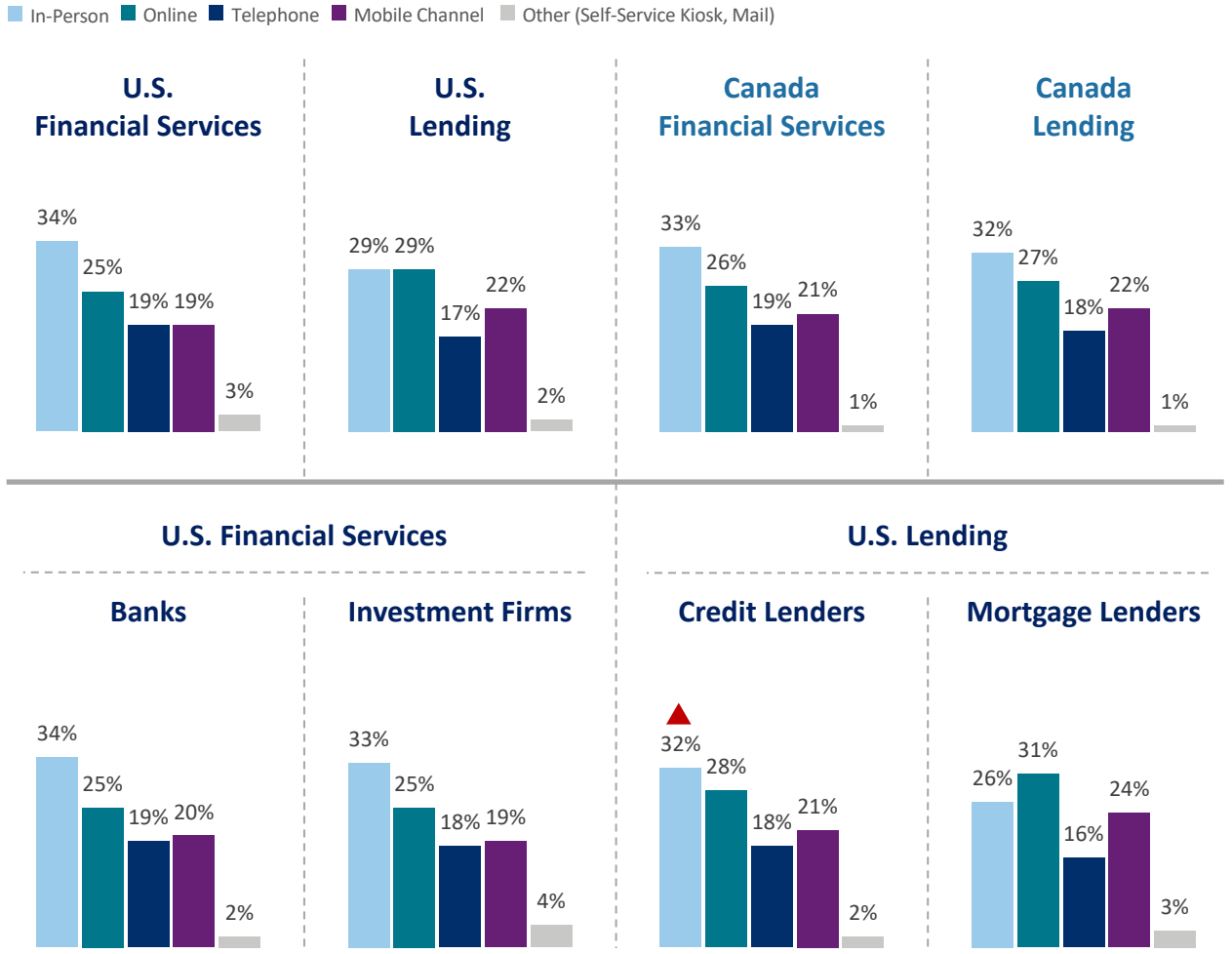
IN-PERSON REVENUE INCREASES

Revenue through physical branches outpaces each alternative channel in isolation, except for U.S. mortgage lenders.

Approximately two-thirds of revenue comes through remote channels.

Survey Question
Q6. Using your best estimate, how does your company's total **annual revenue** during the past 12 months break out for each of the following channels?

% of Revenue Attributed to Channel

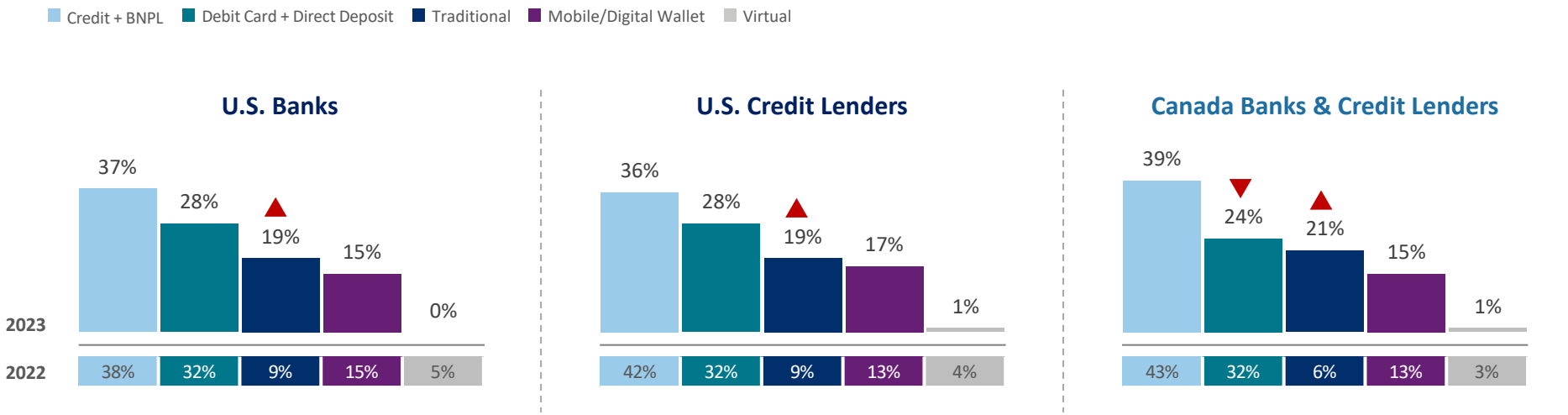


▲ = U.S Credit Lenders reported more revenue through in-branch than U.S. Mortgage Lenders

Traditional transaction methods, such as cash, checks and gifts cards, rebound. Digital wallets and payment apps hold ground while virtual methods decline.

Credit and debit transactions, combined, continue to represent the majority of transaction volume, especially at U.S. Banks. The increase in traditional transaction methods reinforces the importance of omnichannel identity verification and fraud risk assessment strategies.

% Transaction Volume by Method



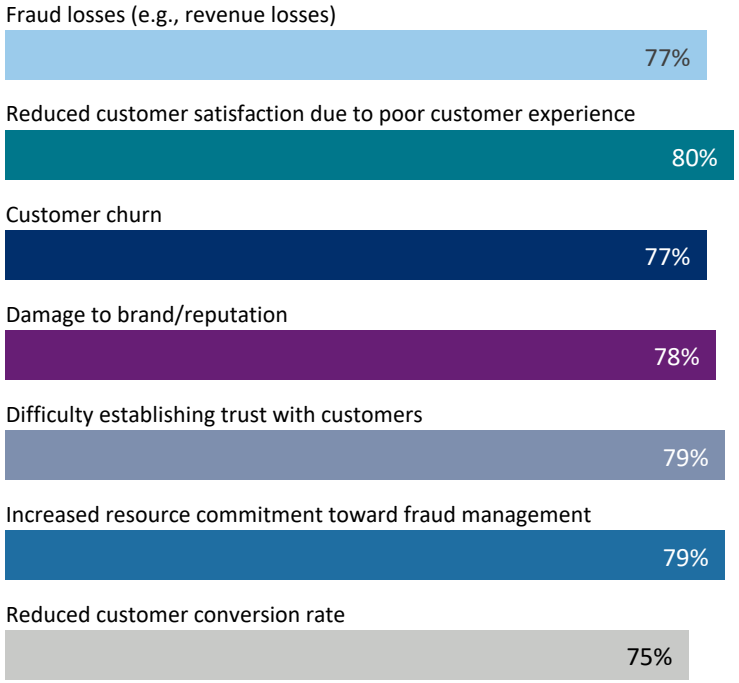
Survey Question
Q7. Using your best estimate, please indicate the percentage for each method your organization used during the past 12 months to fund transactions or disburse funds.

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

Customer experience tops the list of concerns for most financial firms, though slightly less so for U.S. financial services.* Widespread difficulty establishing trust with customers and concerns over customer churn could pose long-term challenges.

U.S. firms report needing to allocate more resources toward fraud management while Canadian firms report greater impact due to direct revenue losses.

Moderate and Significant Impact of Fraud**



Survey Question
Q3. To what extent has fraud impacted the following areas of your business?

MOST SIGNIFICANT IMPACTS

U.S. Financial Services

83%

Increased resource commitment toward fraud management

U.S. Lending

85%

Increased resource commitment toward fraud management

Canada Financial Services

92%

Fraud losses (e.g., revenue losses)

Canada Lending

81%

Fraud losses (e.g., revenue losses)

81%

Reduced customer satisfaction due to poor customer experience

** Percentages are the sum of those who responded either "moderate impact" or "significant impact."

* Nearly all (95%) of U.S. financial institutions cite improved customer experience as an "important" or "very important" priority in a commissioned study conducted by Forrester Consulting on behalf of LexisNexis Risk Solutions, (Defend Against Authorized Transfer Scams) January 2024.

Key Finding 2

Thousands of fraudulent transaction attempts flood into financial institutions every month. More identity-related fraud occurs at account logins, especially via synthetic identity fraud for U.S. financial services and Canadian firms. Scams challenge all industry segments at all customer journey stages, especially for financial services firms.

Nearly two-thirds (63%) of financial firms report overall fraud increasing at least 6% in the prior 12 months. Canadian firms were nearly twice as likely as U.S. counterparts to report an overall increase of 21% or more.

Scams stand out as a top fraud vector for US banks at the point of distribution of funds, while ranking highly for other groups at new account creation. Friendly fraud consistently ranks as a top challenge across the customer journey.

Account logins overtake new account creation as the stage of the customer journey with the most identity-related fraud, except for US Lenders for whom distribution of funds is more problematic.

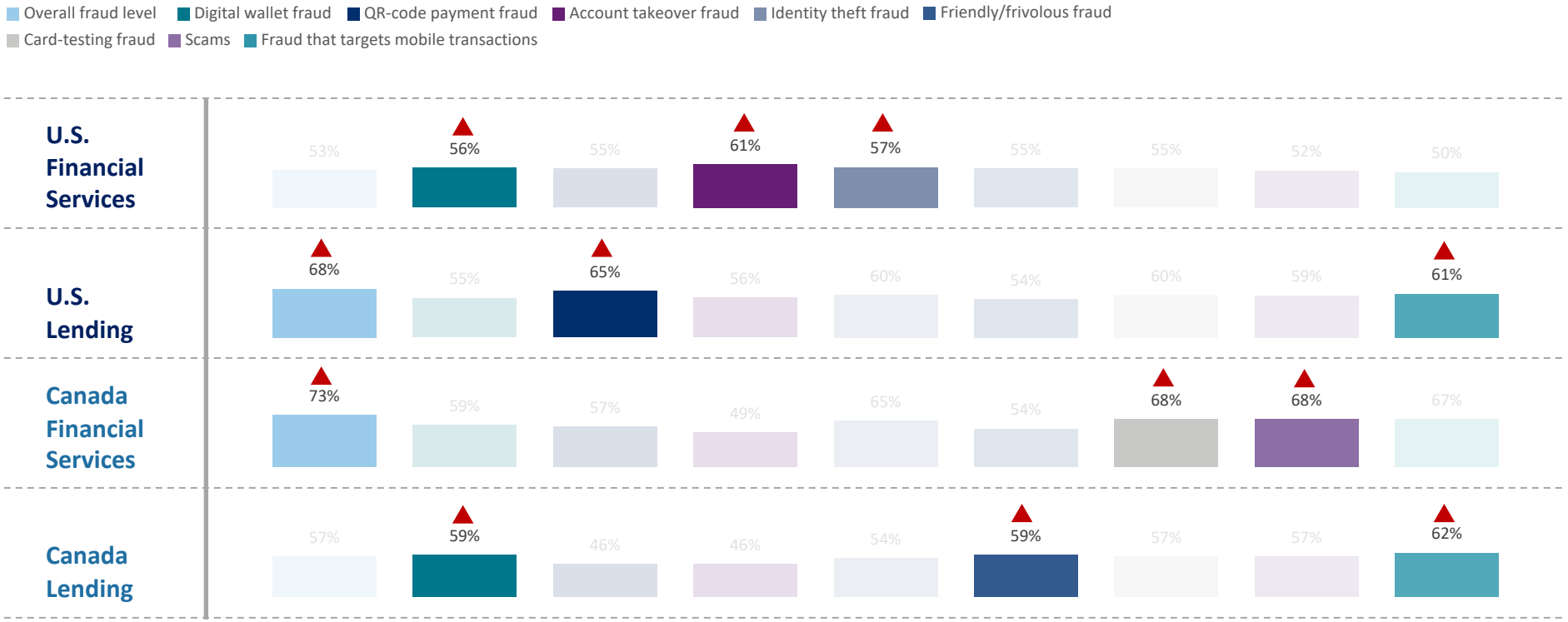
The average number of successful fraudulent transactions per month grew across the industry. This is driven by larger firms, as in 2022.

Identity theft and digital payment fraud are growing fast.

Nearly two-thirds (63%) of financial firms report overall fraud increasing at least 6% in the prior 12 months. Canadian firms were nearly twice as likely as U.S. counterparts to report an overall increase of 21% or more. Overall fraud increased the least for U.S. Financial Services.

Three threats increased faster than others: fraud targeting mobile transactions (particularly for lenders), identity theft and scams.

Fastest growing fraud types



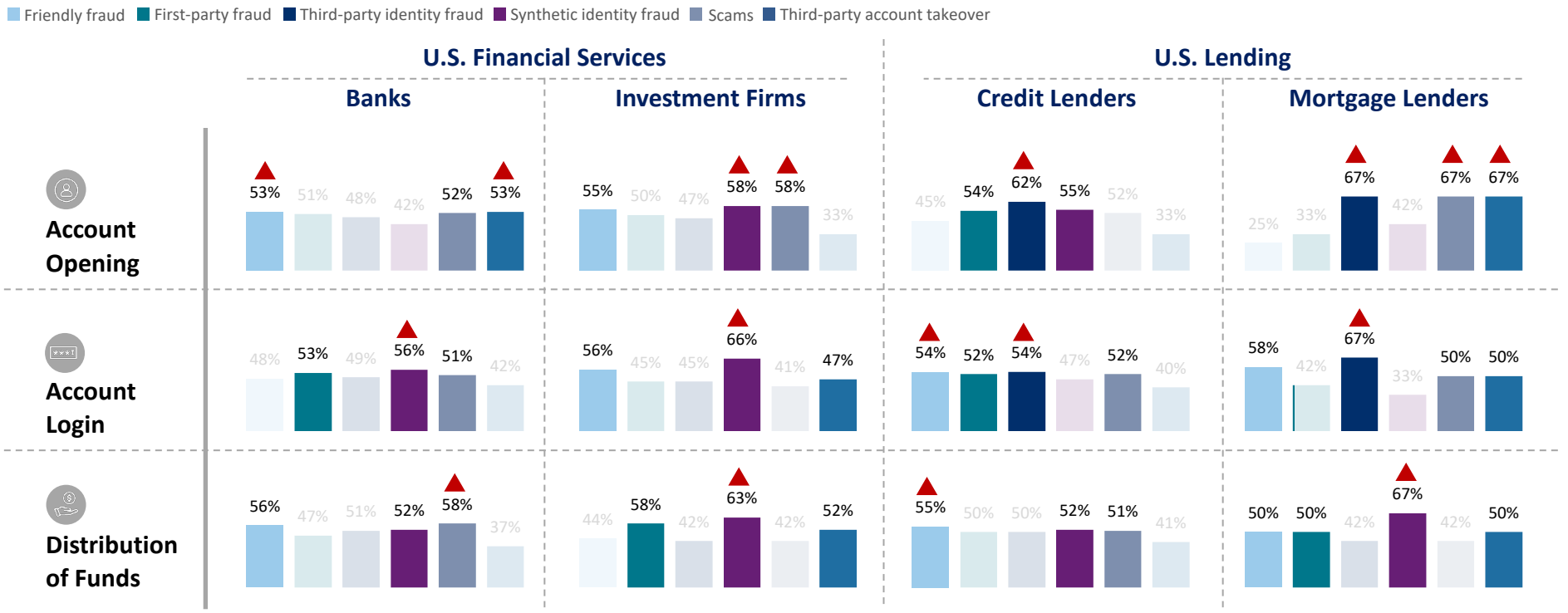
Survey Question
Q2. In the past 12 months, has your company detected less, more, or an equal amount of the following types of online fraud compared to the previous year?

▼▲ = significantly or directionally higher/lower than other fraud types within the industry segment

Synthetic identity fraud afflicts the entire customer journey, causing the greatest impact at distribution of funds for U.S. firms.

Scams stand out for U.S. financial services at distribution of funds, but rank highly for other groups at new account creation. Concurrently, friendly fraud consistently ranks as a top challenge across the customer journey.

% Distribution of Fraud Losses by Fraud Type



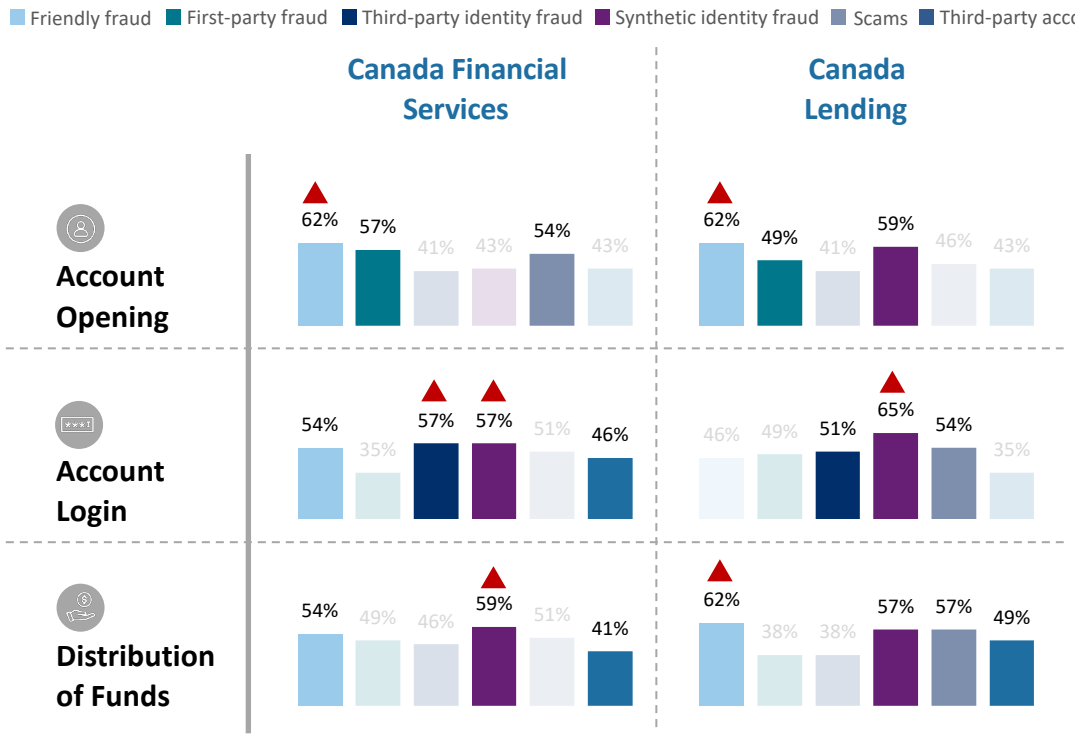
Survey Question
Q8. Think about these three customer-journey phases separately and your organization's fraud losses. During the past 12 months, what are the top three types of fraud you have seen in each specific customer-journey stage?

▲ = top-most costly fraud type(s) by industry segment by customer journey stage

Synthetic identity fraud afflicts the entire customer journey, causing the greatest impact at account login for Canadian firms.

Friendly fraud impacts Canadian firms, financial services more than lending. Concurrently, scams consistently ranks as a top challenge across the customer journey.

% Distribution of Fraud Losses by Fraud Type



Survey Question
Q8. Think about these three customer-journey phases separately and your organization's fraud losses. During the past 12 months, what are the top three types of fraud you have seen in each specific customer-journey stage?

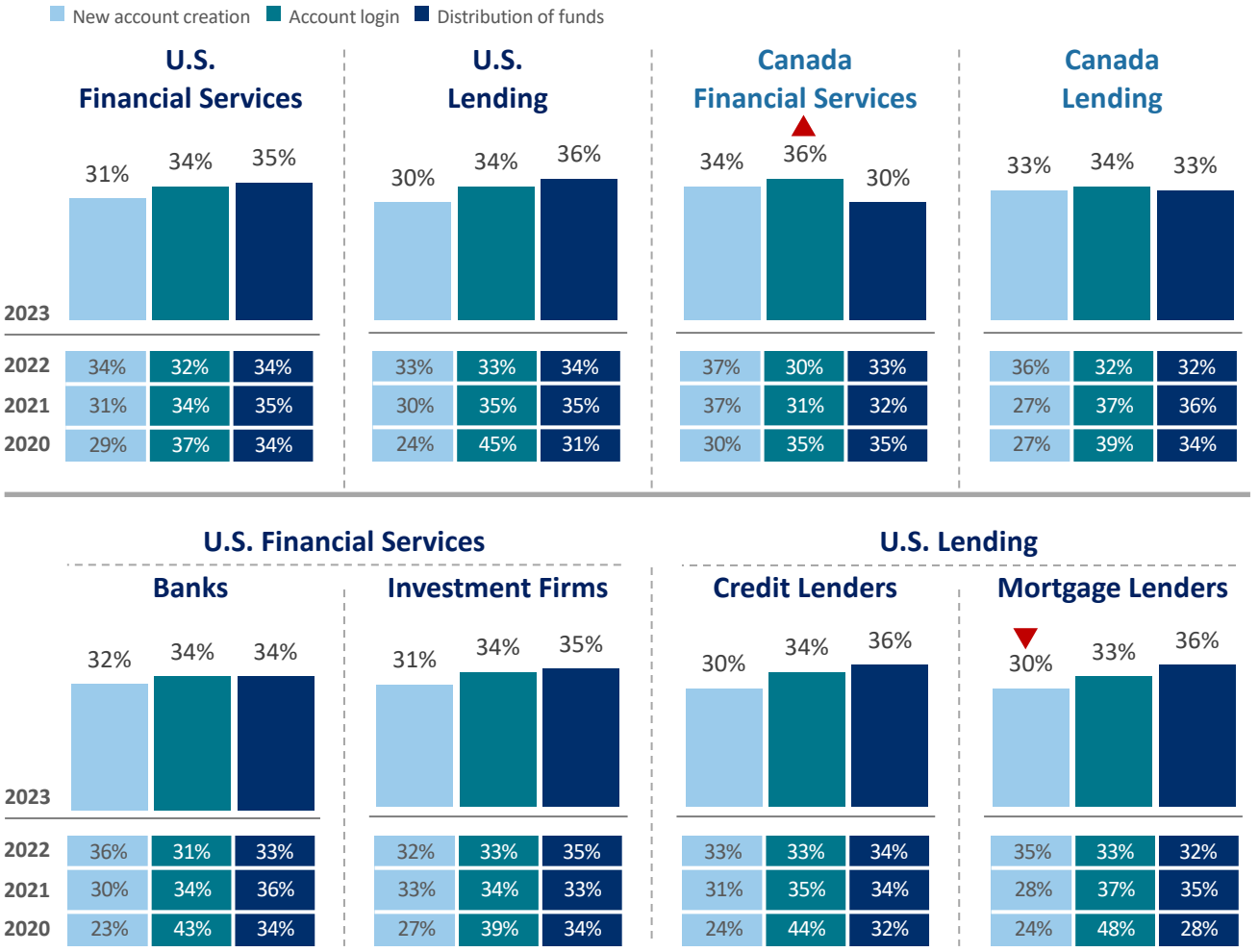
▲ = top-most costly fraud type(s) by industry segment by customer journey stage

Account logins overtake new account creation as the stage of the customer journey with the most identity-related fraud, except for U.S. Lenders for whom distribution of funds is more problematic.

The growth in share of account logins coincides with the rise of synthetic identity fraud and third-party identity fraud at that customer journey stage.*

Survey Question
Q9. For identity-related fraud, what is the distribution by the following types of activities?

Identity-Related Fraud: % Distribution by Activity



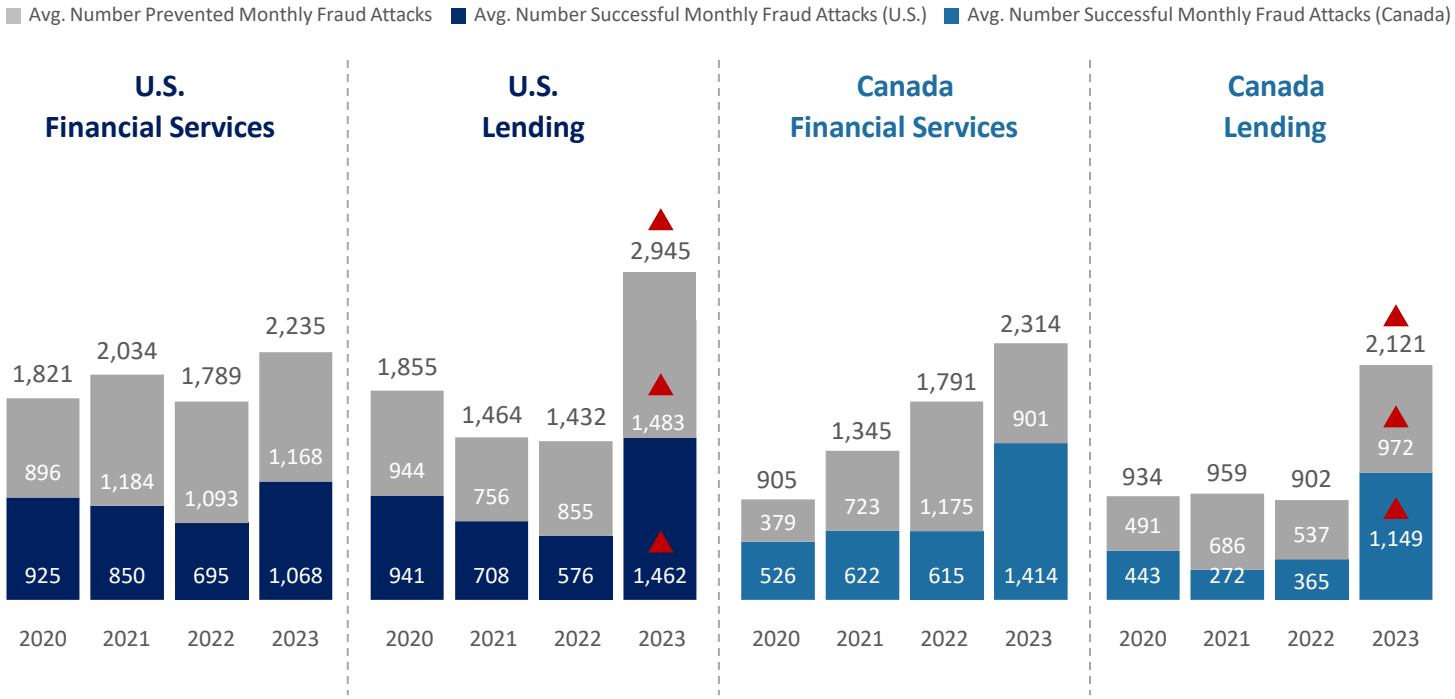
▼▲ = significantly or directionally higher/lower than previous period

* See results from survey question 8, above.

The average number of successful fraudulent transactions per month grew across the industry, with lending firms reporting the greatest increases.

This is driven by larger firms, as in 2022.

Average Monthly Fraudulent Transactions



Mid/Large Segment Highlights

U.S. Financial Services (Overall 2,345)
- Prevented Attacks: 1,253
- Successful Attacks: 1,091

U.S. Lending (Overall 3,489)
- Prevented Attacks: 1,691
- Successful Attacks: 1,798

Canadian Financial Services & Lending (Overall 2,433)
- Prevented Attacks: 1,021
- Successful Attacks: 1,413

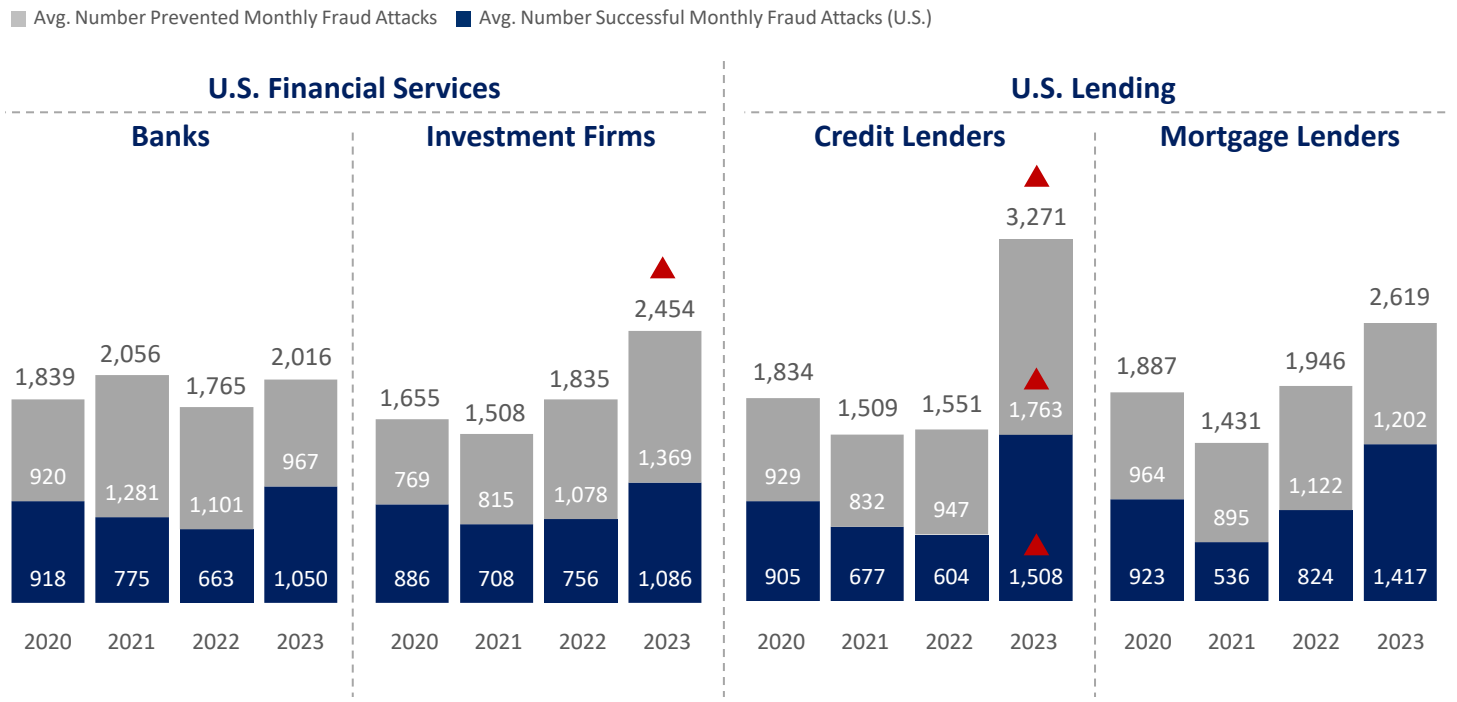
Survey Questions
Q14: In a typical month, approximately how many fraudulent transactions does your company prevent? Q16: In a typical month, approximately how many fraudulent transactions are successfully completed (i.e. not prevented) at your company?

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

Successful fraudulent transactions continue to rise, particularly for U.S. credit lenders.

Across segments, mid/large firms experience a higher volume of fraudulent transactions per month, with U.S. credit lenders reporting the most pronounced increase.

Average Monthly Fraudulent Transactions



Mid/Large Segment Highlights

U.S. Banks (Overall 2,157)
- Prevented Attacks: 1,022
- Successful Attacks: 1,135

U.S. Investment (Overall 2,532)
- Prevented Attacks: 1,485
- Successful Attacks: 1,048

U.S. Credit (Overall 4,011)
- Prevented Attacks: 2,077
- Successful Attacks: 1,934

U.S. Mortgage (Overall 2,968)
- Prevented Attacks: 1,305
- Successful Attacks: 1,663

Survey Questions
Q14: In a typical month, approximately how many fraudulent transactions does your company prevent? Q16: In a typical month, approximately how many fraudulent transactions are successfully completed (i.e. not prevented) at your company?

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

Key Finding 3

Financial institutions continue racing to keep ahead of evolving threats and scams while balancing customer experience. Notable increases in online and mobile challenges across the customer journey, especially at new account creation, add urgency to instill greater robustness and flexibility into fraud detection and mitigation plans.

Financial organizations report struggles with evolving threats and payment methods, and balancing fraud prevention with customer experience. The top challenge for financial services firms was staying current and defending against new, more sophisticated payment frauds. Lenders most often ranked the inability to manage/prevent fraud for new transaction methods.

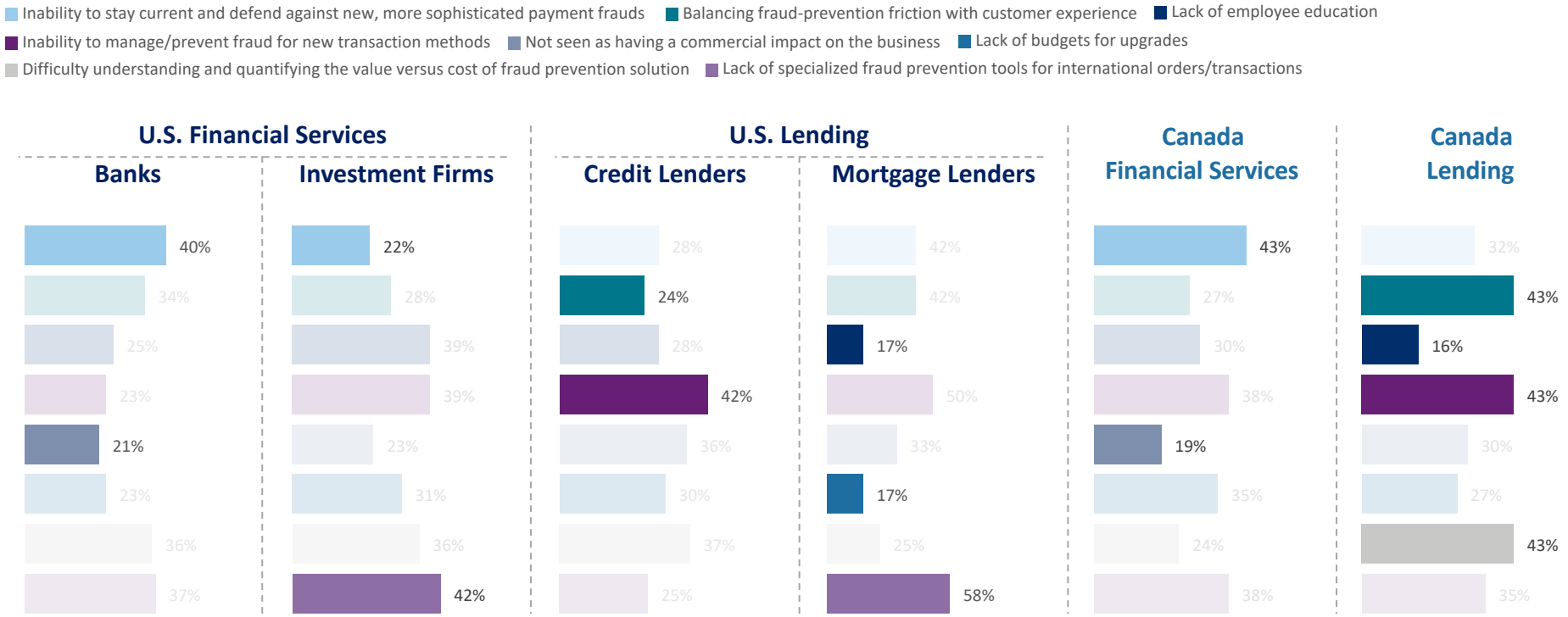
U.S. firms recognize the opportunity to balance customer experience with precautionary measures via improved digital identity verification across online and mobile channels. Malicious bot transactions and the emergence of new/varied transaction methods complicate the mandate to provide customers with a positive experience across touchpoints.

The most widespread efforts to mitigate and prevent scams focus on education, either directly to consumers about their security, or to employees about customer security and privacy. Third-party data and insights are also commonly applied to scam detection and mitigation. Scams put financial institutions in a difficult position.

Fraud teams generally feel supported to meet evolving challenges.

Financial organizations report struggles with evolving threats and payment methods, and balancing fraud prevention with customer experience. The top challenge for financial services firms was staying current and defending against new, more sophisticated payment frauds. Lenders most often ranked the inability to manage/prevent fraud for new transaction methods. Widespread expectations for increased budgets align with confidence in conveying the commercial impact of fraud prevention to the business overall.

Fraud Prevention Challenges



Survey Question
Q20: How challenging have these fraud prevention challenges been for your team over the past 12 months?

U.S. firms recognize opportunity to balance customer experience with precautionary measures via improved digital identity verification across online and mobile channels.

Challenges discerning legitimate humans from malicious bot transactions, and the emergence of new/varied transaction methods, complicate the imperative to provide customers with a positive experience across touchpoints.

Top Online/Mobile Challenges: Notable Increases Since 2022

2022 2023

	New Account Creation		Account Login		Distribution of Funds	
	Online	**Mobile**	**Online**	**Mobile**	**Online**	**Mobile**
U.S. Banks	**Manual reviews** (16% -> 30%) ▲ **Balancing fraud-prevention friction** (18% -> 26%)	**New transaction methods** (18% -> 25%) **Balancing fraud-prevention friction** (23% -> 31%)	**New transaction methods** (18% -> 33%) ▲ **Verification** – Identity (26% -> 33%)	**New transaction methods** (24% -> 28%) **Balancing fraud-prevention friction** (17% -> 23%)	**Verification** – Address (17% -> 29%) **Malicious bot transactions** (23% -> 36%)	**Verification** – Address (22% -> 32%) **Verification** – Email or Device (23% -> 32%)
U.S. Investment Firms	**Malicious bot transactions** (22% -> 36%) **Balancing fraud-prevention friction** (14% -> 20%)	**Lack of specialized tools** (16% -> 38%) ▲ **Balancing fraud-prevention friction** (22% -> 28%)	**New transaction methods** (23% -> 33%) **Malicious bot transactions** (17% -> 33%) ▲	**Malicious bot transactions** (22% -> 38%) ▲ **Balancing fraud-prevention friction** (21% -> 34%)	**Verification** – Address (21% -> 25%) **Verification** – Email or Device (23% -> 28%)	**Verification** – Address (18% -> 25%) **Verification** – Email or Device (20% -> 26%)
U.S. Credit Lenders	**Knowing origination source** (15% -> 31%) ▲ **Balancing fraud-prevention friction** (20% -> 35%) ▲	**Lack of specialized tools** (19% -> 25%) **Malicious bot transactions** (19% -> 33%)	**Lack of specialized tools** (25% -> 37%) **Verification** – Identity (25% -> 33%)	**Verification** – Phone (26% -> 33%) **New transaction methods** (20% -> 27%)	**Verification** – Address (23% -> 29%) **Verification** – Identity (24% -> 33%)	**Knowing origination source** (22% -> 29%) **Balancing fraud-prevention friction** (21% -> 33%)
U.S. Mortgage Firms	**New transaction methods** (16% -> 42%) **Balancing fraud-prevention friction** (12% -> 33%)	**Knowing origination source** (15% -> 42%) ▲ **New transaction methods** (4% -> 42%) ▲	**New transaction methods** (20% -> 50%) **Malicious bot transactions** (21% -> 42%)	**Manual reviews** (15% -> 25%) **Malicious bot transactions** (22% -> 58%)	**Verification** – Address (11% -> 25%) **Verification** – Email or Device (9% -> 25%)	**Lack of specialized tools** (15% -> 33%) **Malicious bot transactions** (15% -> 33%)

Survey Question
Q21/22. Please rank the top three challenges for each customer journey stage related to fraud your company faces when serving customers using the ONLINE/MOBILE channel.

▲ = most notable increase per industry segment

Canadian firms cite challenges with the emergence of new/varied transaction methods at new account creation, assessment of fraud risk by country or region, the lack of specialized fraud prevention tools for international transactions, and the imperative to balance fraud-prevention friction with positive customer experience.

Top Online/Mobile Challenges: Notable Increases Since 2022

2022 2023

	New Account Creation		Account Login		Distribution of Funds	
	Online	**Mobile**	**Online**	**Mobile**	**Online**	**Mobile**
Canada Financial Services	**New transaction methods** (19% -> 32%) **Malicious bot transactions** (14% -> 41%) ▲	**New transaction methods** (27% -> 30%) **Lack of specialized tools** (11% -> 30%) ▲	**Verification** – Email or Device (26% -> 38%) **Manual reviews** (17% -> 24%)	**Verification** – Phone (14% -> 35%) **Lack of specialized tools** (17% -> 41%)	**Assessing risk by country** (23% -> 38%) **New transaction methods** (21% -> 30%)	**Assessing risk by country** (13% -> 22%) **Balancing fraud-prevention friction** (22% -> 35%)
Canada Lending	**New transaction methods** (16% -> 30%) **Manual reviews** (11% -> 30%)	**Assessing risk by country** (11% -> 30%) **Balancing fraud-prevention friction** (15% -> 35%)	**Assessing risk by country** (22% -> 35%) **Malicious bot transactions** (8% -> 22%)	**Assessing risk by country** (26% -> 38%) **Manual reviews** (5% -> 24%) ▲	**Verification** – Email or Device (13% -> 35%) **Lack of specialized tools** (23% -> 35%)	**Knowing origination source** (8% -> 24%) ▲ **Balancing fraud-prevention friction** (12% -> 27%)

Survey Question
Q21/22. Please rank the top three challenges for each customer journey stage related to fraud your company faces when serving customers using the ONLINE/MOBILE channel.

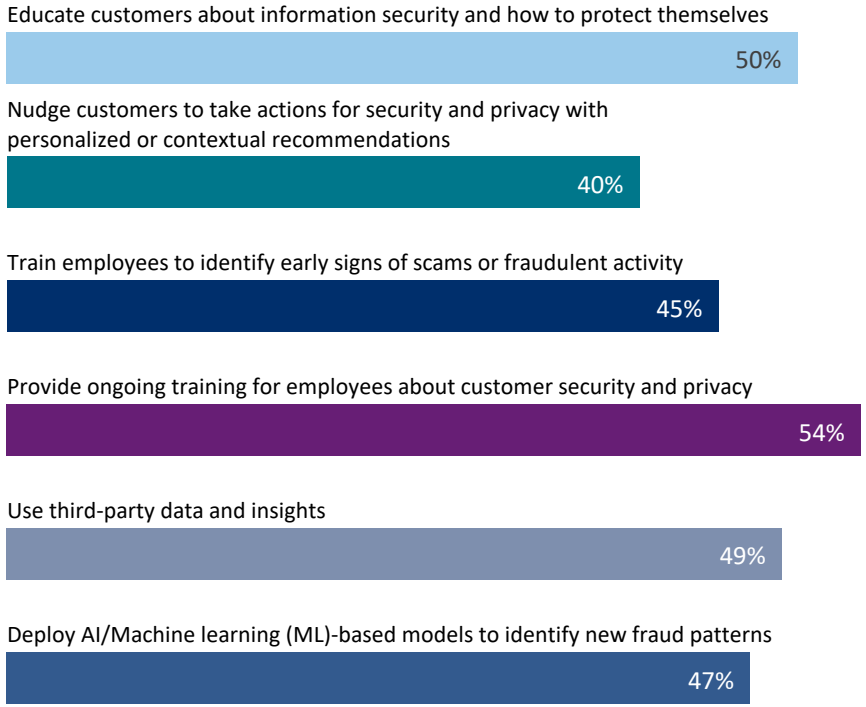
▲ = most notable increase per industry segment

Survey Question
Q27. What steps has your organization taken to mitigate and prevent scams?

Efforts to mitigate and prevent scams include education and technology adoption.

Education, either for consumers about their security or for employees about customer security and privacy, were the most widespread efforts to mitigate and prevent scams, with third-party data and insights also popular. U.S. banks and credit lenders, and Canadian financial services organizations stand out for more frequently sending personalized or contextual recommendations to consumers to take actions for security and privacy.

Distribution of Anti-Scam Initiatives



MOST COMMON INITIATIVE PER SEGMENT

U.S. Financial Services

Banks
55%
Educate customers about information security and how to protect themselves

Investment Firms
53%
(Tie)
Ongoing Employee Training
Use third-party data and insights

U.S. Lending

Credit Lenders
61%
Use third-party data and insights

Mortgage Lenders
50%
(Three-way tie)
Educate Customers
Ongoing Employee Training
Deploy AI/ML models

Canada Financial Services
57%
Educate customers about information security and how to protect themselves

Canada Lending
62%
Provide ongoing training for employees about customer security and privacy

Key Finding 4

Every dollar of direct fraud loss costs financial institutions more than at the time of last year's study. Over one-third (35%) of fraud losses in the region are now attributed to scams, which are increasing in frequency also. Across the region, fraud losses spiked in the phone channel, the channel most frequently used by fraudsters to target consumers in the U.S. for authorized transfer scams.* Firms are succeeding at defending account logins and distribution of funds, but fraudsters are finding new ways of attack at account creation.

International fraud spiked for U.S. firms. The increase aligns with widespread challenges assessing fraud risk by country or region, and a lack of specialized fraud prevention tools for international transactions.

Scams are a major contributor to fraud losses, despite efforts to educate consumers. Although 48% of financial institutions say they have undertaken efforts to educate customers, roughly 6 in 10 financial institutions report an increase in scams over the last year.

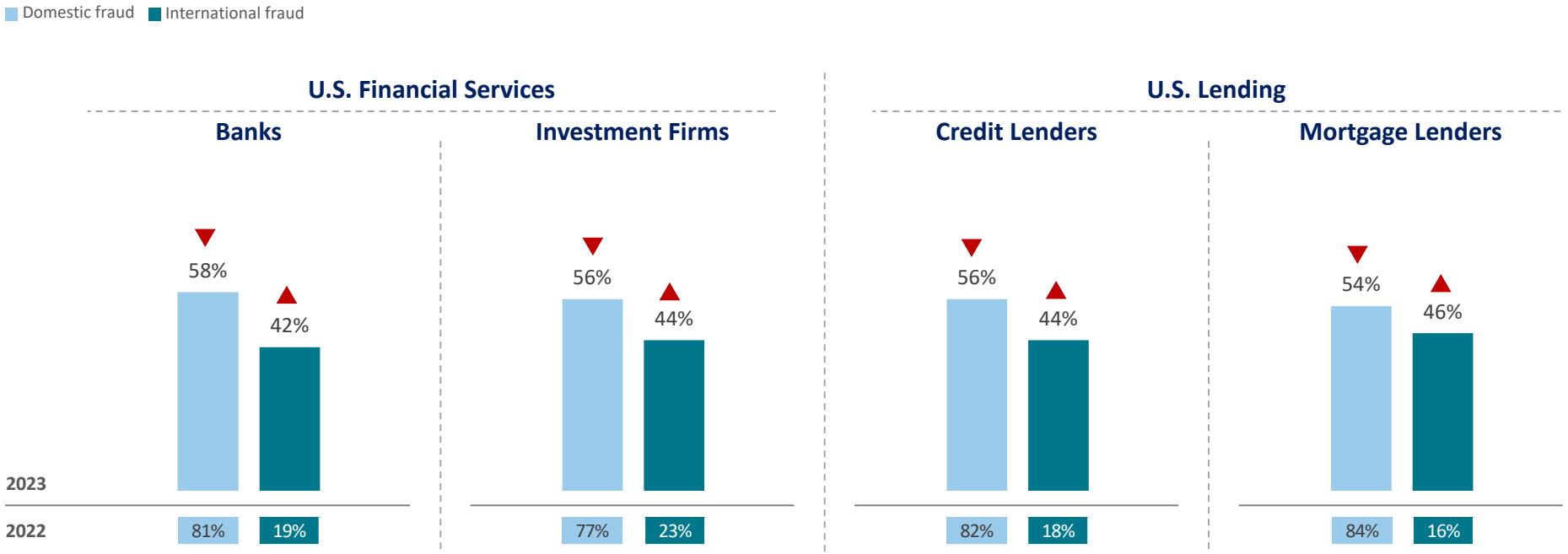
The Fraud Multiplier™ variable rose for all financial services segments, more so in Canada than for U.S. firms. For every $1 of fraud loss, it costs Canadian firms $1 more compared to last year: $4.45 in 2023 versus $3.49 in 2022, a 28% increase on average. U.S. investment firms and credit lenders reported a 9% increase year-over-year.

* According to a commissioned study conducted by Forrester Consulting on behalf of LexisNexis Risk Solutions, (Defend Against Authorized Transfer Scams) January 2024.

International fraud spiked for U.S. firms.

The increase aligns with widespread challenges assessing fraud risk by country or region, and a lack of specialized fraud prevention tools for international transactions.

% Fraud from Domestic and International Transactions



Survey Question
Q10. Using your best estimate, please indicate the percent of fraud costs your organization generated through domestic accounts compared to international accounts during the past 12 months. (U.S. respondents only)

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

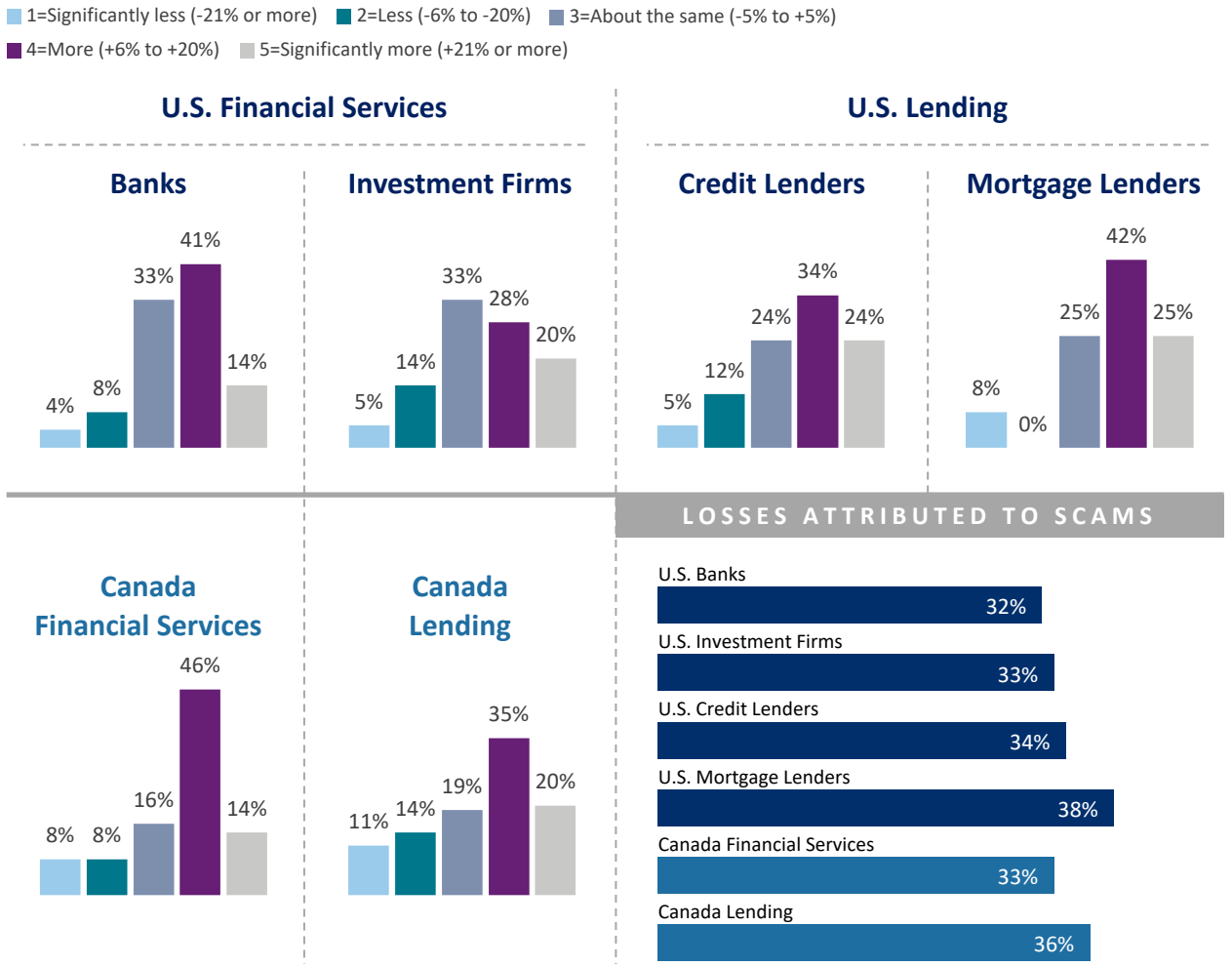
Scams are still a major contributor to fraud losses, despite efforts to educate consumers.

Although 48% of financial institutions surveyed say they have undertaken efforts to educate customers about information security and how to protect themselves, the number of consumers that are falling prey to scammers continue to grow.

Across North America, roughly 6 in 10 financial institutions report seeing an increase in scams over the last year.

To that end, about 35% of fraud losses in the region are now attributed to scams.

Rate of increase of authorized transfer scams



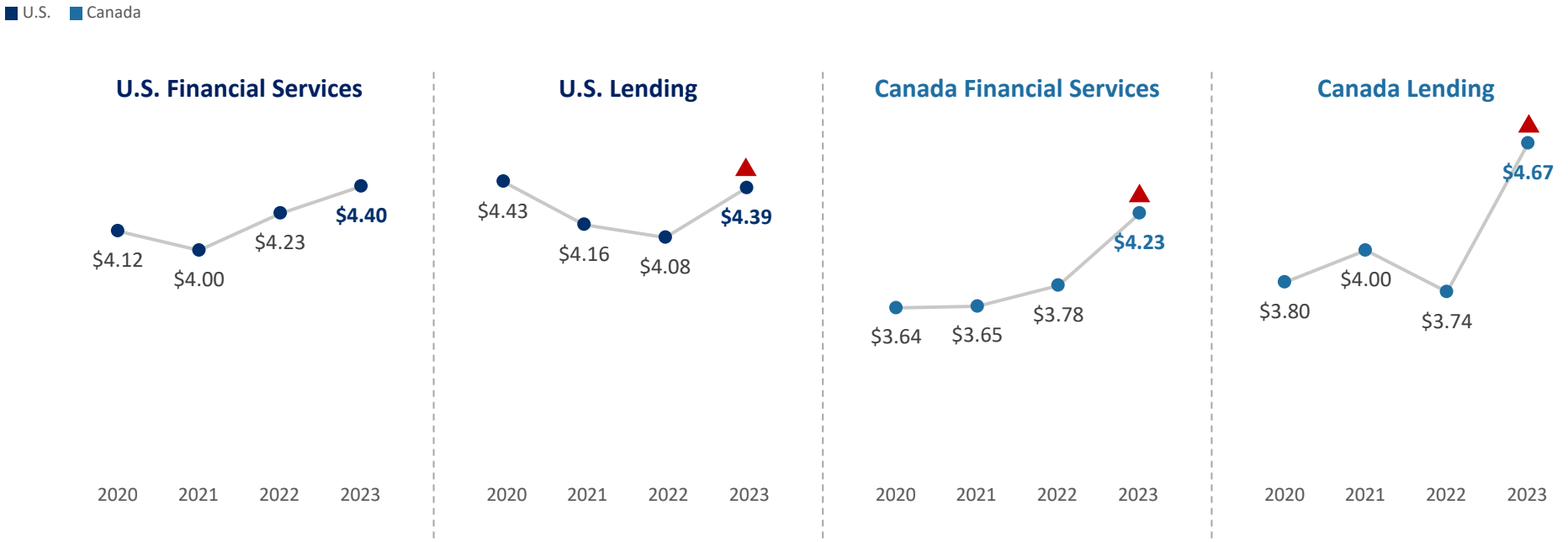
Survey Questions
Q2_15. In the past 12 months, has your company detected less, more, or an equal amount of the following types of online fraud compared to the previous year? — Scams (e.g., consumers manipulated into authorizing transfers against their best interests)
Q5. Of your company's total fraud losses, what percentage of it can be attributed to scams?

Fraud costs rose for all financial services segments, more so in Canada than in the U.S.

For every $1 of fraud loss, it costs Canadian firms $1 more compared to last year: $4.45 in 2023 versus $3.49 in 2022, a 28% increase on average. As businesses battle with rising inflation, labor costs are driven up. This is further compounded by more stringent fraud regulations, which has impacted costs associated with fines and legal fees.

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.

LexisNexis Fraud Multiplier™ Variable



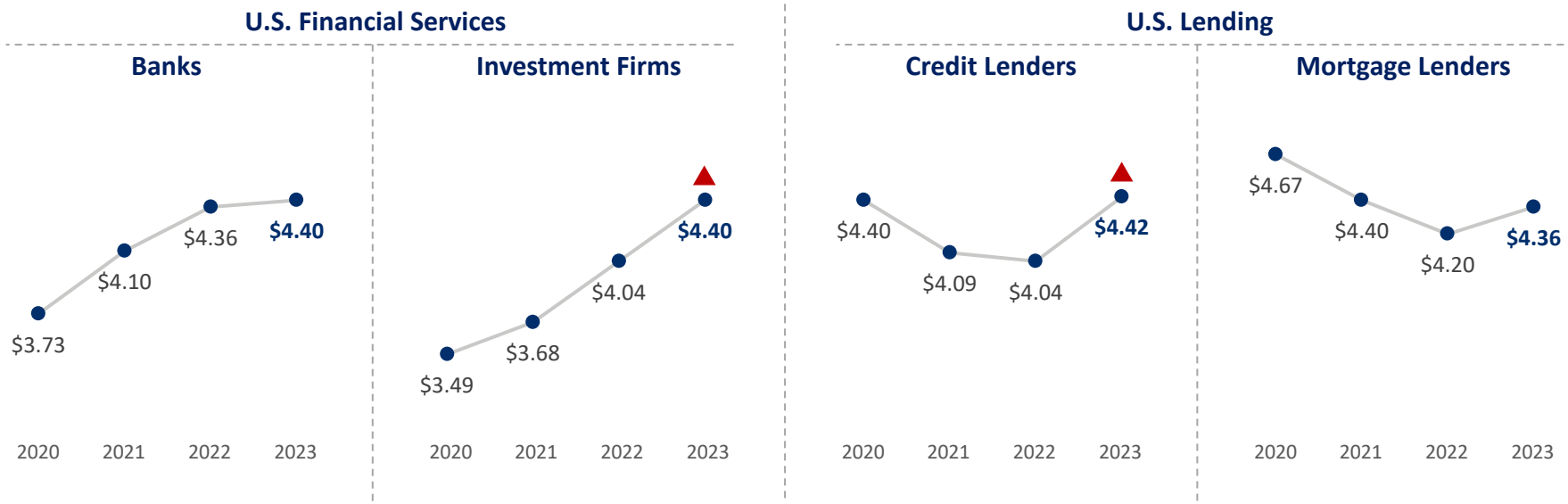
Survey Question
Q6. In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.

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

U.S. investment firms and credit lenders reported a 9% increase year-over-year, noticeably higher than U.S. banks and mortgage lenders.

LexisNexis Fraud Multiplier™ Variable

Domestic fraud International fraud



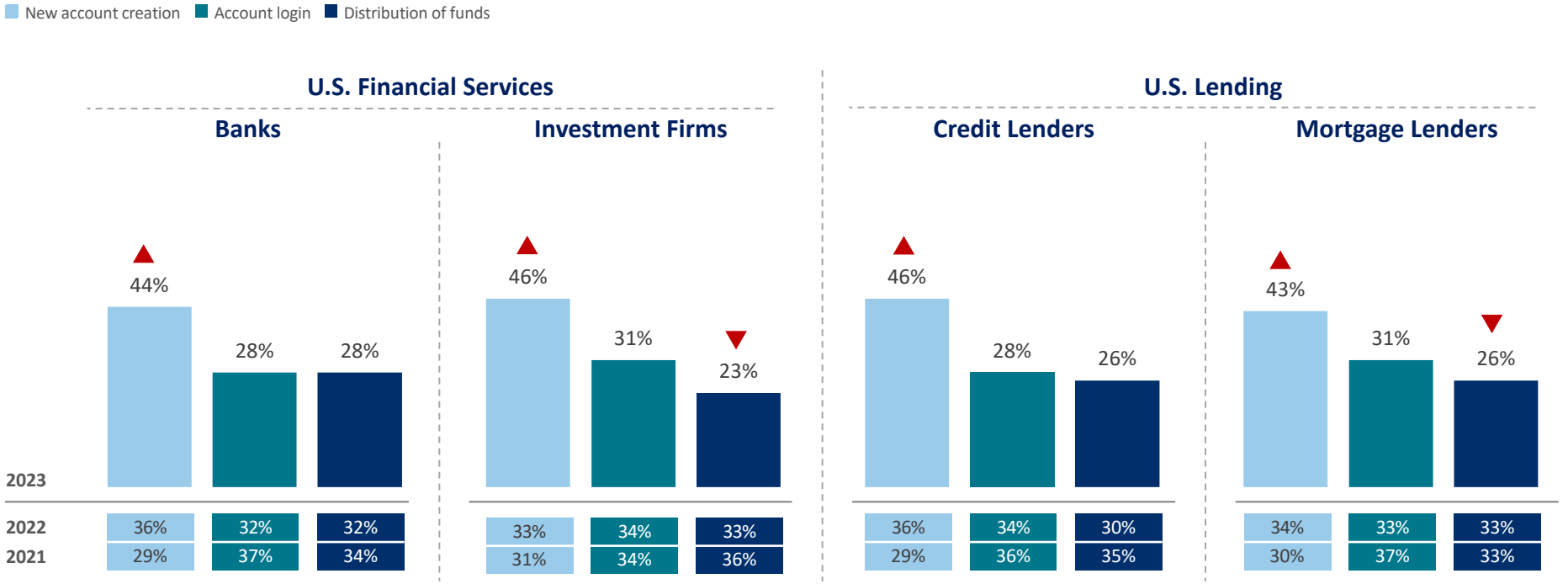
Survey Question
Q6. In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.

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

Fraud losses at the new account creation stage of the customer journey increased significantly between 2022 and 2023.

Organizations are succeeding at defending account logins and distribution of funds, but fraudsters are finding new ways of attack at account creation. With online and mobile banking becoming more pervasive, bad actors can use fake or stolen IDs to open new bank accounts or to obtain loans.

% Distribution of Fraud Losses by Customer Journey Stages

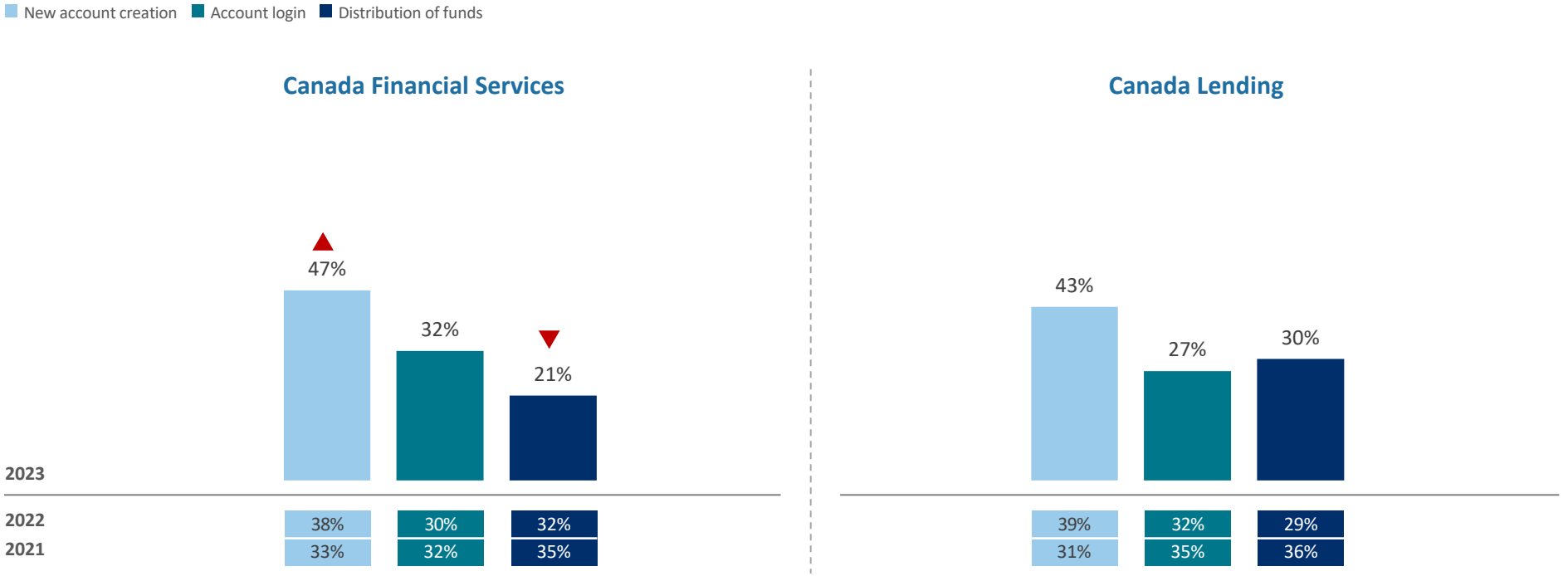


Survey Question
Q7. Approximately how much of your organization's fraud losses would you attribute to each of the following customer-journey stages?

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

New account creation has also become a significantly larger threat for Canadian financial services firms, while Canadian lenders must contend with incremental increases in fraud at both account creation and distribution of funds.

% Distribution of Fraud Losses by Customer Journey Stages



Survey Question
Q7. Approximately how much of your organization's fraud losses would you attribute to each of the following customer-journey stages?

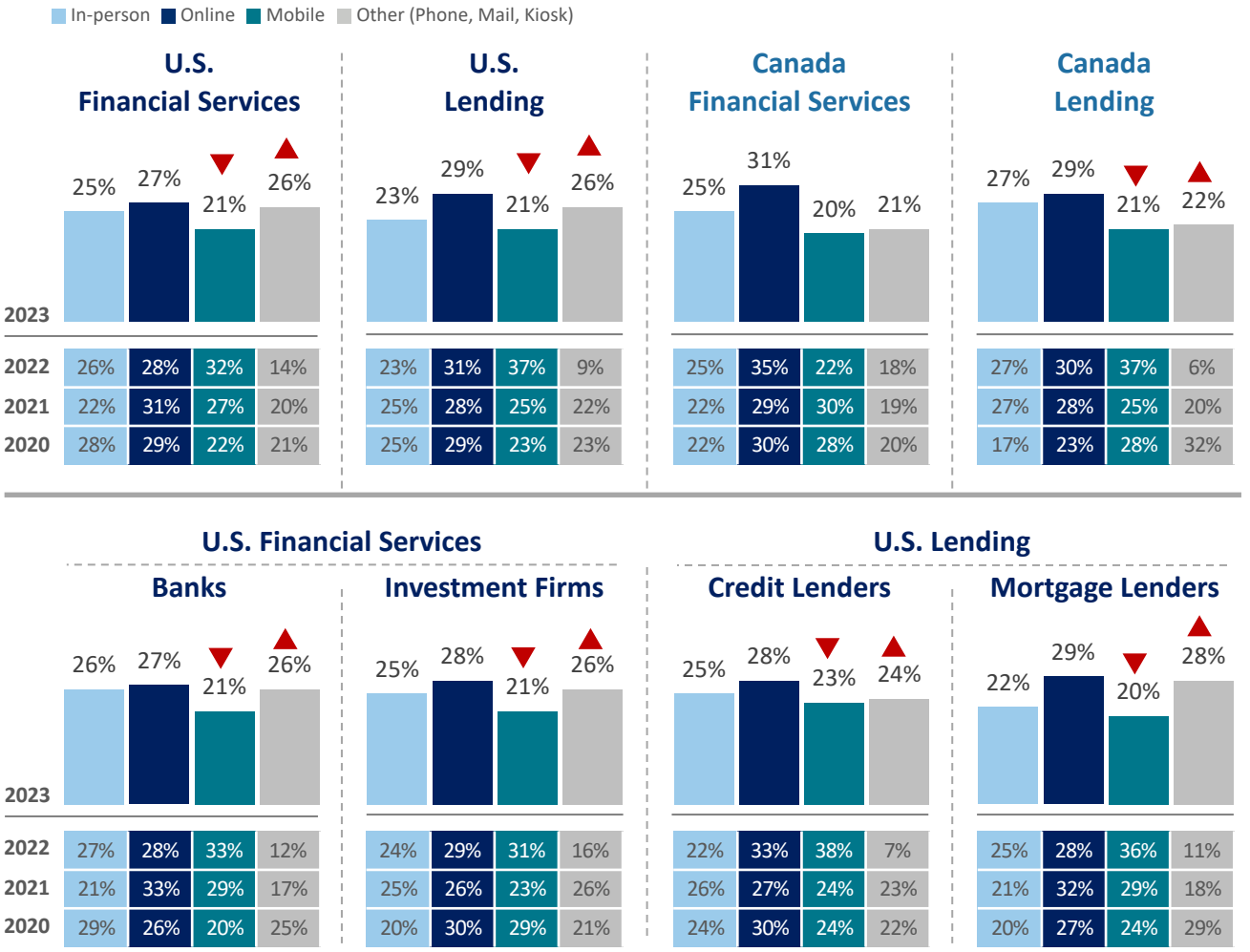
▼▲ = significantly or directionally higher/lower than previous period

Fraud losses in the phone channel spiked across the industry.

Losses in the mobile channel declined after a broad increase in 2022, reflecting financial firms' successful response.

Nearly two-thirds (65%) of U.S. financial institutions ranked 'phone calls' as the channel fraudsters use most often to perpetrate scams.*

% Fraud Costs by Channel



Survey Question
Q11. Using your best estimate, please indicate the percent of fraud costs your organization generated through each of the following transaction channels as a percentage of total annual fraud losses.

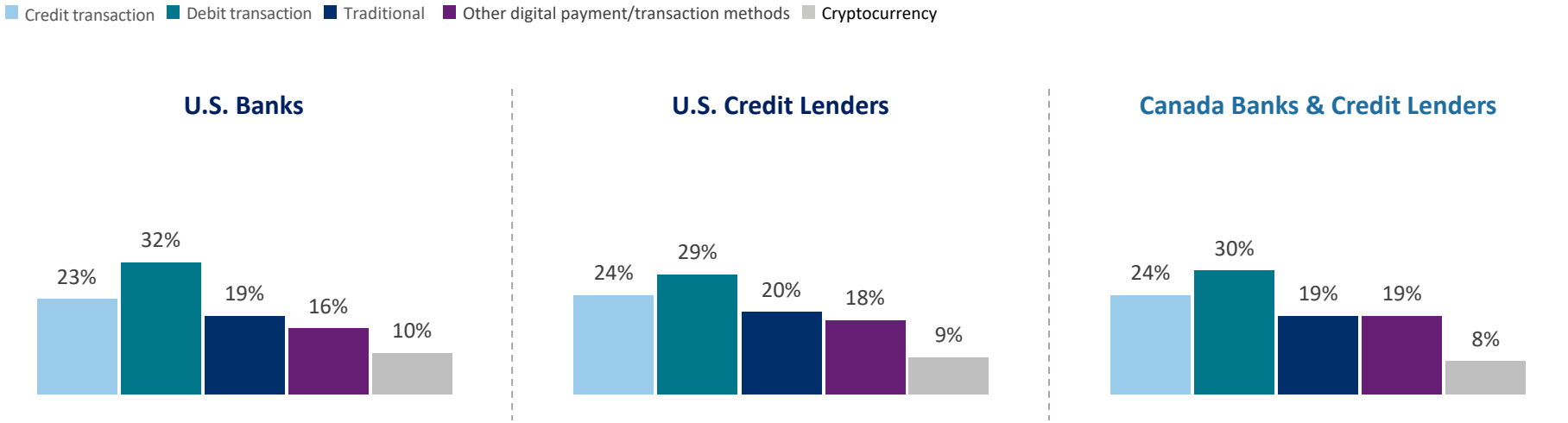
▼▲ = significantly or directionally higher/lower than previous period

* Messaging applications and email were the second- (62%) and third-most (57%) cited channels, according to a commissioned study conducted by Forrester Consulting on behalf of LexisNexis Risk Solutions, (Defend Against Authorized Transfer Scams) January 2024.

Fraud losses via debit transactions exceed losses via other transaction methods, particularly for U.S. banks.

Losses contrast with decline in usage relative to an increase in use of traditional transaction methods.

% of Total Fraud Losses

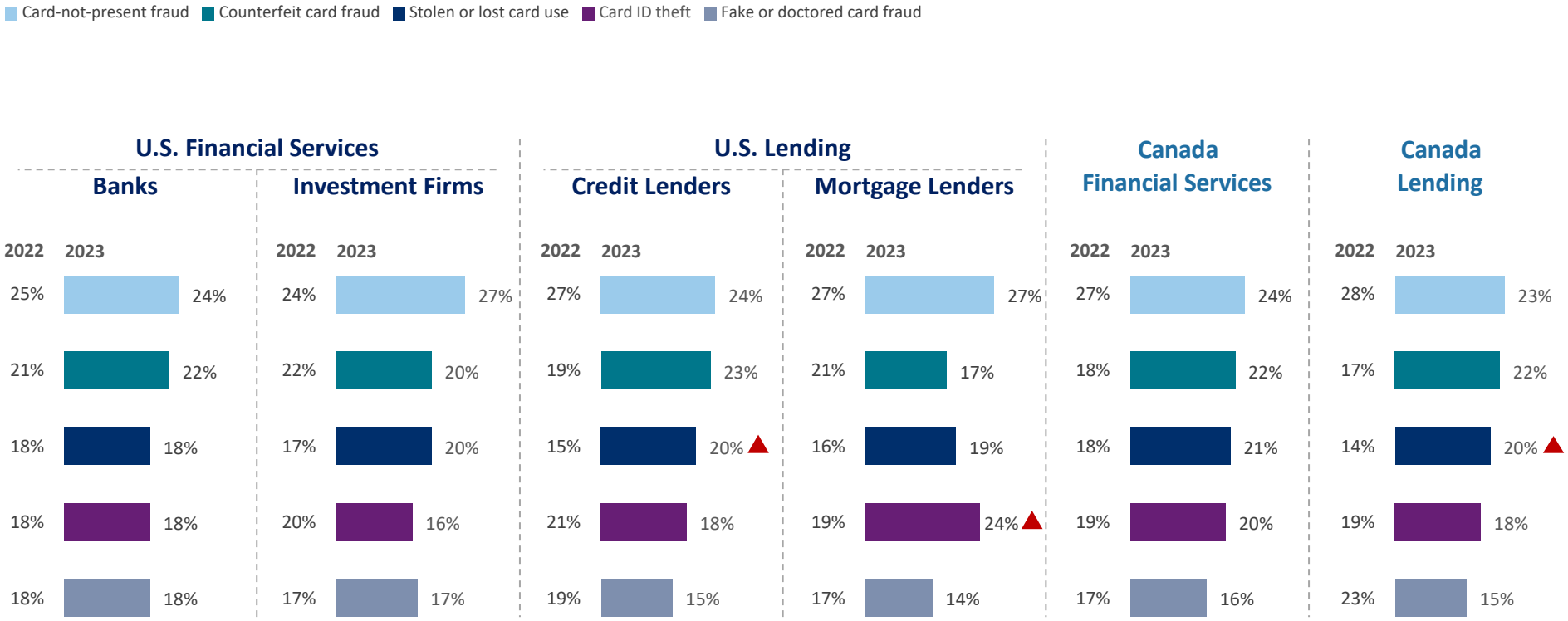


Survey Question
Q12. Using your best estimate, please indicate the percent of fraud costs your organization generated through each of the following transaction methods as a percentage of total annual fraud losses.

Counterfeit card fraud drives incremental increase in card fraud.

U.S. credit lenders and Canadian firms report more losses due to counterfeit, fake or doctored card fraud, with U.S. banks reporting a muted increase in counterfeit card fraud. Stolen or lost card use also increased for these same groups, with U.S. credit lenders hit the hardest. Conversely, lenders reported less use or manipulation of card details to take over or open an account or defraud a merchant.

% of Card-Related Fraud Losses



Survey Question
Q13. Of your organization's credit or debit card related fraud losses, please indicate the distribution across the following types of card fraud.

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

Key Finding 5

Organizations that build a more robust, multi-layered approach against fraud through the customer journey report lower fraud losses.

Across industries, geographies and customer journey stages, firms have implemented more advanced identity authentication and transaction verification solutions, especially behavioral biometrics, device identification, physical biometrics and browser/malware tracking solutions.

Having robust fraud management administration capabilities is key for both financial services and lending firms, as this empowers administrators to effectively configure, monitor, and maintain the fraud management system. Other important features include global network intelligence, utilization of AI/ML models, and segmentation of customers and attributes. Financial services firms also emphasize model explainability and governance.

Firms using a multi-layered, risk-based solutions approach tend to have a lower cost of fraud and fewer challenges across each customer journey stage. Organizations who build a more robust posture against fraud throughout customer journey stages report 41% lower fraud losses compared to the least mature organizations.

Advanced identity authentication solutions have been adopted across the customer journey among U.S. financial services firms, with more banks particularly adopting behavioral and physical biometrics, and investment firms investing in browser/malware tracking and device identification solutions.

Fraud Mitigation Solutions Use – U.S. Financial Services

U.S Banks U.S Investment Firms

	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	Positive & Negative Lists	Gov't issued ID	Quiz or KBA	OTP/ Two-Factor	Authenticate Using Behavioral Biometrics	Authenticate Using Biometrics	Phone # Risk & Verification	Browser/ Malware Tracking	Device ID	Real-Time Fraud Detection	Automated Transaction Scoring
New Accounts 2023	14% 19%	15% 20%	26% 19%	22% 25%	21% 27%	32% 23%	36% 23%	26% 19%	25% 23%	30% 33%	27% 25%	19% 22%	21% 22%
2022	23% 13%	39% 29%	22% 13%	47% 40%	38% 25%	42% 34%	23% 19%	17% 18%	41% 37%	16% 25%	24% 15%	26% 16%	21% 18%
Account Login 2023	22% 28%	23% 11%	16% 28%	22% 17%	18% 19%	23% 14%	40% 36%	25% 20%	18% 23%	22% 30%	23% 25%	23% 22%	25% 30%
2022	20% 11%	37% 24%	19% 17%	41% 28%	36% 23%	45% 42%	18% 19%	17% 19%	53% 33%	20% 10%	20% 15%	16% 14%	21% 15%
Distribution of Funds 2023	32% 27%	30% 28%	21% 30%	26% 22%	30% 13%	23% 28%	47% 38%	33% 27%	38% 31%	29% 25%	23% 34%	25% 31%	32% 25%
2022	29% 18%	42% 40%	23% 27%	42% 35%	29% 20%	46% 32%	22% 19%	31% 17%	51% 27%	25% 15%	31% 22%	19% 26%	30% 15%

Survey Question
Q24. Which fraud detection/mitigation solutions does your company currently use for the following transaction or customer-journey points?

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

The number of U.S. Lenders adopting advanced identity authentication and transaction verification solutions have significantly increased, particularly behavioral biometrics and device identification.

Fraud Mitigation Solutions Use – U.S. Lending

U.S Credit Lenders | U.S 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 2023	20% 0%	23% 8%	28% 8%	16% 8%	28% 33%	28% 42%	28% 17%	28% 33%	37% 42%	23% 33%	26% 0%	25% 8%	32% 17%	32% 33%	36% 17%	22% 8%	33% 33%
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%
Account Login 2023	24% 25%	28% 8%	23% 17%	21% 8%	21% 17%	24% 25%	28% 25%	30% 17%	32% 25%	24% 25%	15% 8%	22% 8%	25% 17%	32% 25%	27% 17%	16% 25%	32% 25%
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%
Distribution of Funds 2023	25% 17%	28% 8%	29% 8%	19% 25%	26% 17%	28% 25%	25% 33%	37% 25%	34% 33%	31% 25%	35% 8%	32% 8%	28% 8%	39% 17%	33% 25%	24% 8%	30% 17%
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%

Survey Question
Q24. Which fraud detection/mitigation solutions does your company currently use for the following transaction or customer-journey points?

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

Canadian institutions report using more passive and digital Identity-based authentication solutions, particularly behavioral biometrics and browser/ malware tracking, as well as automated transaction scoring. Positive and negative lists gained wider adoption as well, especially among financial services firms.

Fraud Mitigation Solutions Use – Canada Financial Services & Lending

Canada Financial Services | Canada Lending

	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	Positive & Negative Lists	Gov't issued ID	Quiz or KBA	OTP/ Two-Factor	Authenticate Using Behavioral Biometrics	Authenticate Using Biometrics	Phone # Risk & Verification	Browser/ Malware Tracking	Device ID	Real-Time Fraud Detection	Automated Transaction Scoring
New Accounts 2023	16% 24%	30% 32%	16% 24%	38% 41%	19% 11%	14% 35%	49% 30%	14% 35%	14% 32%	30% 30%	35% 24%	19% 22%	38% 27%
2022	34% 20%	65% 23%	10% 16%	70% 40%	22% 14%	64% 56%	7% 18%	34% 25%	73% 39%	4% 17%	26% 19%	20% 43%	25% 14%
Account Login 2023	22% 19%	32% 11%	5% 24%	35% 24%	19% 14%	30% 32%	30% 35%	16% 14%	19% 22%	16% 32%	32% 24%	24% 19%	32% 38%
2022	12% 11%	71% 45%	3% 13%	62% 37%	26% 20%	69% 39%	8% 14%	36% 24%	61% 53%	18% 17%	35% 18%	9% 29%	7% 17%
Distribution of Funds 2023	19% 32%	30% 32%	14% 19%	22% 32%	35% 11%	19% 35%	41% 41%	30% 35%	14% 19%	19% 46%	32% 24%	32% 24%	22% 35%
2022	26% 37%	67% 37%	12% 22%	62% 32%	31% 23%	62% 36%	18% 15%	26% 34%	68% 37%	15% 13%	32% 24%	3% 27%	17% 21%

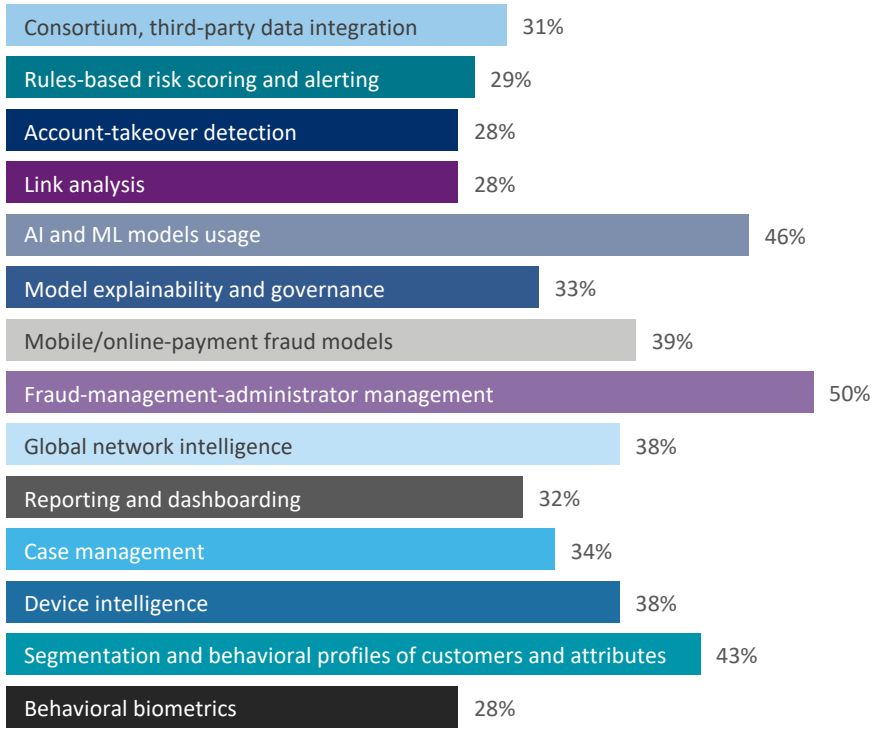
Survey Question
Q24. Which fraud detection/mitigation solutions does your company currently use for the following transaction or customer-journey points?

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

Most important features in fraud management solutions.

Having robust fraud management administration capabilities is key for both financial services and lending firms, as this empowers administrators to effectively configure, monitor, and maintain the fraud management system. Other important features include global network intelligence, utilization of AI/ML models and segmentation of customers and attributes. Financial services firms also emphasize model explain ability and governance.

Rankings Of Solution Success Criteria



Survey Question
Q28. What are the top five most important features in a fraud-management solution?

MOST IMPORTANT FEATURES

U.S. Financial Services

- 38% Model explainability and governance
- 56% Fraud-management-administrator management
- 38% Global network intelligence

U.S. Lending

- 52% AI and ML models usage
- 48% Device Intelligence
- 48% Segmentation and behavioral profiles of customers and attributes

Canada Financial Services

- 46% AI and ML models usage
- 43% Model explainability and governance
- 49% Mobile/online-payment fraud models

Canada Lending

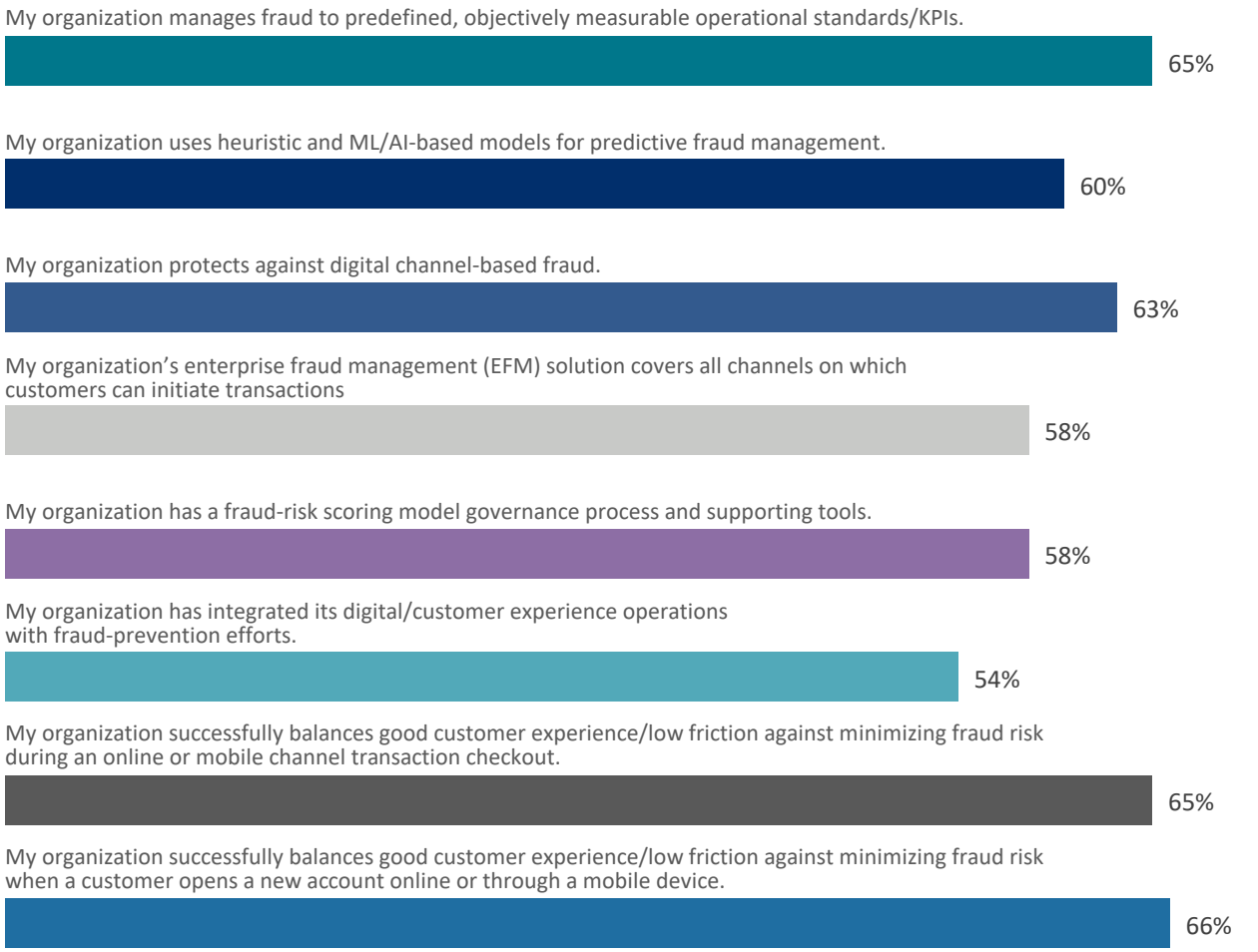
- 57% AI and ML models usage
- 59% Fraud-management-administrator management
- 49% Segmentation and behavioral profiles of customers and attributes

Organizational policies lead ahead of technology implementation and integration with digital/ customer experience.

Although respondents are confident in their organizations' current capabilities, especially continual identity verification, they report opportunities for improvement. U.S. financial services organizations see opportunity to further integrate digital/customer experience with fraud-prevention efforts, while Canadian counterparts are satisfied with their level of integration and balance between these priorities.

Survey Question
Q19. How much do you agree with the following statements? ("Agree" + "Strongly Agree")

Assessment of organizational policy and practice



Customer identity verification is a broad strength across the region. Areas for improvement vary between industries.

U.S. firms will likely continue to integrate digital/customer experience operations with fraud-prevention efforts. Conversations within Canadian firms will likely revolve around refining fraud-risk scoring processes across transaction channels.

Assessments with the most and least agreement

% AGREED OR STRONGLY AGREED

U.S. Financial Services

71%

My organization manages fraud to predefined, objectively measurable operational standards/KPIs.

54%

My organization has integrated its digital/ customer experience operations with fraud-prevention efforts.

U.S. Lending

67%

My organization successfully balances good customer experience/low friction against minimizing fraud risk during an online or mobile channel transaction checkout.

41%

My organization has integrated its digital/ customer experience operations with fraud-prevention efforts.

Canada Financial Services

81%

My organization successfully balances customer experience and fraud risk during new account creation.

44%

My organization has a fraud-risk scoring model governance process and supporting tools.

Canada Lending

68%

My organization uses heuristic and ML/AI-based models

43%

My organization's enterprise fraud management (EFM) solution covers all channels on which customers can initiate transactions

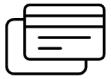
Survey Question
Q19. How much do you agree with the following statements? (Responses survey participants representing each segment were most and least likely to agree with.)

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

Fraud Issues

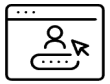
Digital Services

Fast transactions lead to easy synthetic identity and botnet targets. Velocity checks help to determine transaction risk, while data and analytics help to authenticate the individual.



Account-Related Fraud

Breached consumer personal data requires a risk-based security posture, as well as methods to distinguish legitimate consumers from bots or synthetic identities.



Synthetic Identities

Authenticate the individual behind the transaction more holistically in-order-to distinguish from a manufactured a manipulated identity based partially on real data.

Botnet Attacks

Mass human or automated attacks occur often to test cards, passwords/credentials or harvest consumer personal and device identifying information.

Mobile Channel

Source origination and infected devices add risk. Mobile bots and malware increase risk of identity fraud. Assess the device and its user, both in conjunction and in isolation.

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

Solution of Options

Assess the Transaction Risk

Velocity checks/transaction scoring: Compares current transactions against historical transaction patterns of an individual to detect if volume or other behavior by the cardholder indicates risk.

Solution examples: Real-time transaction scoring; automated transaction scoring

Assess the Transaction Risk

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: personal data known to the customer or via a physical device in the user's possession.

Solution examples: Authentication by challenge or quiz; one-time passwords; push authentication.

Authenticating the Digital Person

Digital Identity/Behavioral Biometrics: Analyzes signals from digital interactions, including device usage and digital identifiers, to discern between legitimate users and potential fraud risks.

Solution examples: Authentication by behavioral biometrics; email/phone risk assessment; browser/malware tracking.

Device assessment: Uniquely identify a remote computing device or user.

Solution examples: Device ID/ fingerprint; geolocation.

Fraud costs and the 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.

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

Minimize Friction While Maximizing Fraud Protection

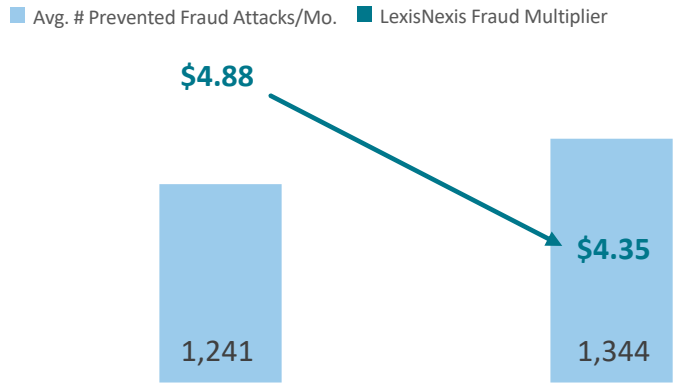
- Track successful and prevented fraud both by transaction channel and payment method
- Use digital/passive authentication solutions to reduce customer effort
- Assess both the individual and transactional risk

Integrate Cybersecurity and Digital Customer Experience Operations with Fraud Prevention

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 via risk-based workflows.

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 ($4.35) than those firms which do not follow this approach ($4.88). Furthermore, the former group reports preventing fraud attacks per month compared to those not using this approach.



LexisNexis Fraud Multiplier	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 to None	☑
Solution(s) to assess device risk, location (e.g., Device ID, Geolocation)	Limited to None	☑
Solution(s) to assess behavior (e.g., Behavioral Biometrics, Transaction Risk)	Limited to 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.

Implementing a broad range of solutions is more effective at preventing fraud.

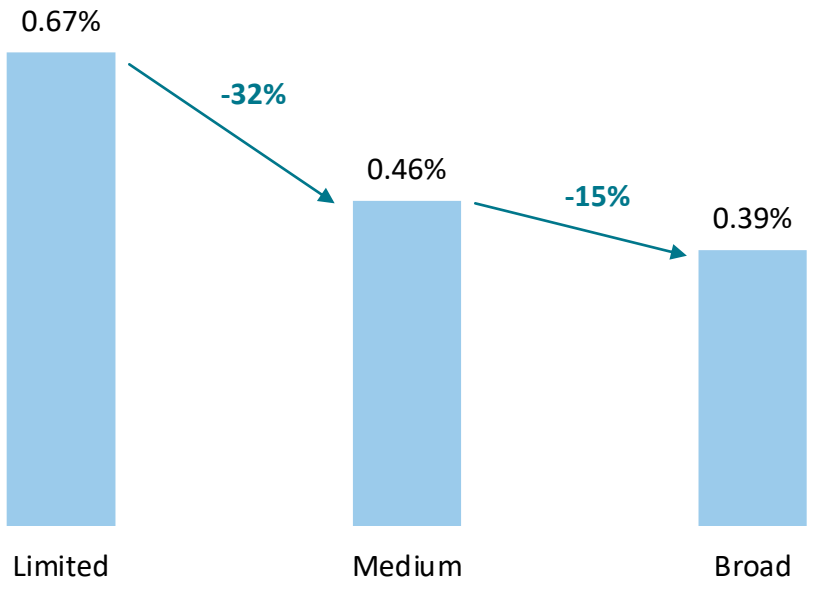
Organizations that build a more robust, multi-layered approach against fraud throughout customer journey stages report lower fraud losses. Having proper fraud management solutions in place may also help to increase compliance and limit liability in cases of fraud: these same organizations see slightly lower fraud losses.

Fraud Losses (as Percent of Revenue), by Strength of Fraud Prevention Measures

-41%

Difference in fraud loss of most mature vs. least mature organizations

Range of solutions implemented across the three customer journey stages.



Recommendations

To respond faster to emerging fraud trends and rising consumer expectations, forward-thinking financial institutions increasingly take a dynamic, agile and simplified approach to risk assessment. Capabilities integrated via risk-based workflows, supported by deep troves of identity intelligence and robust linking technology promote the flexibility, agility and simplicity necessary for safe and convenient interactions and transactions.

Financial institutions need to become more nimble to keep ahead of rising consumer expectations and emerging fraud attack schemes and vectors.

To pivot quickly and reduce complexity — across the three primary consumer journey stages, across all channels and according to all risk levels — financial firms should implement and optimize risk-based workflows composed of a flexible, robust and interoperable array of physical, digital and behavioral risk and authentication assessment capabilities, which derive from deep, broad and relevant troves of reliable, actionable intelligence.

Risk-based workflows respond effectively to the risk level of the present interaction or transaction, correctly blocking fraudulent actions while promoting positive experiences for legitimate consumers. This hinges on a firm's ability to call an appropriate combination of risk-assessment capabilities and detect the risk level of the present interaction or transaction.

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

Identity proofing involves both verification and authentication. Verification relates to self-provided data (date of birth, national ID number, address, etc.) to determine if the person/identity is real and that the data relates to a single identity. **This is particularly important with the rise of synthetic identity fraud. Authentication confirms that the person is legitimate (i.e., they are 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.) is not longer adequate to fully authenticate identity.

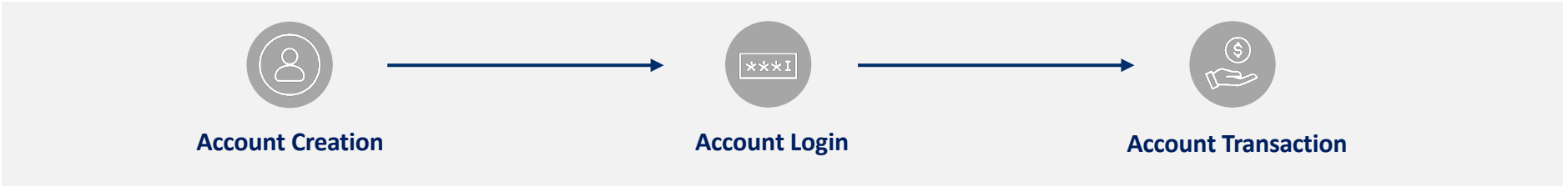
Businesses should have a robust fraud and security technology platform that helps them adapt to this changing digital environment, offering strong fraud management and resulting in a more seamless experience for genuine customers.

Deploying technologies that better recognize legitimate customers, mitigate fraud and build the fraud knowledge base to streamline on-boarding can prevent account takeovers and detect insider threats.

Using a 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.

Meet rising consumer expectations, and detect and mitigate more numerous, severe and sophisticated fraud and identity risks via risk-based workflows customized to each phase of the customer journey and transaction channel.



- Single point protection can be inadequate and can result in a 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.

- 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 risk-based workflows approach, composed of a flexible, robust and interoperable array of physical, digital and behavioral risk and authentication assessment capabilities, which derive from deep, broad and relevant troves of reliable, actionable intelligence.

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.

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.

Protect Entry Points:
Implement strong customer identity and access management (CIAM) controls by integrating cybersecurity and digital experience operations with fraud detection technology. This helps guard against attacks while minimizing friction.

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

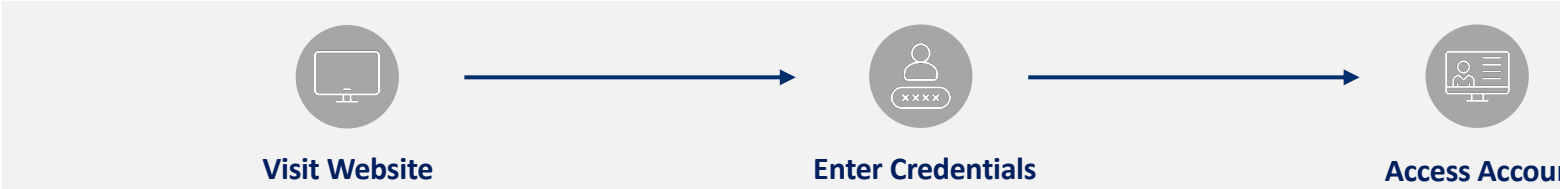
Authenticate the Physical Person:
Verify physical identity attributes, consumer identity events and account-creation behavior.

Authenticate the Digital Person:
Analyze signals from digital interactions, including device usage, device reputation and digital identifiers, to discern between legitimate users and potential fraud risks.
Solution Examples: Authentication by behavioral biometrics; Device ID/fingerprint – seamless risk assessment that minimizes customer effort and friction

Continue to Manage Risk Across All Endpoints:
Increase flexibility and reduce complexity via a robust and interoperable array of physical, digital and behavioral risk and authentication assessment capabilities.

Use technologies that recognize your customers, determine their point of access and distinguish them from fraudsters and malicious bots. Solutions layered in a risk-based workflow support an assessment and response appropriate for each individual interaction, minimizing impact on customer experience.

Use technologies that recognize your customers, determine their point of access and distinguish them from fraudsters and malicious bots. Solutions layered in a risk-based workflow support an assessment and response appropriate for each individual interaction, minimizing impact on customer experience.



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 legitimate consumer from a bot or synthetic identity

Authenticate the Physical Person:
Analyze human-device interactions and behavioral patterns, such as mouse clicks and keystrokes, to discern between a real user and an imposter. This is particularly important at account login since fraudsters deploy mass attacks, using breached data, to test passwords for account takeover. Leverage crowdsourced device and account intelligence for additional risk signal that would be otherwise unavailable.
Solution Examples: Authentication by biometrics; email/phone risk assessment, device intelligence consortiums – seamless risk assessment that minimizes customer effort and friction.

Active Identity Authentication:
Confirm the user's claimed identity via personal data known only to the customer or via a physical device in the user's possession.
Solution examples: Authentication by challenge or quiz; one-time passwords; push authentication.

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

Add transaction and payee 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.

Authenticate the Digital Person:
Analyze signals from digital interactions, including device usage, device reputation and digital identifiers, to discern between legitimate users and potential fraud risks.
Solution Examples: Authentication by behavioral biometrics; email/phone risk assessment; Device ID/ fingerprint – 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:
Confirm the user's claimed identity via personal data known only to the customer or via a physical device in the user's possession.
Solution examples: Authentication by challenge or quiz; one-time passwords; push authentication.

Access the Transaction:
Velocity checks/transaction scoring: Compare current transactions against historical transaction patterns of an individual to detect if volume or other behavior by the cardholder indicates risk.
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, sophisticated analytics platforms and technology solutions to provide insights that help businesses across multiple industries and governmental entities reduce risk and improve decisions to benefit people around the globe. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

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

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	When a fraudulent party manipulates or deceives an authorized account owner to transfer funds to an account under the fraudulent party's control
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

Survey Question
Q21/22. Please rank the top four challenges for each customer journey stage related to fraud your company faces when serving customers using the ONLINE/MOBILE channel.

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

2023

	New Account Creation		Account Login		Distribution of Funds	
	Banks	**Investment Firms**	**Banks**	**Investment Firms**	**Banks**	**Investment Firms**
Top Online Channel Challenges	**Verification** – Address (30%) – Email or Device (30%) **Assessing risk by country** (32%) **Manual reviews** (30%)	**Verification** – Address (30%) – Identity (30%) **New transaction methods** (30%) **Manual reviews** (30%) **Lack of specialized tools** (31%) **Malicious bot transactions** (36%)	**Verification** – Address (32%) – Identity (33%) **Knowing origination source** (33%) **New transaction methods** (33%)	**Verification** – Address (33%) – Identity (36%) **New transaction methods** (33%) **Lack of specialized tools** (31%)	**Verification** – Address (29%) – Identity (30%) – Phone (44%) **Malicious bot transactions** (36%)	**Verification** – Email or Device (28%) **Knowing origination source** (33%) **Lack of specialized tools** (31%) **Malicious bot transactions** (45%)
Top Mobile Channel Challenges	**Verification** – Address (31%) – Email or Device (34%) **Assessing risk by country** (34%) **Balancing fraud-prevention friction** (31%)	**Verification** – Phone (38%) – Identity (28%) **Lack of specialized tools** (38%) **Malicious bot transactions** (30%) **Balancing fraud-prevention friction** (28%)	**Verification** – Address (37%) – Email or Device (28%) – Identity (30%) **Assessing risk by country** (28%) **Knowing origination source** (28%) **New transaction methods** (28%) **Lack of specialized tools** (30%)	**Assessing risk by country** (30%) **Lack of specialized tools** (36%) **Malicious bot transactions** (38%) **Balancing fraud-prevention friction** (34%)	**Verification** – Address (32%) – Email or Device (32%) – Identity (31%) **Knowing origination source** (31%)	**Manual reviews** (28%) **Lack of specialized tools** (38%) **Malicious bot transactions** (34%) **Verification** – Identity (38%) **Balancing fraud-prevention friction** (28%)

Survey Question
Q21/22. Please rank the top four challenges for each customer journey stage related to fraud your company faces when serving customers using the ONLINE/MOBILE channel.

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

■ 2023

	New Account Creation		Account Login		Distribution of Funds	
	Credit Lending	**Mortgage Firms**	**Credit Lending**	**Mortgage Firms**	**Credit Lending**	**Mortgage Firms**
Top Online Channel Challenges	**Lack of specialized tools** (32%) **Malicious bot transactions** (33%) **Verification** – Identity (32%) **Balancing fraud-prevention friction** (35%)	**Knowing origination source** (33%) **New transaction methods** (42%) **Lack of specialized tools** (33%) **Malicious bot transactions** (33%) **Verification** – Identity (42%) **Balancing fraud-prevention friction** (33%)	**Verification** – Email or Device (30%) – Identity (33%) **Manual Reviews** (30%) **Lack of specialized tools** (37%) **Balancing fraud-prevention friction** (33%)	**Verification** – Email or Device (33%) **New transaction methods** (50%) **Malicious bot transactions** (42%) **Balancing fraud-prevention friction** (42%)	**Verification** – Address (29%) – Identity (33%) **Malicious bot transactions** (33%) **Balancing fraud-prevention friction** (34%)	**Knowing origination source** (33%) **New transaction methods** (33%) **Lack of specialized tools** (42%) **Verification** – Identity (42%) **Balancing fraud-prevention friction** (33%)
Top Mobile Channel Challenges	**Verification** – Phone (30%) – Identity (33%) **Malicious bot transactions** (33%) **Balancing fraud-prevention friction** (28%)	**Knowing origination source** (42%) **New transaction methods** (42%) **Verification** – Identity (50%) **Balancing fraud-prevention friction** (42%)	**Verification** – Phone (33%) – Identity (32%) **Knowing origination source** (33%) **Lack of specialized tools** (30%)	**Verification** – Email or Device (42%) – Identity (33%) **Knowing origination source** (33%) **Malicious bot transactions** (58%)	**Knowing origination source** (29%) **Malicious bot transactions** (29%) **Verification** – Identity (32%) **Balancing fraud-prevention friction** (33%)	**Knowing origination source** (33%) **Lack of specialized tools** (33%) **Malicious bot transactions** (33%) **Verification** – Identity (50%) **Balancing fraud-prevention friction** (42%)

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.

Canada Financial Services & Lending

2023

	New Account Creation		Account Login		Distribution of Funds	
	Financial Services	**Lending**	**Financial Services**	**Lending**	**Financial Services**	**Lending**
Top Online Channel Challenges	**Assessing risk by country** (32%) **Knowing origination source** (32%) **New transaction methods** (32%) **Malicious bot transactions** (41%) **Verification** – Identity (32%)	**Verification** – Address (41%) – Identity (41%) **Assessing risk by country** (35%) **New transaction methods** (30%) **Manual reviews** (30%)	**Verification** – Email or Device (38%) – Identity (32%) **Knowing origination source** (35%) **Malicious bot transactions** (38%)	**Verification** – Address (38%) – Email or Device (35%) **Assessing risk by country** (35%) **New transaction methods** (27%) **Manual reviews** (27%) **Balancing fraud-prevention friction** (27%)	**Assessing risk by country** (38%) **New transaction methods** (30%) **Lack of specialized tools** (38%) **Malicious bot transactions** (35%) **Verification** – Identity (30%) **Balancing fraud-prevention friction** (30%)	**Verification** – Email or Device (35%) – Identity (32%) **Manual reviews** (32%) **Lack of specialized tools** (35%)
Top Mobile Channel Challenges	**Assessing risk by country** (30%) **Verification** – Phone (32%) **New transaction methods** (30%) **Lack of specialized tools** (30%) **Balancing fraud-prevention friction** (30%)	**Assessing risk by country** (30%) **Knowing origination source** (30%) **Manual reviews** (32%) **Balancing fraud-prevention friction** (35%)	**Verification** – Phone (35%) **Knowing origination source** (32%) **Lack of specialized tools** (41%) **Malicious bot transactions** (32%) **Balancing fraud-prevention friction** (38%)	**Verification** – Address (32%) – Email or Device (30%) – Identity (32%) **Assessing risk by country** (38%) **Knowing origination source** (30%) **Malicious bot transactions** (30%)	**Verification** – Phone (38%) **Knowing origination source** (30%) **New transaction methods** (41%) **Balancing fraud-prevention friction** (35%)	**Assessing risk by country** (35%) **Manual reviews** (30%) **Malicious bot transactions** (30%) **Verification** – Identity (38%)

Survey Question
Q21/22. Please rank the top four challenges for each customer journey stage related to fraud your company faces when serving customers using the ONLINE/MOBILE channel.