6th Annual True Cost of Fraud™ Study: Financial Services and Lending Report
U.S. and Canada Edition 2022
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).

<table>
<thead>
<tr>
<th>Total</th>
<th>Company Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Financial Services</td>
<td>Credit &amp; Lending</td>
</tr>
<tr>
<td># Completions</td>
<td>502</td>
<td>251</td>
</tr>
</tbody>
</table>

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

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

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.

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.

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.
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.
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.

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

Key Finding 1
FRAUD TARGETING MOBILE CHANNEL TRANSACTIONS

Fraud Targeting Mobile Channel Transactions

<table>
<thead>
<tr>
<th>Financial Services (Overall)</th>
<th>Banks</th>
<th>Investment Firms</th>
<th>Lending (Overall)</th>
<th>Credit Lenders</th>
<th>Mortgage Lenders</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022</td>
<td>95%</td>
<td>96%</td>
<td>93%</td>
<td>96%</td>
<td>99%</td>
</tr>
<tr>
<td>2021</td>
<td>98%</td>
<td>92%</td>
<td>98%</td>
<td>96%</td>
<td>96%</td>
</tr>
</tbody>
</table>

% 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

U.S. Financial Services vs. Lending

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

- 2022
- 2021

Key Findings

- Trends/Landscape
- Attacks & Costs
- Scams Impacting Customer Journey Risks
- BNPL Impact on Fraud Detection
- Identity-related Fraud
- Risk Mitigation Smart Practices
- Recommendations

#1

Overview

Key Findings

Trends/Landscape

Attacks & Costs

Scams Impacting Customer Journey Risks

BNPL Impact on Fraud Detection

Identity-related Fraud

Risk Mitigation Smart Practices

Recommendations

#2

#3

#4

#5

#6

#2

#4

#5

#6
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.

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

% Saying Fraud Targeting Mobile Has Increased

<table>
<thead>
<tr>
<th>Year</th>
<th>Financial Services (Overall)</th>
<th>Lending (Overall)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022</td>
<td>84% ▼</td>
<td>94%</td>
</tr>
<tr>
<td>2021</td>
<td>95%</td>
<td>89%</td>
</tr>
</tbody>
</table>

% Increase

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

= 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.
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

---

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.

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. 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. 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.

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

- Consumer phishing
- Wire/money transfer fraud
- Scams targeting/involving digital payments
- Money mule scams

Key Finding 1
SCAMS LEADING TO FRAUD LOSSES

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

<table>
<thead>
<tr>
<th>Scam Type</th>
<th>U.S. Financial Services</th>
<th>U.S. Lending</th>
<th>Canada Financial Services</th>
<th>Canada Lending</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer phishing</td>
<td>66%</td>
<td>75%</td>
<td>67%</td>
<td>88%</td>
</tr>
<tr>
<td>Wire/money transfer fraud</td>
<td>61%</td>
<td>51%</td>
<td>46%</td>
<td>55%</td>
</tr>
<tr>
<td>Scams targeting/involving digital payments</td>
<td>66% for M/L Mortgage</td>
<td>61% for above avg. mobile transactions</td>
<td>65%</td>
<td>65%</td>
</tr>
<tr>
<td>Money mule scams</td>
<td>72% for M/L and above avg. mobile transactions</td>
<td>19%</td>
<td>25%</td>
<td></td>
</tr>
</tbody>
</table>

---

1. 71% for M/L Banks vs 49% for Small Banks
2. 80% for Credit Lenders vs 57% for Mortgage Lenders
3. = significantly or directionally higher than same category in other industry segments

---

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

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

U.S. Financial Services
- 2019: 3%
- 2020: 14%
- 2021: 24%
- 2022: 29%

U.S. Lending
- 2019: 2%
- 2020: 16%
- 2021: 25%
- 2022: 24%

Canada Financial Services
- 2020: 20%
- 2021: 22%
- 2022: 29%

Canada Lending
- 2020: 28%
- 2021: 45%
- 2022: 27%

Segments Highlights
- U.S. Financial Services
  - Bot Attacks: Small: 18%; Medium/Large: 35%
- U.S. Investment Firms
  - Bot Attacks: Small: 23%; Medium/Large: 35%
- U.S. Banks
  - Bot Attacks: Small: 15%; Medium/Large: 35%
- U.S. Lending
  - Bot Attacks: Small: 20%
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.
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.

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.

\[\text{Cost of Fraud: LexisNexis Fraud Multiplier™} \]

Key Finding 2
INCREASED FRAUD COSTS
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.
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.

Survey Questions:
Q22: In a typical month, approximately how many fraudulent transactions are prevented by your company? Q24: In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

Average Monthly Fraudulent Transactions

<table>
<thead>
<tr>
<th></th>
<th>U.S. Financial Services</th>
<th>U.S. Lending</th>
<th>Canada Financial Services</th>
<th>Canada Lending</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2019</strong></td>
<td>1,570</td>
<td>1,801</td>
<td>1,345</td>
<td>1,791</td>
</tr>
<tr>
<td>Pre-pandemic</td>
<td>985</td>
<td>965</td>
<td>802</td>
<td>734</td>
</tr>
<tr>
<td>During pandemic</td>
<td>585</td>
<td>836</td>
<td>670</td>
<td>635</td>
</tr>
<tr>
<td><strong>2020</strong></td>
<td>1,821</td>
<td>2,034</td>
<td>944</td>
<td>905</td>
</tr>
<tr>
<td>Pre-pandemic</td>
<td>1,184</td>
<td>1,039</td>
<td>694</td>
<td>723</td>
</tr>
<tr>
<td>During pandemic</td>
<td>850</td>
<td>695</td>
<td>708</td>
<td>615</td>
</tr>
<tr>
<td><strong>2021</strong></td>
<td>2,034</td>
<td>1,855</td>
<td>941</td>
<td>1,175</td>
</tr>
<tr>
<td>Pre-pandemic</td>
<td>1,093</td>
<td>1,039</td>
<td>786</td>
<td>912</td>
</tr>
<tr>
<td>During pandemic</td>
<td>650</td>
<td>708</td>
<td>708</td>
<td>615</td>
</tr>
<tr>
<td><strong>2022</strong></td>
<td>1,789</td>
<td>1,432</td>
<td>855</td>
<td>1,175</td>
</tr>
</tbody>
</table>

Key Finding 2
INCREASED FRAUD ATTACKS

MID/LARGE SEGMENT HIGHLIGHTS

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

U.S. Lending
- Prevented Attacks: 1,022
- Successful Attacks: 712

Canadian Financial Services & Lending
- Prevented Attacks: 1,129
- Successful Attacks: 873
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. Across segments, mid/large firms experience a higher volume of fraudulent transactions per month.
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.
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.
In the True Cost of Fraud™ Report, 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
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

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.
**Key Finding 3**

**TOP ONLINE/MOBILE CHANNEL CHALLENGES ACROSS THE CUSTOMER JOURNEY**

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**

<table>
<thead>
<tr>
<th>U.S. Banks</th>
<th>U.S. Investment Firms</th>
<th>U.S. Credit Lenders</th>
<th>U.S. Mortgage Firms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Online</strong></td>
<td><strong>Mobile</strong></td>
<td><strong>Online</strong></td>
<td><strong>Mobile</strong></td>
</tr>
<tr>
<td>Verification</td>
<td>Verification</td>
<td>Verification</td>
<td>Verification</td>
</tr>
<tr>
<td>Phone (23% -&gt; 33%)</td>
<td>Email/device (31% -&gt; 41%)</td>
<td>Assessing risk by country (23% -&gt; 31%)</td>
<td>Manual reviews (25% -&gt; 36%)</td>
</tr>
<tr>
<td>Email/device (23% -&gt; 42%)</td>
<td>Phone (23% -&gt; 31%)</td>
<td>Knowing origination source (26% -&gt; 36%)</td>
<td>Knowing origination source (23% -&gt; 34%)</td>
</tr>
</tbody>
</table>

2021 – 2022

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.

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.
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.
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).
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.

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.

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.
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.

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?

Key Finding 3
SCAMS IMPACT ON FRAUD COSTS

Cost of Fraud: LexisNexis Fraud Multiplier™

U.S. Banks

Lower Cost of Fraud

More Scams (3+)

Higher Cost of Fraud

29% involving labor investigation

$4.75

$4.14

$4.36

21% involving labor investigation

U.S. Investment Firms

Lower Cost of Fraud

More Scams (3+)

Higher Cost of Fraud

$4.29

$3.65

$4.04

U.S. Mortgage Firms

Lower Cost of Fraud

More Scams (3+)

Higher Cost of Fraud

29% involving labor investigation

$4.73

$3.49

$4.00

20% involving labor investigation

U.S. Credit Lenders

Lower Cost of Fraud

More Scams (3+)

Higher Cost of Fraud

31% involving labor investigation

$4.81

$2.92

$4.04

18% involving labor investigation

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

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

#2

#1

#3

#4

#5

#6

Recommendations

Overview

Key Findings

Trends/Landscape

Attacks & Costs

Scams Impacting Customer Journey Risks

BNPL Impact on Fraud Detection

Identity-related Fraud

Risk Mitigation Smart Practices
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.
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***

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

---

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

- **Within the next 6 months**
  - U.S. Banks: 17%
  - U.S. Credit: 37%
  - Canada Banks and Credit Lenders: 35%
- **Within the next 6 – 12 months**
  - U.S. Banks: 46%
  - U.S. Credit: 0%
  - Canada Banks and Credit Lenders: 3% (for Small) 23% (for M/L)
- **Within the next 12 – 18 months**
  - U.S. Banks: 0%
  - U.S. Credit: 17%
  - Canada Banks and Credit Lenders: 0%
- **Within the next 24 months**
  - U.S. Banks: 0%
  - U.S. Credit: 6%
  - Canada Banks and Credit Lenders: 19%
- **Beyond the next 24 months**
  - U.S. Banks: 0%
  - U.S. Credit: 14%
  - Canada Banks and Credit Lenders: 17%
Key Finding 4
BUY NOW, PAY LATER CREATING CHALLENGES TO FRAUD DETECTION/PREVENTION

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)

<table>
<thead>
<tr>
<th>U.S. Banks</th>
<th>U.S. Credit Lenders</th>
<th>Canada Banks &amp; Credit Lenders</th>
</tr>
</thead>
<tbody>
<tr>
<td>To a large degree</td>
<td>17%</td>
<td>15%</td>
</tr>
<tr>
<td>To a moderate degree</td>
<td>52%</td>
<td>28%</td>
</tr>
<tr>
<td>To some degree</td>
<td>24%</td>
<td>43%</td>
</tr>
<tr>
<td>Not at all</td>
<td>7%</td>
<td>9%</td>
</tr>
<tr>
<td>Not sure</td>
<td>2%</td>
<td>5%</td>
</tr>
</tbody>
</table>

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?

* Asked of those who currently offer point-of-sale BNPL credit.
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*  
(U.S. and Canada banks & 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.

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?

- High volume of transactions
- Difficulty in determining transaction location/origination
- Ensuring that payment service providers act in compliance with financial regulations
- Speed/real-time nature of value transfer
- Lack of consistency across payment applications
- Lack of information about payment service providers’ customers
- Volume of false positives that need to be reviewed

* 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.
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.

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.

<table>
<thead>
<tr>
<th>Method of Providing Access to Point-of-Sale Buy Now, Pay Later Credit</th>
<th>U.S. Banks</th>
<th>U.S. Credit</th>
<th>Canada Banks &amp; Credit Lenders</th>
</tr>
</thead>
<tbody>
<tr>
<td>In partnership with BNPL app providers</td>
<td>58%</td>
<td>57%</td>
<td>65%</td>
</tr>
<tr>
<td>In partnership with credit institutions</td>
<td>66%</td>
<td>66%</td>
<td>56%</td>
</tr>
<tr>
<td>Through your own branded point of sale lending platform</td>
<td>15%</td>
<td>10%</td>
<td>14%</td>
</tr>
</tbody>
</table>
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.
Survey Questions: Q12a, Q12b, Q12c: For each specific customer journey stage, please indicate the percentage distribution your past 12-month’s fraud losses across the following fraud methods.

<table>
<thead>
<tr>
<th></th>
<th>U.S. Financial Services</th>
<th>U.S. Lending</th>
<th>Canada Financial Services</th>
<th>Canada Lending</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Banks</td>
<td>Investment Firms</td>
<td>Credit Lenders</td>
<td>Mortgage Lenders</td>
</tr>
<tr>
<td></td>
<td>New Account Creation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td>40% 40% 20%</td>
<td>39% 40% 22%</td>
<td>40% 41% 19%</td>
<td>43% 38% 19%</td>
</tr>
<tr>
<td>2022</td>
<td>39% 41% 20%</td>
<td>38% 40% 22%</td>
<td>39% 42% 19%</td>
<td>35% 47% 18%</td>
</tr>
<tr>
<td></td>
<td>Distribution of Funds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td>41% 41% 19%</td>
<td>37% 41% 22%</td>
<td>42% 40% 18%</td>
<td>42% 38% 20%</td>
</tr>
<tr>
<td>2022</td>
<td>40% 40% 20%</td>
<td>38% 42% 20%</td>
<td>40% 39% 21%</td>
<td>40% 38% 20%</td>
</tr>
<tr>
<td></td>
<td>Account Login</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td>42% 37% 21%</td>
<td>36% 43% 21%</td>
<td>38% 42% 20%</td>
<td>41% 37% 22%</td>
</tr>
<tr>
<td>2022</td>
<td>42% 37% 21%</td>
<td>36% 43% 21%</td>
<td>40% 39% 21%</td>
<td>40% 39% 18%</td>
</tr>
</tbody>
</table>

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

Key Finding 5
INCREASED LOSSES DUE TO IDENTITY- AND ACCOUNT-RELATED FRAUD ACROSS THE CUSTOMER JOURNEY

= significantly or directionally higher/lower than previous period
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?

<table>
<thead>
<tr>
<th>Activity</th>
<th>U.S. Financial Services</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution of funds</td>
<td>34%</td>
<td>35%</td>
<td>34%</td>
<td>35%</td>
</tr>
<tr>
<td>With account takeover</td>
<td>32%</td>
<td>48%</td>
<td>37%</td>
<td>56%</td>
</tr>
<tr>
<td>At point of new account creation</td>
<td>33%</td>
<td>13%</td>
<td>18%</td>
<td>13%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activity</th>
<th>U.S. Lending</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution of funds</td>
<td>34%</td>
<td>35%</td>
<td>33%</td>
<td>35%</td>
</tr>
<tr>
<td>With account takeover</td>
<td>33%</td>
<td>45%</td>
<td>29%</td>
<td>45%</td>
</tr>
<tr>
<td>At point of new account creation</td>
<td>33%</td>
<td>24%</td>
<td>29%</td>
<td>13%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activity</th>
<th>Canada Financial Services</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution of funds</td>
<td>33%</td>
<td>35%</td>
<td>30%</td>
<td>35%</td>
</tr>
<tr>
<td>With account takeover</td>
<td>30%</td>
<td>31%</td>
<td>37%</td>
<td>31%</td>
</tr>
<tr>
<td>At point of new account creation</td>
<td>37%</td>
<td>24%</td>
<td>24%</td>
<td>27%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activity</th>
<th>Canada Lending</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution of funds</td>
<td>32%</td>
<td>48%</td>
<td>24%</td>
<td>39%</td>
</tr>
<tr>
<td>With account takeover</td>
<td>32%</td>
<td>37%</td>
<td>27%</td>
<td>39%</td>
</tr>
<tr>
<td>At point of new account creation</td>
<td>27%</td>
<td>37%</td>
<td>37%</td>
<td>37%</td>
</tr>
</tbody>
</table>
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%).
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 ACROSS THE CUSTOMER JOURNEY

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

<table>
<thead>
<tr>
<th>Key Finding 6</th>
<th>FRAUD MITIGATION SOLUTIONS USE ACROSS THE CUSTOMER JOURNEY</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>There is, however, a sizeable majority that is not using these solutions.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Solution Type</th>
<th>U.S. Lending</th>
<th>US Credit Lenders</th>
<th>US Mortgage Lenders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Verification and Transaction Solutions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification of Checks</td>
<td>16%</td>
<td>20%</td>
<td>18%</td>
</tr>
<tr>
<td>Authentication Using Payment Instrument</td>
<td>25%</td>
<td>22%</td>
<td>21%</td>
</tr>
<tr>
<td>Name Address DDB Verification</td>
<td>51%</td>
<td>63%</td>
<td>61%</td>
</tr>
<tr>
<td>Positive &amp; Negative Lists</td>
<td>65%</td>
<td>71%</td>
<td>55%</td>
</tr>
<tr>
<td>Gov’t issued ID</td>
<td>9%</td>
<td>13%</td>
<td>17%</td>
</tr>
</tbody>
</table>

**Active/Interactive Authentication by . . .**

<table>
<thead>
<tr>
<th>Challenge Questions</th>
<th>Quiz or KBA</th>
<th>OTP/Two-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate</td>
<td>12%</td>
<td>17%</td>
</tr>
<tr>
<td>Using Behavioral Biometrics</td>
<td>20%</td>
<td>21%</td>
</tr>
<tr>
<td>Email Risk &amp; Verification</td>
<td>30%</td>
<td>46%</td>
</tr>
<tr>
<td>Phone # Risk &amp; Verification</td>
<td>38%</td>
<td>40%</td>
</tr>
<tr>
<td>Browser/ Malware Tracking</td>
<td>17%</td>
<td>17%</td>
</tr>
<tr>
<td>Geolocation Device ID</td>
<td>12%</td>
<td>15%</td>
</tr>
<tr>
<td>Real-Time Fraud Detection</td>
<td>25%</td>
<td>21%</td>
</tr>
<tr>
<td>Automated Transaction Scoring</td>
<td>14%</td>
<td>22%</td>
</tr>
</tbody>
</table>

**Passive/Digital Identity-based**

<table>
<thead>
<tr>
<th>Email Risk &amp; Verification</th>
<th>Phone # Risk &amp; Verification</th>
<th>Browser/ Malware Tracking</th>
<th>Geolocation Device ID</th>
<th>Real-Time Fraud Detection</th>
<th>Automated Transaction Scoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>68%</td>
<td>66%</td>
<td>62%</td>
<td>61%</td>
<td>22%</td>
<td>25%</td>
</tr>
<tr>
<td>62%</td>
<td>66%</td>
<td>65%</td>
<td>62%</td>
<td>17%</td>
<td>15%</td>
</tr>
<tr>
<td>38%</td>
<td>40%</td>
<td>14%</td>
<td>17%</td>
<td>16%</td>
<td>21%</td>
</tr>
<tr>
<td>17%</td>
<td>14%</td>
<td>16%</td>
<td>15%</td>
<td>21%</td>
<td>19%</td>
</tr>
<tr>
<td>22%</td>
<td>30%</td>
<td>20%</td>
<td>24%</td>
<td>14%</td>
<td>25%</td>
</tr>
<tr>
<td>15%</td>
<td>24%</td>
<td>10%</td>
<td>30%</td>
<td>21%</td>
<td>25%</td>
</tr>
<tr>
<td>13%</td>
<td>16%</td>
<td>21%</td>
<td>21%</td>
<td>21%</td>
<td>19%</td>
</tr>
<tr>
<td>12%</td>
<td>12%</td>
<td>12%</td>
<td>12%</td>
<td>12%</td>
<td>12%</td>
</tr>
<tr>
<td>24%</td>
<td>24%</td>
<td>24%</td>
<td>24%</td>
<td>21%</td>
<td>21%</td>
</tr>
<tr>
<td>21%</td>
<td>21%</td>
<td>21%</td>
<td>21%</td>
<td>21%</td>
<td>21%</td>
</tr>
<tr>
<td>19%</td>
<td>19%</td>
<td>19%</td>
<td>19%</td>
<td>19%</td>
<td>19%</td>
</tr>
<tr>
<td>21%</td>
<td>21%</td>
<td>21%</td>
<td>21%</td>
<td>21%</td>
<td>21%</td>
</tr>
</tbody>
</table>

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

- **New Accounts Login 2022**
  - Verification of Checks: 16%
  - Authentication Using Payment Instrument: 25%
  - Name Address DDB Verification: 51%
  - Positive & Negative Lists: 65%
  - Gov’t issued ID: 9%

- **New Accounts Login 2021**
  - Verification of Checks: 27%
  - Authentication Using Payment Instrument: 10%
  - Name Address DDB Verification: 34%
  - Positive & Negative Lists: 23%
  - Gov’t issued ID: 21%

- **Distribution of Funds 2022**
  - Verification of Checks: 16%
  - Authentication Using Payment Instrument: 58%
  - Name Address DDB Verification: 74%
  - Positive & Negative Lists: 10%
  - Gov’t issued ID: 21%

- **Distribution of Funds 2021**
  - Verification of Checks: 24%
  - Authentication Using Payment Instrument: 33%
  - Name Address DDB Verification: 29%
  - Positive & Negative Lists: 19%
  - Gov’t issued ID: 22%

- **Account Login 2022**
  - Verification of Checks: 16%
  - Authentication Using Payment Instrument: 61%
  - Name Address DDB Verification: 61%
  - Positive & Negative Lists: 11%
  - Gov’t issued ID: 25%

- **Account Login 2021**
  - Verification of Checks: 17%
  - Authentication Using Payment Instrument: 20%
  - Name Address DDB Verification: 30%
  - Positive & Negative Lists: 13%
  - Gov’t issued ID: 21%

- **Key Findings**
  - Fraud Mitigation Solutions Use across the Customer Journey
  - Overview
  - Key Findings
  - Trends/Landscape
  - Attacks & Costs
  - Scams Impacting Customer Journey Risks
  - BNPL Impact on Fraud Detection
  - Identity-related Fraud
  - Risk Mitigation Smart Practices
  - Recommendations

- **Advanced Transaction Verification Solutions**
  - Real-Time Fraud Detection
  - Automated Transaction Scoring
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.

### Key Finding 6

**FRAUD MITIGATION SOLUTIONS USE ACROSS THE CUSTOMER JOURNEY**

<table>
<thead>
<tr>
<th>Survey Question: Q27: Which fraud detection/mitigation solutions does your company currently use for the following transaction or customer journey points?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

#### Basic Verification and Transaction Solutions

<table>
<thead>
<tr>
<th>Solution</th>
<th>2022</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification of Checks</td>
<td>20%</td>
<td>15%</td>
</tr>
<tr>
<td>Authentication Using Payment Instrument</td>
<td>34%</td>
<td>32%</td>
</tr>
<tr>
<td>Name Address DOB Verification</td>
<td>65%</td>
<td>65%</td>
</tr>
<tr>
<td>Positive &amp; Negative Lists</td>
<td>58%</td>
<td>38%</td>
</tr>
<tr>
<td>Government-issued ID</td>
<td>16%</td>
<td>14%</td>
</tr>
<tr>
<td>Gov’t issued ID</td>
<td>10%</td>
<td>14%</td>
</tr>
<tr>
<td>Challenge Questions</td>
<td>8%</td>
<td>20%</td>
</tr>
<tr>
<td>Quiz or KBA</td>
<td>14%</td>
<td>22%</td>
</tr>
<tr>
<td>OTP/Two-Factor</td>
<td>56%</td>
<td>64%</td>
</tr>
</tbody>
</table>

#### Advanced Identity Authentication Solutions

<table>
<thead>
<tr>
<th>Solution</th>
<th>2022</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Using Behavioral Biometrics</td>
<td>19%</td>
<td>18%</td>
</tr>
<tr>
<td>Authentication Using Biometrics</td>
<td>25%</td>
<td>26%</td>
</tr>
<tr>
<td>Email Risk &amp; Verification</td>
<td>34%</td>
<td>36%</td>
</tr>
<tr>
<td>Phone # Risk &amp; Verification</td>
<td>71%</td>
<td>39%</td>
</tr>
<tr>
<td>Browser/ Malware Tracking</td>
<td>39%</td>
<td>73%</td>
</tr>
<tr>
<td>Geolocation Device ID</td>
<td>32%</td>
<td>35%</td>
</tr>
</tbody>
</table>

#### Active/Interactive

<table>
<thead>
<tr>
<th>Solution</th>
<th>2022</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavioral Biometrics</td>
<td>25%</td>
<td>26%</td>
</tr>
<tr>
<td>Biometrics</td>
<td>34%</td>
<td>36%</td>
</tr>
<tr>
<td>Email Risk &amp; Verification</td>
<td>18%</td>
<td>17%</td>
</tr>
<tr>
<td>Phone # Risk &amp; Verification</td>
<td>35%</td>
<td>30%</td>
</tr>
</tbody>
</table>

#### Passive/Digital Identity-based

<table>
<thead>
<tr>
<th>Solution</th>
<th>2022</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavioral Biometrics</td>
<td>34%</td>
<td>35%</td>
</tr>
<tr>
<td>Biometrics</td>
<td>18%</td>
<td>17%</td>
</tr>
<tr>
<td>Email Risk &amp; Verification</td>
<td>29%</td>
<td>28%</td>
</tr>
<tr>
<td>Phone # Risk &amp; Verification</td>
<td>34%</td>
<td>23%</td>
</tr>
</tbody>
</table>

#### New Accounts 2022

<table>
<thead>
<tr>
<th>Solution</th>
<th>2022</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification of Checks</td>
<td>20%</td>
<td>15%</td>
</tr>
<tr>
<td>Authentication Using Payment Instrument</td>
<td>34%</td>
<td>32%</td>
</tr>
<tr>
<td>Name Address DOB Verification</td>
<td>65%</td>
<td>65%</td>
</tr>
<tr>
<td>Positive &amp; Negative Lists</td>
<td>58%</td>
<td>38%</td>
</tr>
<tr>
<td>Government-issued ID</td>
<td>16%</td>
<td>14%</td>
</tr>
<tr>
<td>Gov’t issued ID</td>
<td>10%</td>
<td>14%</td>
</tr>
<tr>
<td>Challenge Questions</td>
<td>8%</td>
<td>20%</td>
</tr>
<tr>
<td>Quiz or KBA</td>
<td>14%</td>
<td>22%</td>
</tr>
<tr>
<td>OTP/Two-Factor</td>
<td>56%</td>
<td>64%</td>
</tr>
</tbody>
</table>

#### Account Login 2022

<table>
<thead>
<tr>
<th>Solution</th>
<th>2022</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification of Checks</td>
<td>20%</td>
<td>15%</td>
</tr>
<tr>
<td>Authentication Using Payment Instrument</td>
<td>34%</td>
<td>32%</td>
</tr>
<tr>
<td>Name Address DOB Verification</td>
<td>65%</td>
<td>65%</td>
</tr>
<tr>
<td>Positive &amp; Negative Lists</td>
<td>58%</td>
<td>38%</td>
</tr>
<tr>
<td>Government-issued ID</td>
<td>16%</td>
<td>14%</td>
</tr>
<tr>
<td>Gov’t issued ID</td>
<td>10%</td>
<td>14%</td>
</tr>
<tr>
<td>Challenge Questions</td>
<td>8%</td>
<td>20%</td>
</tr>
<tr>
<td>Quiz or KBA</td>
<td>14%</td>
<td>22%</td>
</tr>
<tr>
<td>OTP/Two-Factor</td>
<td>56%</td>
<td>64%</td>
</tr>
</tbody>
</table>

#2

**Attacks & Costs**

**Scams Impacting Customer Journey Risks**

**BNPL Impact on Fraud Detection**

**Identity-related Fraud**

**Risk Mitigation Smart Practices**

**Recommendations**

---

*Note: A significantly or directionally higher than previous period is indicated by a symbol.*
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**

For the following transaction or customer journey points:

- **Basic Verification and Transaction Solutions**
  - Verification of Checks
  - Authenticate Using Payment Instrument
  - Name Address
  - Positive & Negative Lists
  - Gov’t issued ID

- **Active/Interactive**
  - Challenge Questions
  - Quiz or KBA
  - OTP/Two-Factor

- **Advanced Identity Authentication Solutions**
  - Authenticate Using Behavioral Biometrics
  - Email Risk & Verification
  - Phone # Risk & Verification

- **Passive/Digital Identity-based**
  - Browser/Malware Tracking
  - Geolocation

- **Real-Time Fraud Detection**
  - Automated Transaction Scoring

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

- **2022**
  - Experience 1 or No Scams
  - Experience 3+ Scam Types

- **Key Finding 6**

**FRAUD MITIGATION SOLUTIONS USE AT NEW ACCOUNT CREATION**

#6

- **Key Findings**
- **Survey Question**
- **Recommendations**
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

<table>
<thead>
<tr>
<th>% Firms Using Solution at Account Creation</th>
<th>Firms with Limited Digital Solutions Use</th>
<th>Firms with Multi-Layered Digital Solutions Use Involving Biometrics*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email risk and verification</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>Authentication using challenge questions</td>
<td>30%</td>
<td>87%</td>
</tr>
<tr>
<td>Authentication using quiz or KBA</td>
<td>27%</td>
<td>84%</td>
</tr>
<tr>
<td>Geolocation</td>
<td>23%</td>
<td>74%</td>
</tr>
<tr>
<td>Phone number risk and verification</td>
<td>26%</td>
<td>70%</td>
</tr>
<tr>
<td>Authentication using behavioral biometrics</td>
<td>18%</td>
<td>66%</td>
</tr>
</tbody>
</table>

**% Indicating Top Online Channel Challenge**
- Email/device verification (34%)
- Address verification (39%)

**% Indicating Top Mobile Channel Challenge**
- Email/device verification (37%)
- Address verification (38%)
- Phone # verification (55%)

**Every $1 of fraud loss at Account Creation actually costs**
- $4.28
- $3.69

* 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.
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

<table>
<thead>
<tr>
<th>Solution Approach</th>
<th>Firms Limited Digital Solutions Use</th>
<th>Firms Multi-Layered Digital Solutions Use Involving Biometrics*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email risk and verification</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>Automated transaction scoring</td>
<td>18%</td>
<td>76%</td>
</tr>
<tr>
<td>Authentication using behavioral biometrics</td>
<td>26%</td>
<td>76%</td>
</tr>
<tr>
<td>Authentication using biometrics</td>
<td>16%</td>
<td>73%</td>
</tr>
<tr>
<td>Authentication using OTP/2 Factor</td>
<td>0%</td>
<td>68%</td>
</tr>
<tr>
<td>Device ID/Device fingerprinting</td>
<td>23%</td>
<td>57%</td>
</tr>
</tbody>
</table>

### % Indicating Top Online Channel Challenge
- Manual reviews (35%)
- Balancing fraud detection with friction (31%)

### % Indicating Top Mobile Channel Challenge
- Email/device verification (36%)
- Determining origination (37%)
- Balancing fraud detection with friction (31%)

### 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.
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**

<table>
<thead>
<tr>
<th>% Firms Using Solution at Distribution of Funds</th>
<th>Firms with Limited Digital Solutions Use</th>
<th>Firms with Multi-Layered Digital Solutions Use Involving Biometrics*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email risk and verification</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>Authentication using biometrics</td>
<td>28%</td>
<td>80%</td>
</tr>
<tr>
<td>Authentication using OTP/2 Factor</td>
<td>0%</td>
<td>79%</td>
</tr>
<tr>
<td>Device ID/Device fingerprinting</td>
<td>21%</td>
<td>76%</td>
</tr>
<tr>
<td>Phone # risk &amp; verification</td>
<td>23%</td>
<td>68%</td>
</tr>
<tr>
<td>Real-time transaction tracking tools</td>
<td>25%</td>
<td>41%</td>
</tr>
</tbody>
</table>

% Indicating Top Online Channel Challenge:
- Identifying bots from humans (35%)
- Phone # verification (34%)

% Indicating Top Mobile Channel Challenge:
- Manual reviews (30%)
- Determining origination (36%)
- Balancing fraud detection with friction (29%)

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

**Fraud Detection and Prevention Solution Layering**

- **Address both identity and transaction fraud risks**
- **Tackle different challenges and risks for mobile versus online**
- **Authenticate both the user and the device since botnets and malware can compromise mobile devices**
- **Mitigate the different risks of selling digital versus physical goods**

**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 Tools and Capabilities with Fraud Prevention Approach**

- Cybersecurity Alerts
- Social Media Intelligence
- AI/ML Models
- Crowdsourcing
- Cybersecurity Operations
- Digital/Customer Experience Operations
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.
Mid/large U.S. investment firms and credit lenders are particularly likely to use the FraudClassifier℠ 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.
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.

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?

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.
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**

<table>
<thead>
<tr>
<th>Financial Services</th>
<th>U.S.</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution of Funds</td>
<td>44%</td>
<td>31%</td>
<td>51%</td>
</tr>
<tr>
<td>New Account Creation</td>
<td>47%</td>
<td>3%</td>
<td>61%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Investment Firms</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution of Funds</td>
<td>56%</td>
<td>66%</td>
</tr>
<tr>
<td>New Account Creation</td>
<td>48%</td>
<td>61%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>U.S. Lending</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution of Funds</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>New Account Creation</td>
<td>33%</td>
<td>50%</td>
</tr>
</tbody>
</table>

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/lower than previous period

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

$ = significantly or directionally higher/lower than previous period
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.
Compared to 2021, more financial institutions have achieved full integration of cybersecurity operations with fraud prevention efforts.

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

- **Fully integrated**
- **Partially integrated**
- **Net: Not integrated**

### U.S. Financial Services
- 2021:
  - Banks: S = 35%, M/L = 50%
  - Investment Firms: S = 52%
  - Credit Lenders: S = 49%
  - Mortgage Lenders: S = 50%

### U.S. Lending
- 2021:
  - Banks: S = 36%, M/L = 48%
  - Investment Firms: S = 43%
  - Credit Lenders: S = 49%
  - Mortgage Lenders: S = 50%

### Canada Financial Services
- 2021:
  - U.S. Lending: S = 36%
  - Canada Lending: S = 56%

### Scans of integrations:
- Net: Not integrated
- Fully integrated
- Partially integrated
- 2021
- 2020

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

<table>
<thead>
<tr>
<th>Capability</th>
<th>U.S. Financial Services</th>
<th>U.S. Lending</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social media intelligence</td>
<td>34% (2021) / 35% (2020)</td>
<td>26% (2021) / 30% (2020)</td>
</tr>
<tr>
<td>Cybersecurity alerts</td>
<td>37% (2021) / 50% (2020)</td>
<td>31% (2021) / 73% (2020)</td>
</tr>
<tr>
<td>Crowdsourcing</td>
<td>29% (2021) / 34% (2020)</td>
<td>36% (2021) / 44% (2020)</td>
</tr>
<tr>
<td>AI/ML models</td>
<td>38% (2021) / 26% (2020)</td>
<td>31% (2021) / 37% (2020)</td>
</tr>
</tbody>
</table>

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.
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.

Integration of Cybersecurity, Digital Experience with Fraud Ops: 
- Not Using Smart Practice Approach: No
- Fully Using Smart Practice Approach: Yes

Focus on Optimizing Fraud Risk-to-Friction Levels:
- Not Using Smart Practice Approach: No
- Fully Using Smart Practice Approach: Yes

Solution(s) to verify physical attributes (e.g., Name, DOB, Address):
- Not Using Smart Practice Approach: Limited or None
- Fully Using Smart Practice Approach: ✔

Solution(s) to verify digital attributes (e.g., Email, phone # risk, biometrics):
- Not Using Smart Practice Approach: Limited or None
- Fully Using Smart Practice Approach: ✔

Solution(s) to assess device risk, location (e.g., Device ID, Geolocation):
- Not Using Smart Practice Approach: Limited or None
- Fully Using Smart Practice Approach: ✔

Solution(s) to assess behavior (e.g., Behavioral Biometrics, Transaction Risk):
- Not Using Smart Practice Approach: Limited or None
- Fully Using Smart Practice Approach: ✔

*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
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

- 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

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.

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

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.

Enter Credentials

Visit Website

Access Account

Multi-layered Solutions Approach

**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.

**Authenticated by biometrics; email/phone risk assessment—seamless risk assessment that minimizes customer effort and friction.**

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

**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. Breached data to account login since fraudsters deploy mass bot attacks, using breached data, to test passwords for account takeover.

**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

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

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

Multi-layered Solutions Approach

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

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

Active Identity Authentication
Use personal data known to the customer for authentication; or where a user provides two different authentication factors to verify themselves. Solution examples: Authentication by challenge, quiz or shared secrets; 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:


+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.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI/ML models</td>
<td>Mathematical algorithms that are “trained” using data and human expert input to replicate a decision an expert would make when provided that same information</td>
</tr>
<tr>
<td>Crowdsourcing</td>
<td>Collection of information, opinions or work from a group of people, usually sourced via the internet</td>
</tr>
<tr>
<td>Cybersecurity alerts</td>
<td>Notifications that specific attacks have been directed at an organization’s information systems</td>
</tr>
<tr>
<td>Integrated</td>
<td>Various parts or aspects linked or coordinated (e.g. integrating digital/CX operations with fraud prevention)</td>
</tr>
<tr>
<td>Mid/Large (M/L)</td>
<td>Mid/large companies earning at least $10 million in annual revenues</td>
</tr>
<tr>
<td>Rules-based approaches</td>
<td>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)</td>
</tr>
<tr>
<td>Scams</td>
<td>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</td>
</tr>
<tr>
<td>Smart practice multi-layered solutions approach</td>
<td>Using some combination of passive/digital identity-based solutions and those which assess physical identity attributes and transaction risk</td>
</tr>
<tr>
<td>Social media intelligence</td>
<td>Collective tools and solutions that allow organizations to analyze conversations, respond to social signals and synthesize social data points into meaningful trends and analysis</td>
</tr>
</tbody>
</table>
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. 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.

### Account Opening

**Credit Lending**
- **Verification**
  - Address (42%)
  - Email or device (36%)
  - Identity (36%)
- **Assessing risk by country (41%)**
- **Address verification (33%)**

**Mortgage Firms**
- **Verification**
  - Address (42%)
  - Email or device (36%)
  - Identity (36%)
- **Assessing risk by country (29%)**
- **Address verification (33%)**

### Account Login

**Credit Lending**
- **Verification**
  - Address (38%)
  - Phone (46%)
  - Email or device (35%)
- **Assessing risk by country (38%)**
- **Balancing fraud prevention friction (34%)**
- **Verification**
  - Address (38%)
  - Phone (46%)
  - Email or device (35%)

**Mortgage Firms**
- **Verification**
  - Address (30%)
  - Email or device (32%)
  - Identity (34%)
- **Balancing fraud prevention friction (36%)**
- **Assessing risk by country (38%)**
- **Verification**
  - Address (30%)
  - Email or device (32%)

### Distribution of Funds

**Credit Lending**
- **Verification**
  - Address (32%)
  - Phone (36%)
  - Email or device (36%)
  - Identity (33%)
- **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 (32%)

**Mortgage Firms**
- **Verification**
  - Address (30%)
  - Email or device (32%)
  - Identity (34%)
- **Knowing origination source (35%)**
- **Verification**
  - Address (30%)
  - Email or device (32%)

**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.
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.

### Key Finding 3
TOP ONLINE/MOBILE CHANNEL CHALLENGES ACROSS THE CUSTOMER JOURNEY

---

**Canadian Financial Services & Lending**

---

**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.