

LexisNexis® Risk Solutions
2020 True Cost of Fraud™ Study
Financial Services & Lending Report
US & Canada Edition



2020

TRUE COST OF FRAUD™
FINANCIAL SERVICES &
LENDING STUDY



Overview



Key Findings



Attacks & Costs



Trends



Challenges & Impacts



Potential COVID-19
Impacts



Solutions Use



Strategic Approaches



Recommendations

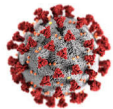
The LexisNexis® Risk Solutions True Cost of Fraud™ Study helps companies grow their businesses safely by navigating the growing risk of fraud.



This research provides a **snapshot of** current fraud trends in the United States and Canada.



It spotlights key pain points related to adding new payment mechanisms, transacting through online and mobile channels, & expanding internationally.



Where this report references pre vs. during COVID-19 time periods:

- Pre=Aug 2019 – Feb 2020
- During=March 2020 onward

Fraud Definitions



- Fraudulent transactions due to identity fraud, which is the misuse of stolen payments methods (such as credit cards) or personal information
- Fraudulent requests for refunds/returns, bounced checks
- Fraudulent 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™

- Estimates the total amount of loss a firm incurs based on the actual dollar value of a fraudulent transaction

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations

The study included a comprehensive survey of 500 risk and fraud executives in financial services and lending companies in the U.S. and Canada

Financial Services Companies Include:



- Retail/Commercial Banks
- Credit Unions



- Investments
- Trusts
- Wealth Management

Lending Institutions Include:



Auto Lenders



Finance Companies



Mortgage Companies



Non-Bank Credit Card Issuer



Non-Bank Personal Loan Issuer

Segment definitions



Small

Earns less than \$10 million in annual revenues



Mid/large

Earns \$10 million+ in annual revenues



Non-Digital

Less than 50% of transactions through the online and/or mobile channels



Digital

50% or more of transactions through the online and/or mobile channels

	Company Type		Size		Digital	
	Financial Services	Credit & Lending	Small (<\$10M)	Mid/Large (\$10M+)	Non-digital	Digital
# Completions	250	250	141	359	194	306

2020

TRUE COST OF FRAUD™
FINANCIAL SERVICES &
LENDING STUDY

Key Findings



Overview



Key Findings



#1

Attacks & Costs



#2

Trends



#3

Challenges & Impacts



#4

Potential COVID-19
Impacts



#5

Solutions Use

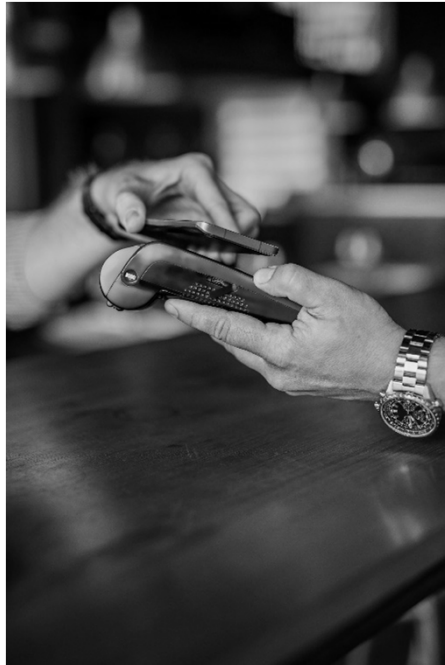


#6

Strategic Approaches



Recommendations



1

Attacks and Costs: Financial services and lending fraud continues to increase, impacting a broader set of mid/large firms most, including digital plus non-digital.

2

Trends: Key trends include increased fraud with mobile channel transactions, the rise of synthetic identity fraud, bot attacks and fraudulent creation of new accounts.

3

Challenges and Impacts: In addition to identity verification, the ability to balance fraud prevention with minimal customer friction is becoming harder as fraud becomes more digitally complex.

4

Potential COVID-19 Impacts: The COVID-19 pandemic has had a significantly negative impact on financial services and lending firms.

5

Solutions Use: As fraud becomes more sophisticated, there has been some adoption of solutions designed to address unique digital/online/mobile risks, though that is still limited for the most part.

6

Strategic Approaches: There is movement towards cloud-based solutions and the integration of cybersecurity, the digital customer experience and fraud prevention efforts.

2020

TRUE COST OF FRAUD™
FINANCIAL SERVICES &
LENDING STUDY



Overview



Key Findings



#1

Attacks & Costs



#2

Trends



#3

Challenges & Impacts



#4

Potential COVID-19
Impacts



#5

Solutions Use



#6

Strategic Approaches



Recommendations

Key Finding #1: Financial services and lending fraud continues to increase, impacting a broader set of mid/large firms most, including digital and non-digital.

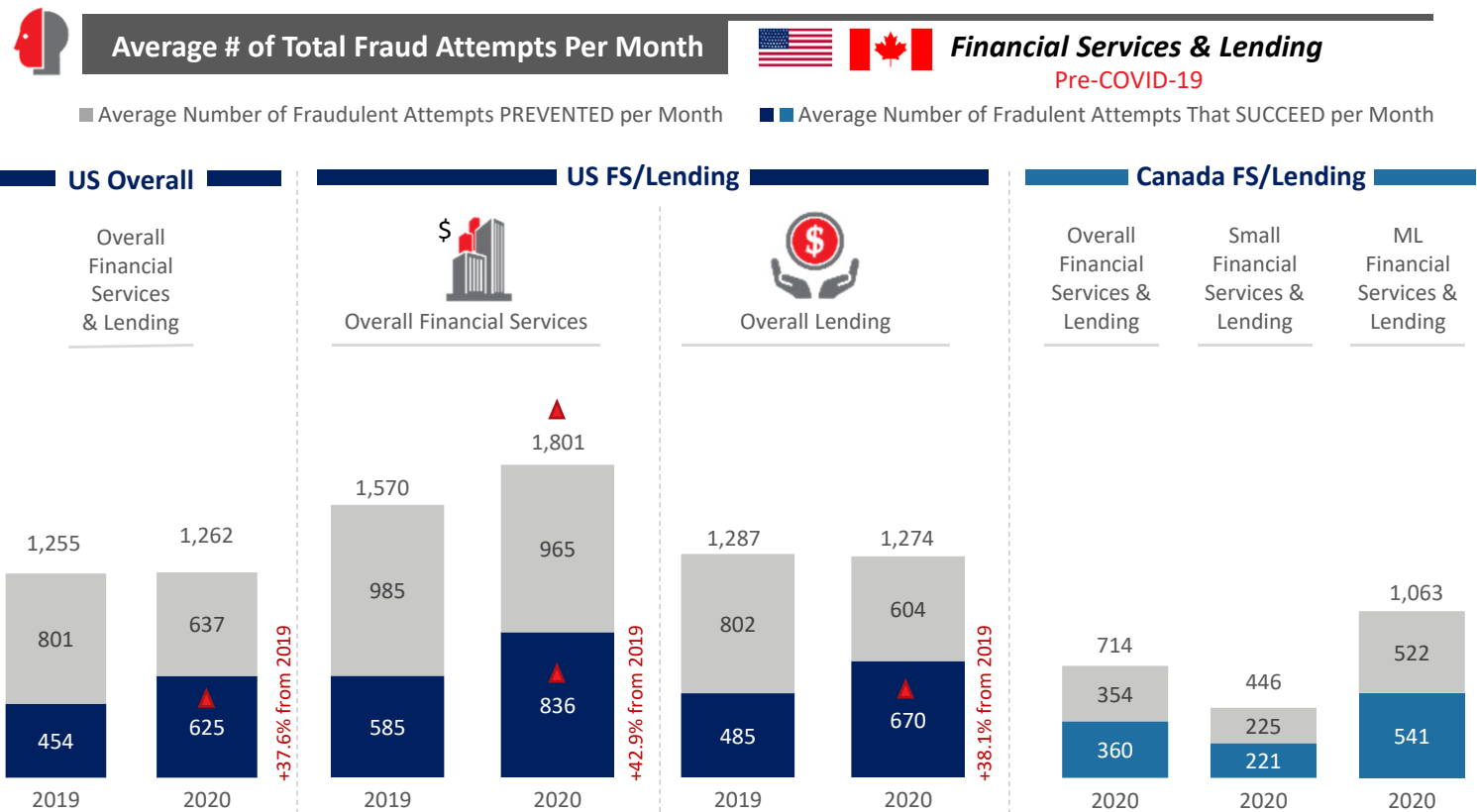


- The cost of pre-COVID-19 fraud among U.S. financial services and lending firms continues to rise at a similar double-digit rate as during the previous reporting period (2nd half 2018/1st half 2019). Lending firms continue to have somewhat higher costs than financial services firms.
- U.S. fraud costs are higher than for Canadian firms, though still high for the latter.
- The increased pre-COVID-19 cost of fraud aligns with significantly increased successful fraud attacks during the same reporting period.
- Mid/large digital firms get hit hardest, though fraud is also focusing on non-digital firms who are not far behind in terms of fraud costs and attack volumes.

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
#1	Attacks & Costs
#2	Trends
#3	Challenges & Impacts
#4	Potential COVID-19 Impacts
#5	Solutions Use
#6	Strategic Approaches
	Recommendations
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 successful monthly fraud attacks have increased significantly for U.S. financial services and lending firms.

This is a key indicator that fraud is becoming increasingly difficult to detect and prevent in these segments, as more sophisticated fraudsters are getting through fraud detection checkpoints. This occurs at a time when mobile banking options increase for consumers, including bill-to-mobile payments and adoption of a financial firm’s branded apps for transactions.



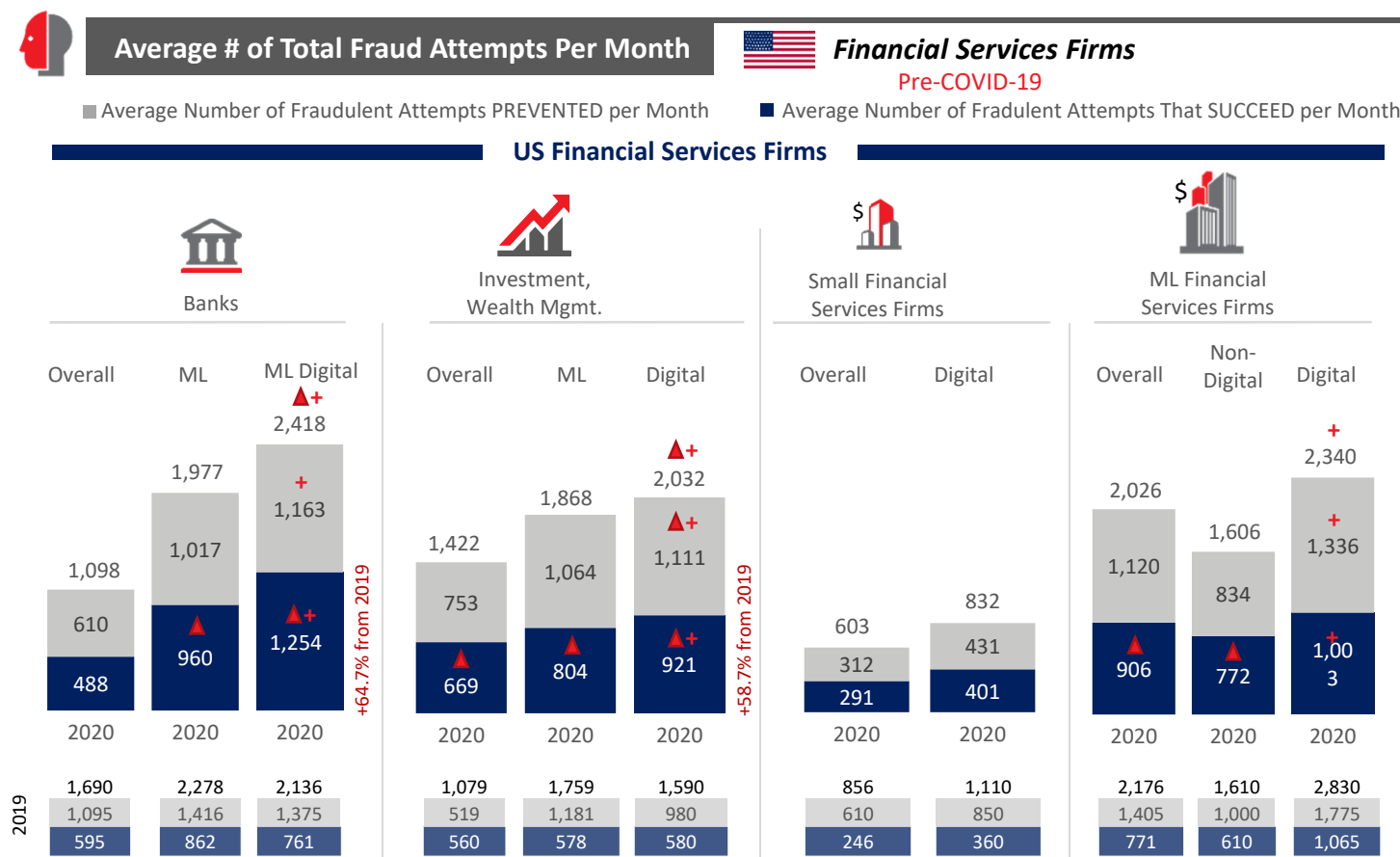
2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations

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?

Within U.S. financial services, mid/large and digital firms continue to experience sizeable fraud attack levels, including those which succeed.

Mid/large digital banks lead this ongoing trend from prior years, though to new levels.

But while the spike among non-digital firms has leveled off overall, they too are seeing an increase in successful attacks. It’s important to keep in mind that while non-digital firms (according to our definition) do not conduct the majority of business through remote channels, they nonetheless have a multi-channel business model that includes higher risk online and mobile transactions – and are often less likely to invest in risk mitigation solutions to address those specific risks.

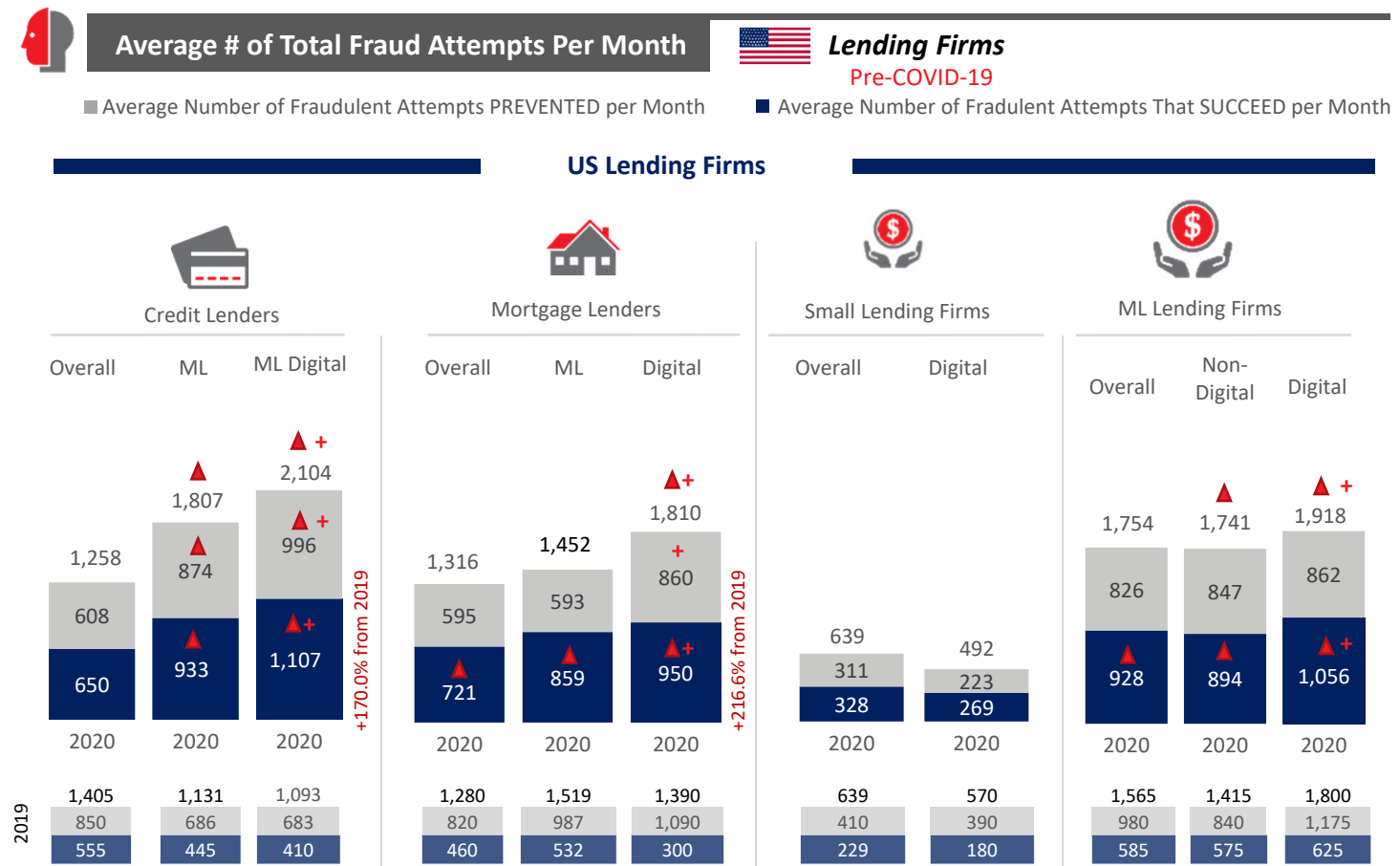


2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations

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?

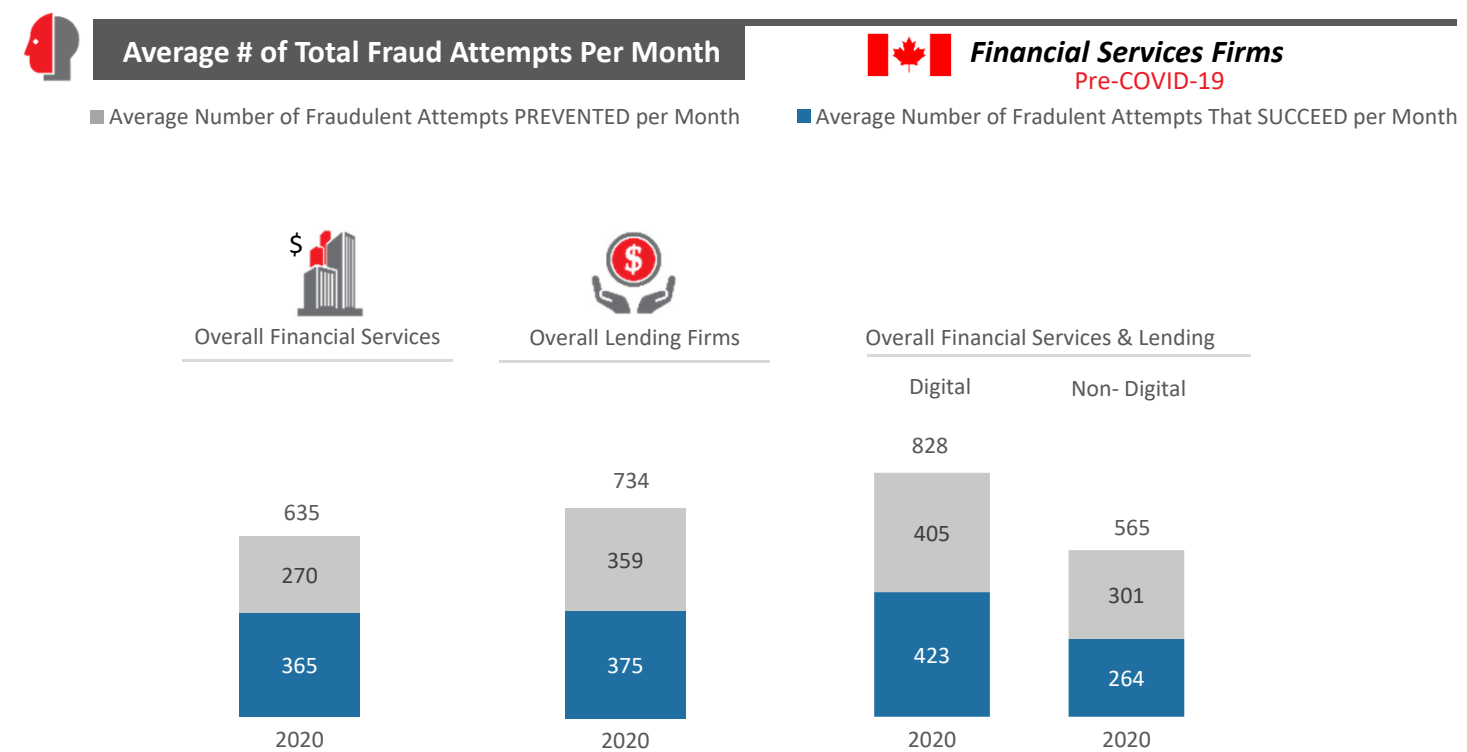
Successful fraud attacks continue to hit larger credit and mortgage lenders too, with sharp YOY increases. However, attacks have also broadened to focus on larger non-digital lenders as well.

As attacks grew among mid/large digital mortgage lenders during recent years, the level of attacks is catching up to mid/large digital credit lenders which have traditionally been more of a focus by fraudsters. Further, the level of fraud attacks is similar between larger digital and non-digital firms as the latter increases adoption of mobile channel transactions.



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
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 attack volumes are similar between Canadian financial services and lending firms, and higher for those with a digital business model.



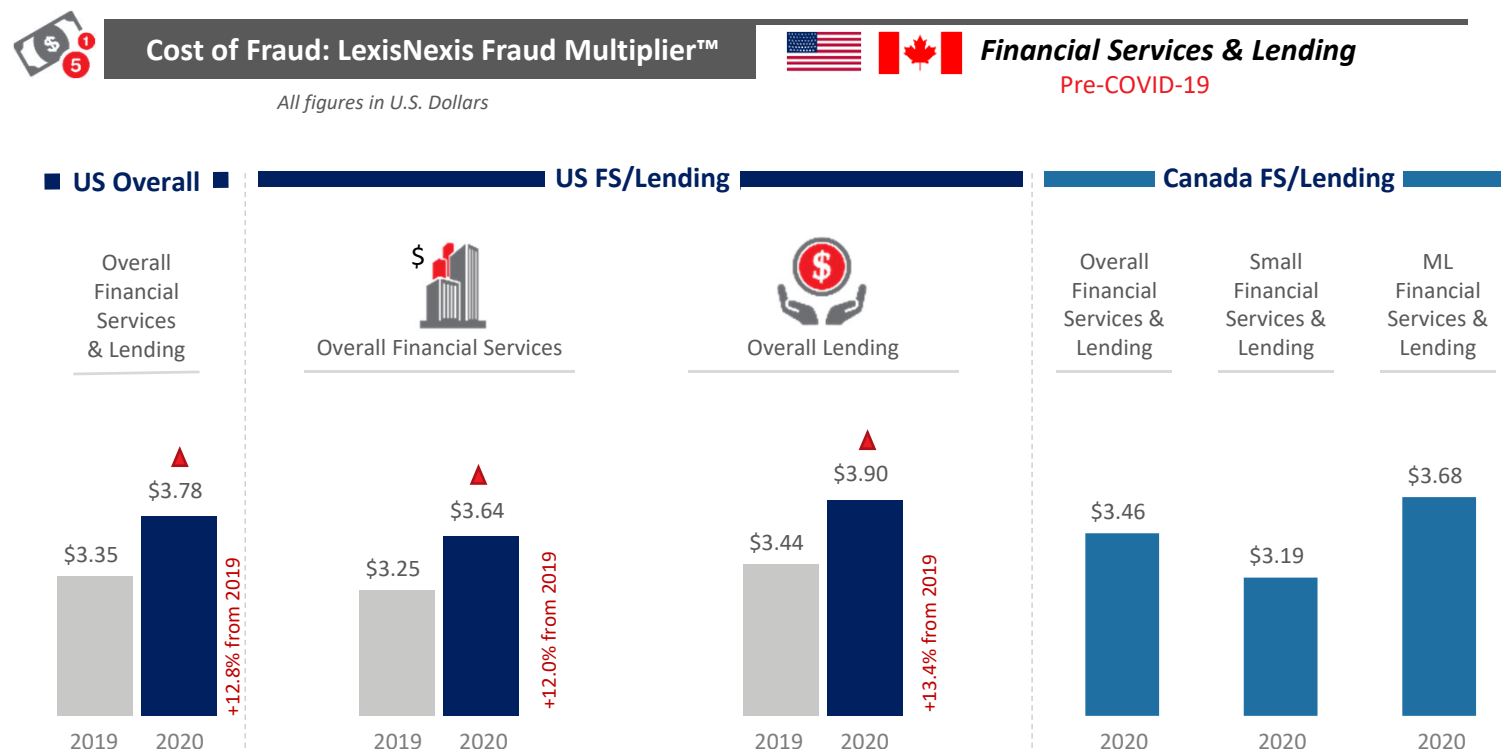
2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
<p>Survey Question: Q16a: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.</p>	

The pre-COVID-19 cost of fraud rose for U.S. financial services and lending firms at a similar rate (13%) as observed in 2018-19 (11% - 13%).

For every \$1 of fraud, it costs financial services firms \$3.64 compared to \$3.25 in late 2018/1st half 2019 (a 12.0% increase); fraud costs tend to be somewhat higher for lenders and have risen 13.4% (compared to 12.8% in the prior period), from \$3.44 to \$3.90 for every \$1 of fraud.

Such fraud costs involve losses related to the transaction face value for which firms are held liable, plus fees/interest incurred during applications/underwriting/processing stages, fines/legal fees, labor/investigation and external recovery expenses. In this case, there have been increases related to labor and external recovery support.

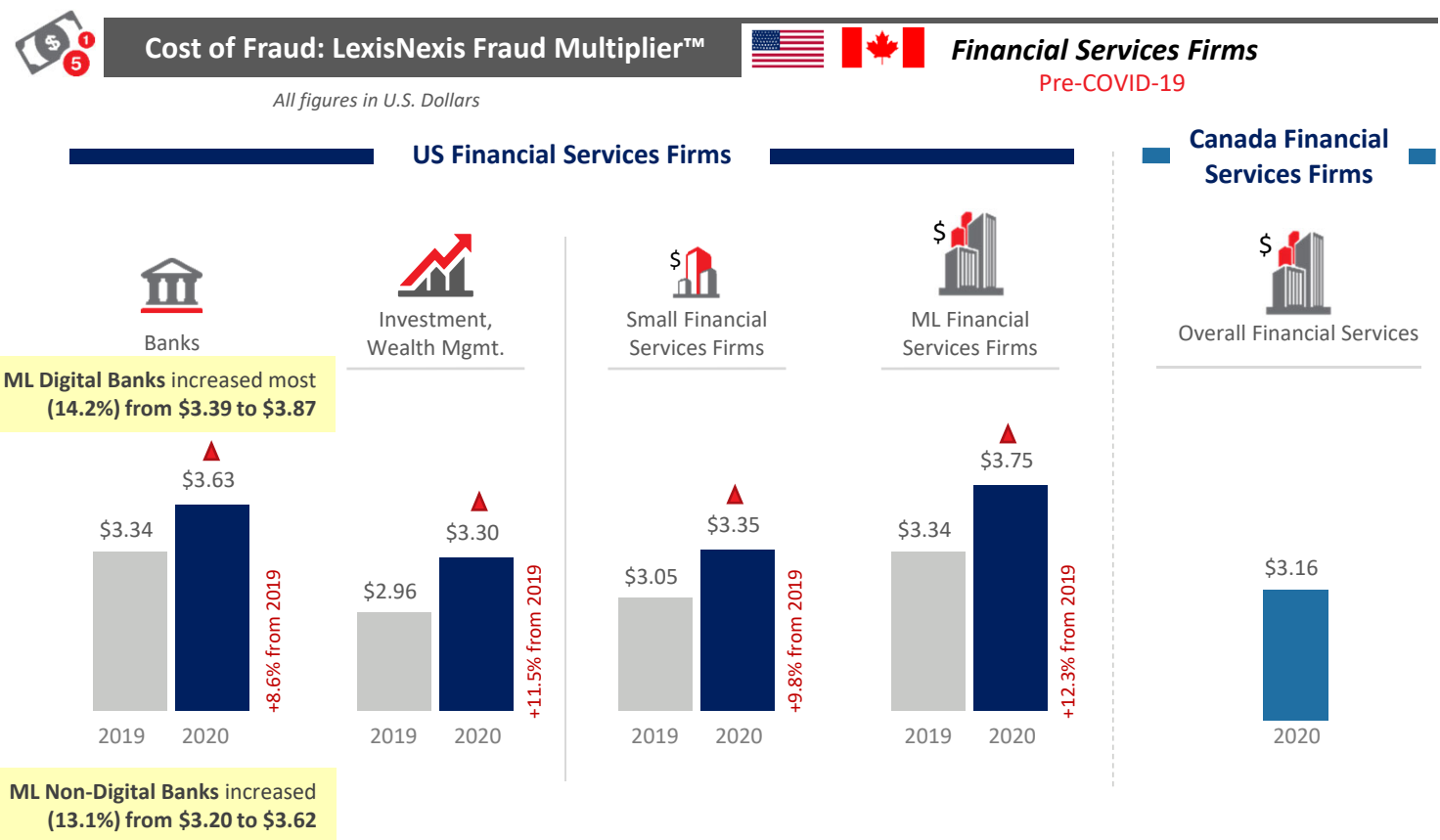
The cost of fraud is slightly lower for Canadian firms, but still at high levels for every \$1 of fraud.



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
<p>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.</p>	

Among U.S. financial services firms, mid/large digital banks have experienced the sharpest pre-COVID-19 fraud cost increases. However, even larger non-digital, multi-channel banks experienced sizeable increases as well.

Overall, every \$1 of fraud costs U.S. mid/large digital banks 14.2% more during second half 2019/early 2020 compared to the corresponding 2018-2019 period. There is a similar cost increase for mid/large non-digital banks. In both cases, increased costs are attributed to more labor for fraud detection and investigation, as well as with fees and interest during the underwriting process. There are challenges from mobile channel transactions and digital identity attributes that are contributing to these increases.

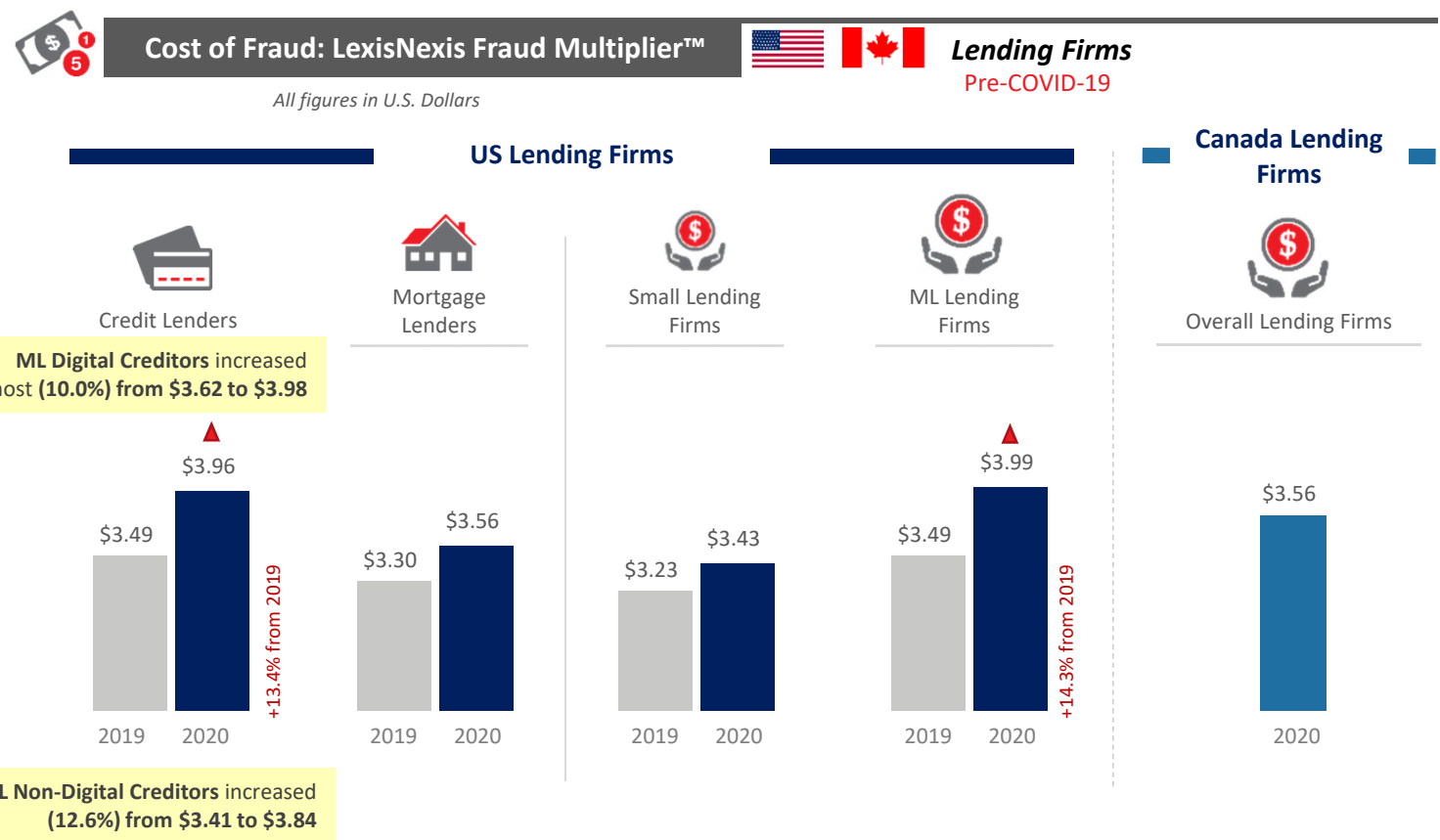


2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
#1	Attacks & Costs
#2	Trends
#3	Challenges & Impacts
#4	Potential COVID-19 Impacts
#5	Solutions Use
#6	Strategic Approaches
	Recommendations
Survey Question: Q16a: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.	

Among U.S. lending firms, both digital and non-digital mid/large credit lenders are experiencing the sharpest increases in pre-COVID-19 fraud costs.

Overall, every \$1 of fraud costs larger digital credit lenders \$3.98 during second half 2019/early 2020 compared to \$3.62 during the corresponding 2018-2019 period. The cost for larger non-digital credit lenders is close to this. As with larger banks, there mobile channel and digital identity challenges that are contributing to these increases.

The cost of fraud is much higher for Canadian lending firms compared to Canadian financial services organizations (\$3.56 vs. \$3.16).





Overview



Key Findings



#1

Attacks & Costs



#2

Trends



#3

Challenges & Impacts



#4

Potential COVID-19
Impacts

#5

Solutions Use



#6

Strategic Approaches



Recommendations

Key Finding #2: Key trends include increased fraud with mobile channel transactions, the rise of synthetic identity fraud, bot attacks and fraudulent creation of new accounts.



- The mobile channel is typically higher risk for fraud.
 - Successful fraud attacks have grown among those using this channel, at a somewhat higher rate compared to overall.
 - There is increased use of branded mobile apps and ability for consumers to use bill-to-mobile. This occurs at a time of reported increased cell phone account fraud and malware attacks on mobile devices.
 - The mobile channel accounts for somewhat more fraud costs compared to the previous reporting period.
- Identity-based fraud remains as a top factor for fraud losses. While the overall percentage of reported identity-based fraud has remained similar to the previous period, the amount that is linked to synthetic identity fraud has increased.
 - Account-based fraud remains the top identity-related fraud activity, particularly account takeover. However, the portion attributed to fraudulent new account creation has increased. This could be a result of increased cell phone account fraud.
- The above add to the challenge of dealing with increased botnet attacks.

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
<p>Survey Question: Q4: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment channels currently accepted by your company. Q6: Is your company considering accepting payments by mobile device over the next 12 months?</p>	

The percent of financial services and lending firms which offer mobile channel transactions remains high.

This continues the upward trend from previous years.



Use of the Mobile Channel

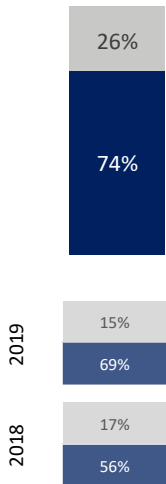


Financial Services & Lending

■ Considering M-commerce
■ Currently allow M-commerce

US Overall

Overall
Financial
Services
& Lending



US FS/Lending



Overall Financial Services

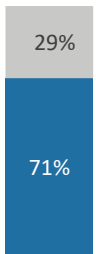


Overall Lending

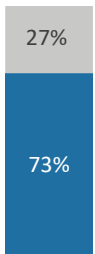


Canada FS/Lending

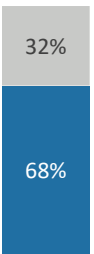
Overall
Financial
Services &
Lending



Small
Financial
Services &
Lending



ML
Financial
Services &
Lending

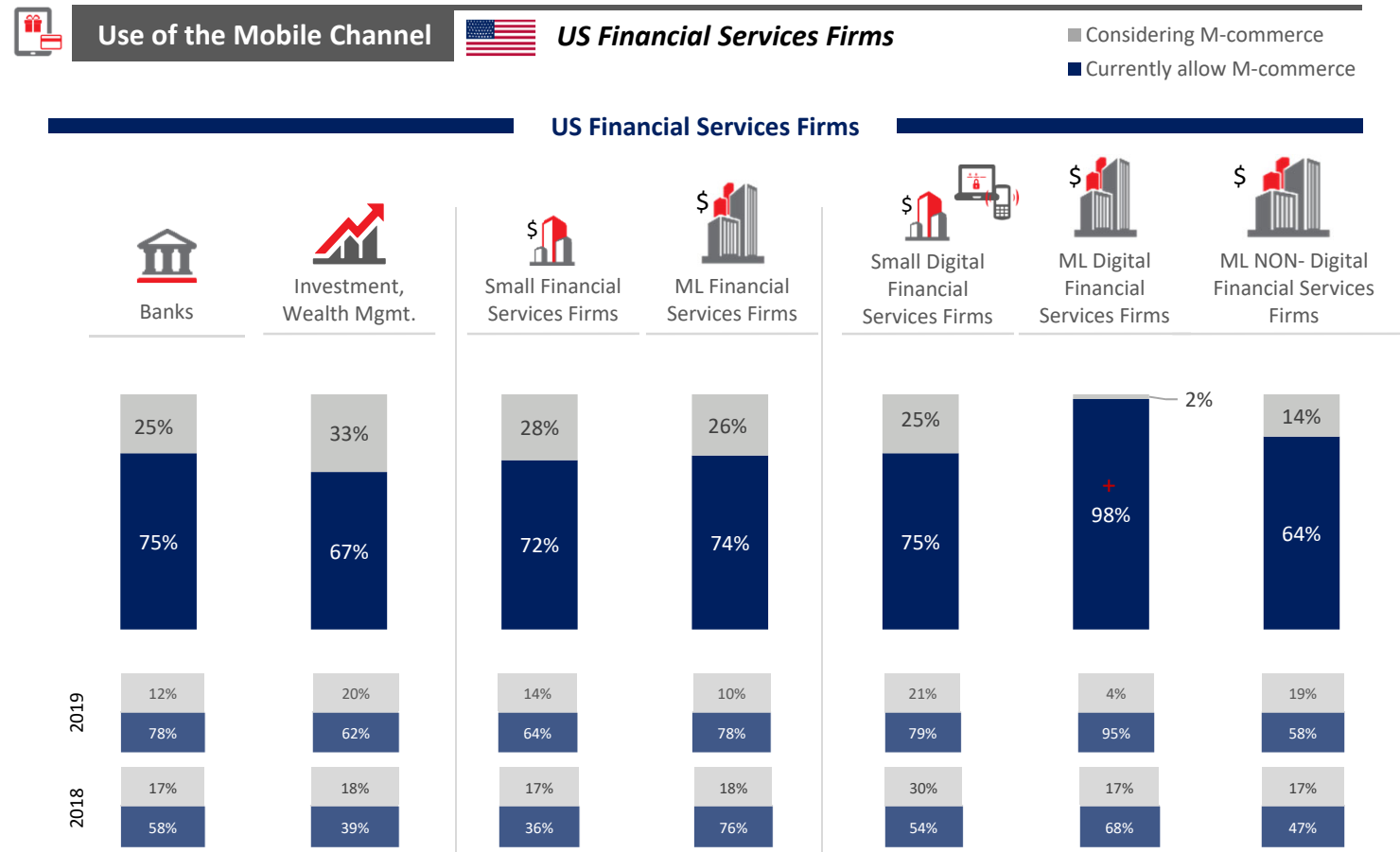


Somewhat more Canadian digital firms use the mobile channel (78%) compared to their non-digital counterparts (66%)

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
<p>Survey Question: Q4: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment channels currently accepted by your company. Q6: Is your company considering accepting payments by mobile device over the next 12 months?</p>	

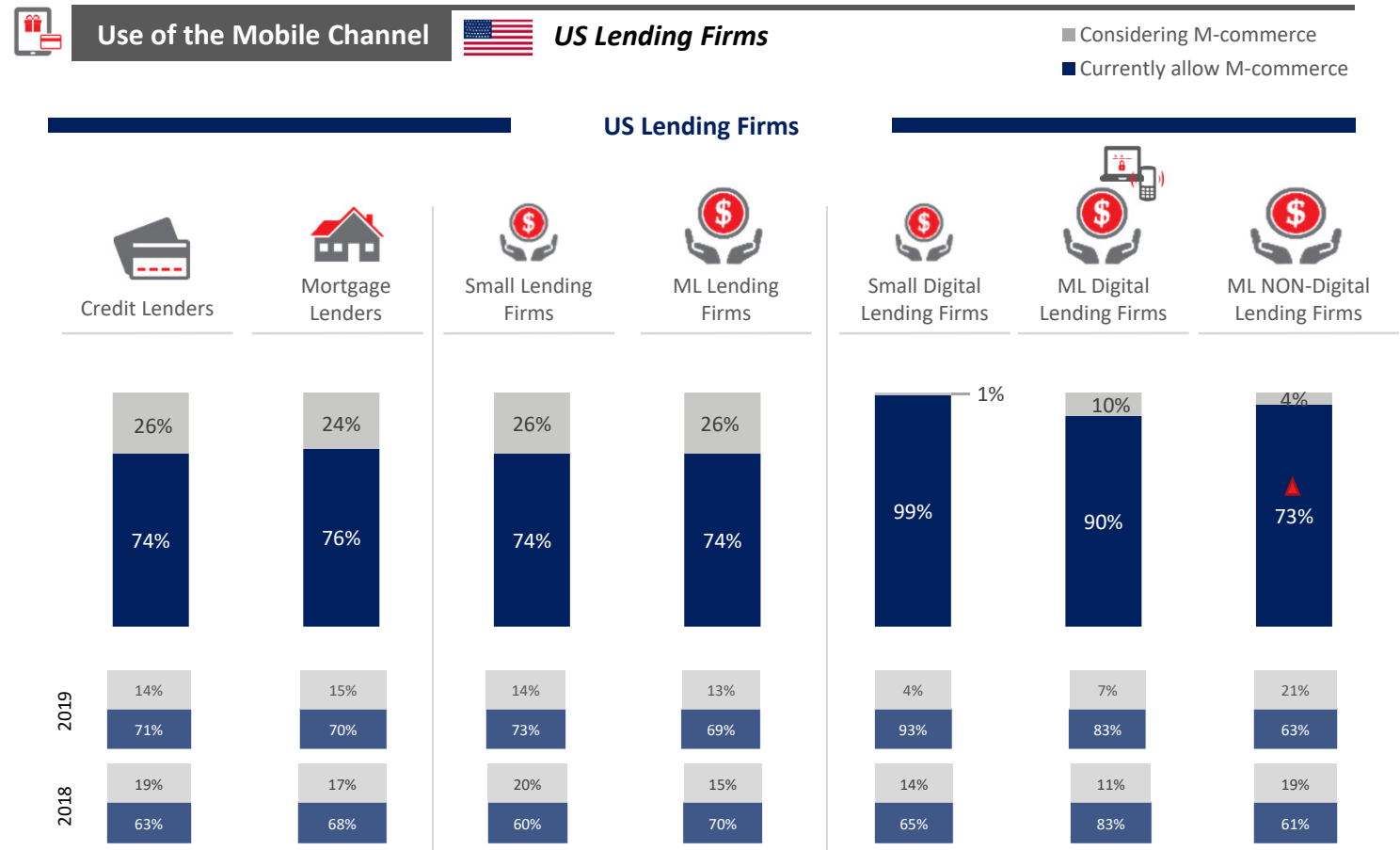
Digital U.S. financial services firms continue to lead the way towards mobile channel adoption, though non-digital firms are recognizing the need to add this to their multi-channel strategy.

There is a directional increase in mobile channel adoption among mid/large non-digital firms. But while doing so, many have not yet adopted risk mitigation solutions that are designed to address mobile channel risks that are unique from online and in-person transactions. This increases the risk of fraud and higher fraud costs.



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
<p>Survey Question: Q4: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment channels currently accepted by your company. Q6: Is your company considering accepting payments by mobile device over the next 12 months?</p>	

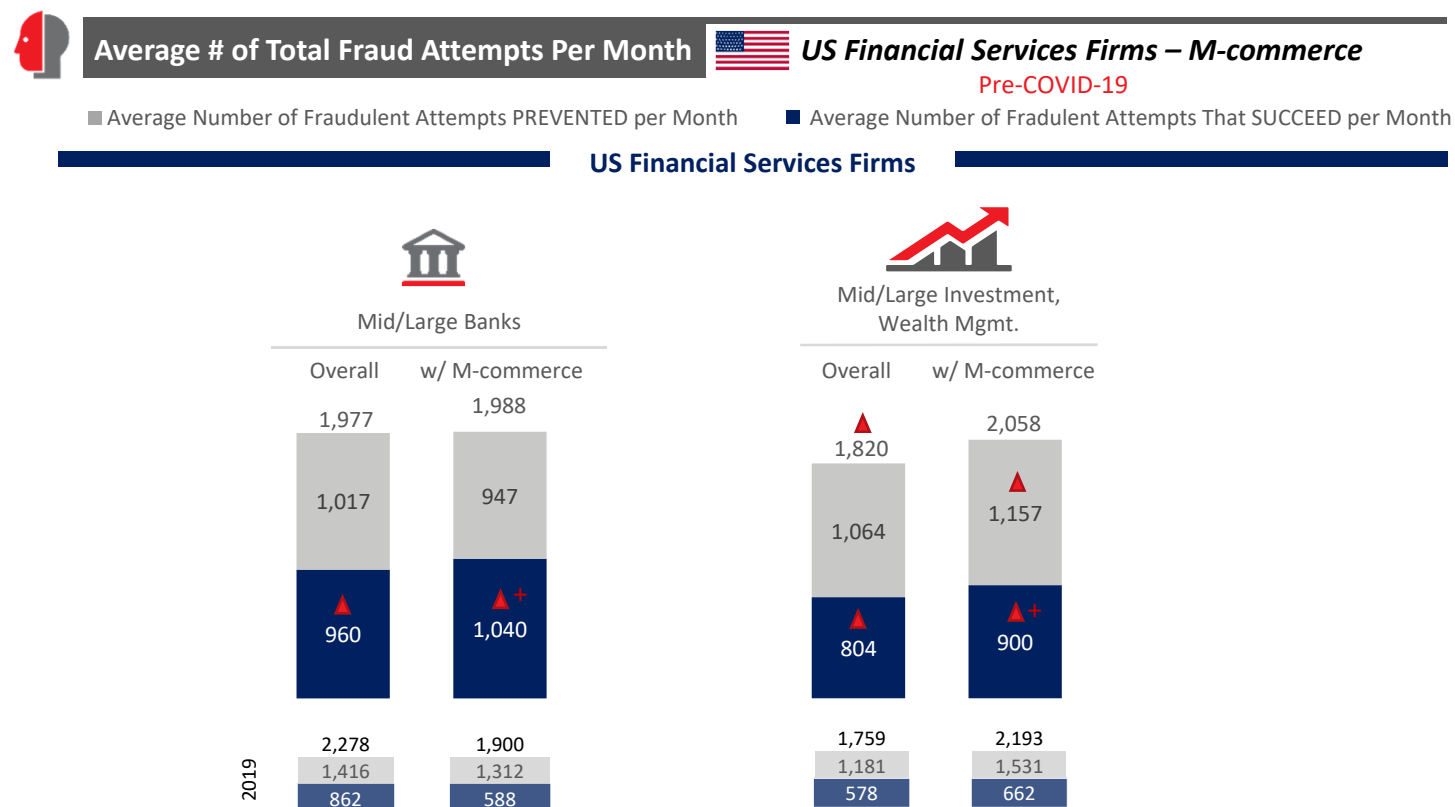
More mid/large non-digital lending firms have also begun offering mobile channel transactions.



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
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?	

Mid/large U.S. financial services organizations have experienced a rise in average monthly successful fraud attacks. These have been somewhat higher among those allowing mobile channel transactions.

This has been a typical trend over recent years, where mobile transactions = more fraud.



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Question: Q4: What is the distribution of transactions through each of the mobile channels your company uses/accepts?	

Mobile transaction options have broadened for consumers as more U.S. financial services have offered their own branded mobile app and use of bill-to-mobile payments.

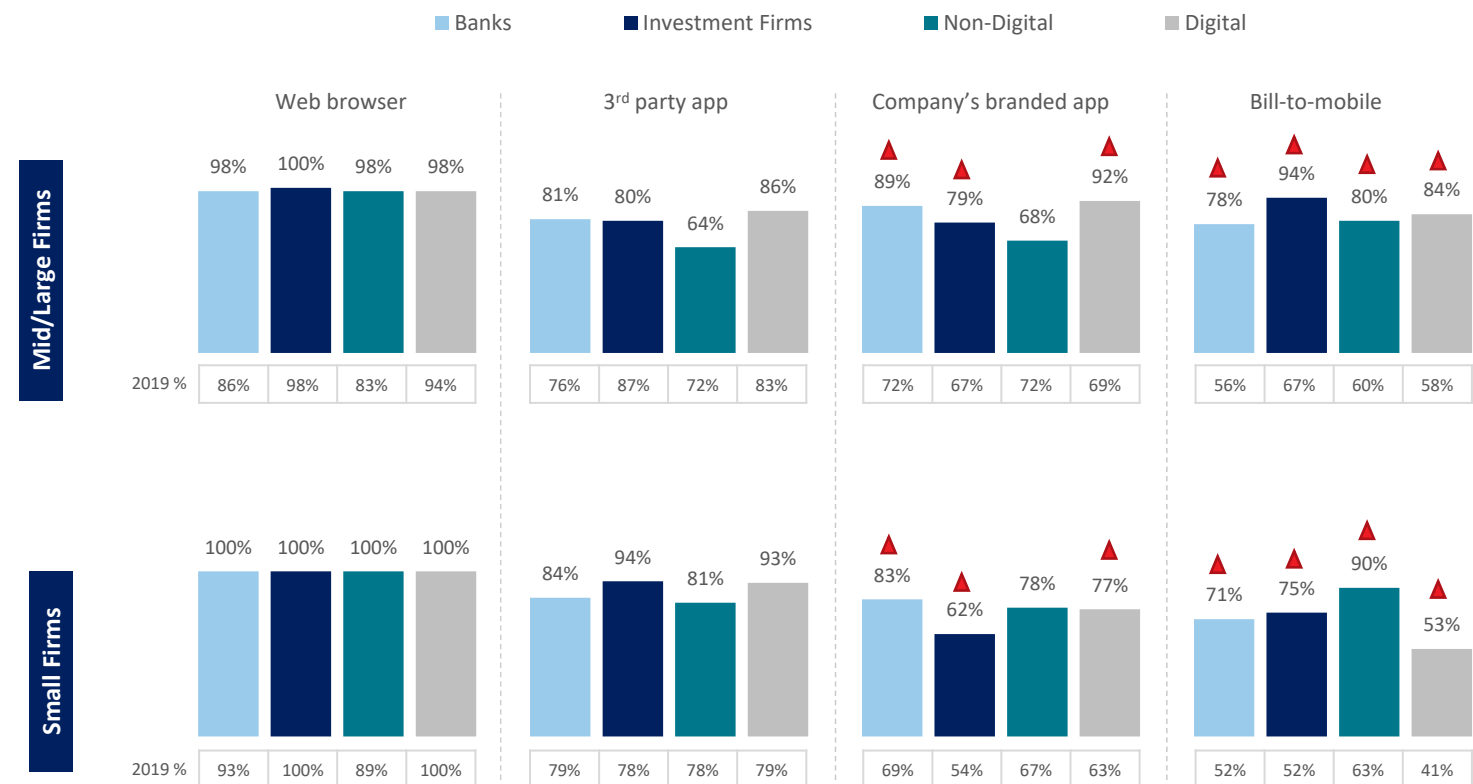
At the same time, Consumer Reports has cited an increase with cell phone account fraud, which can involve hacking consumers' mobile account or stealing/porting their number in order to open accounts, apply for credit cards, and access bank accounts.¹ Separately, the FBI recently issued a warning to consumers about Trojans that infect mobile phones and then activate when a person launches a legitimate banking app.²



% Using Each Mobile Channel



US Financial Services Firms



▲ = significantly higher than 2019

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Question: Q4: What is the distribution of transactions through each of the mobile channels your company uses/accepts?	

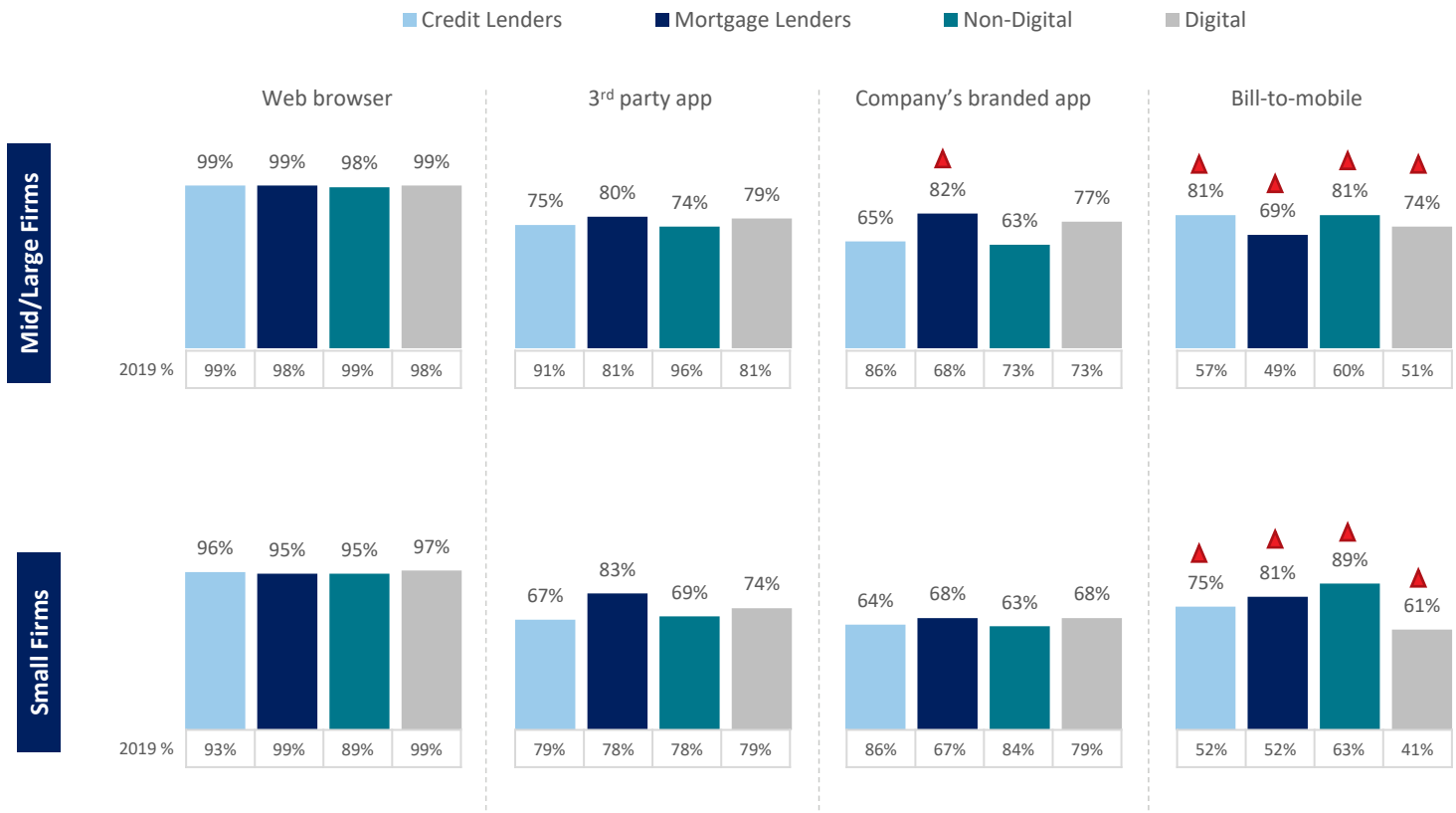
Similar adoption of bill-to-mobile has occurred among U.S. lending firms, as a high incidence of mobile app use for customers.



% Using Each Mobile Channel



US Lending Firms



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Question: Q4: What is the distribution of transactions through each of the mobile channels your company uses/accepts?	

Mobile apps use is still emerging among Canadian financial services and lending firms, though bill-to-mobile is widely offered.

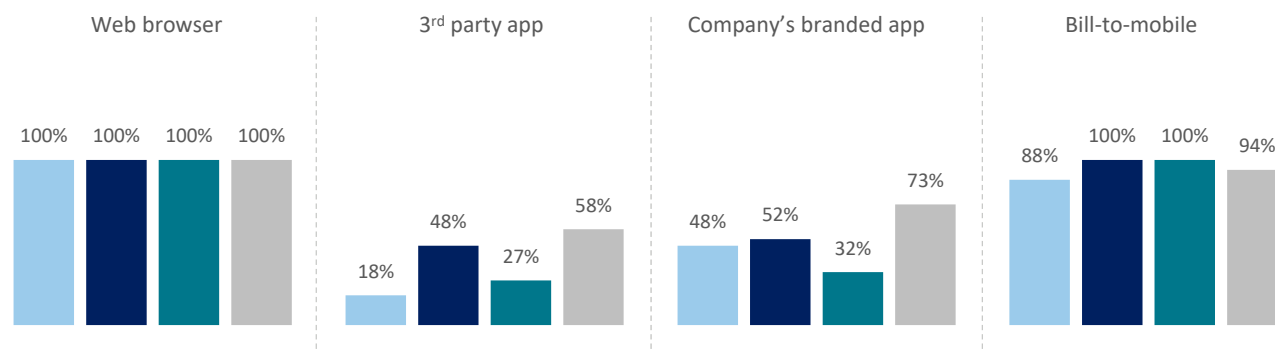


% Using Each Mobile Channel



Canada Financial Services & Lending Firms

Financial Services Overall Lending Overall Non-Digital Digital





Overview



Key Findings



#1 Attacks & Costs



#2 Trends



#3 Challenges & Impacts

#4 Potential COVID-19
Impacts

#5 Solutions Use



#6 Strategic Approaches

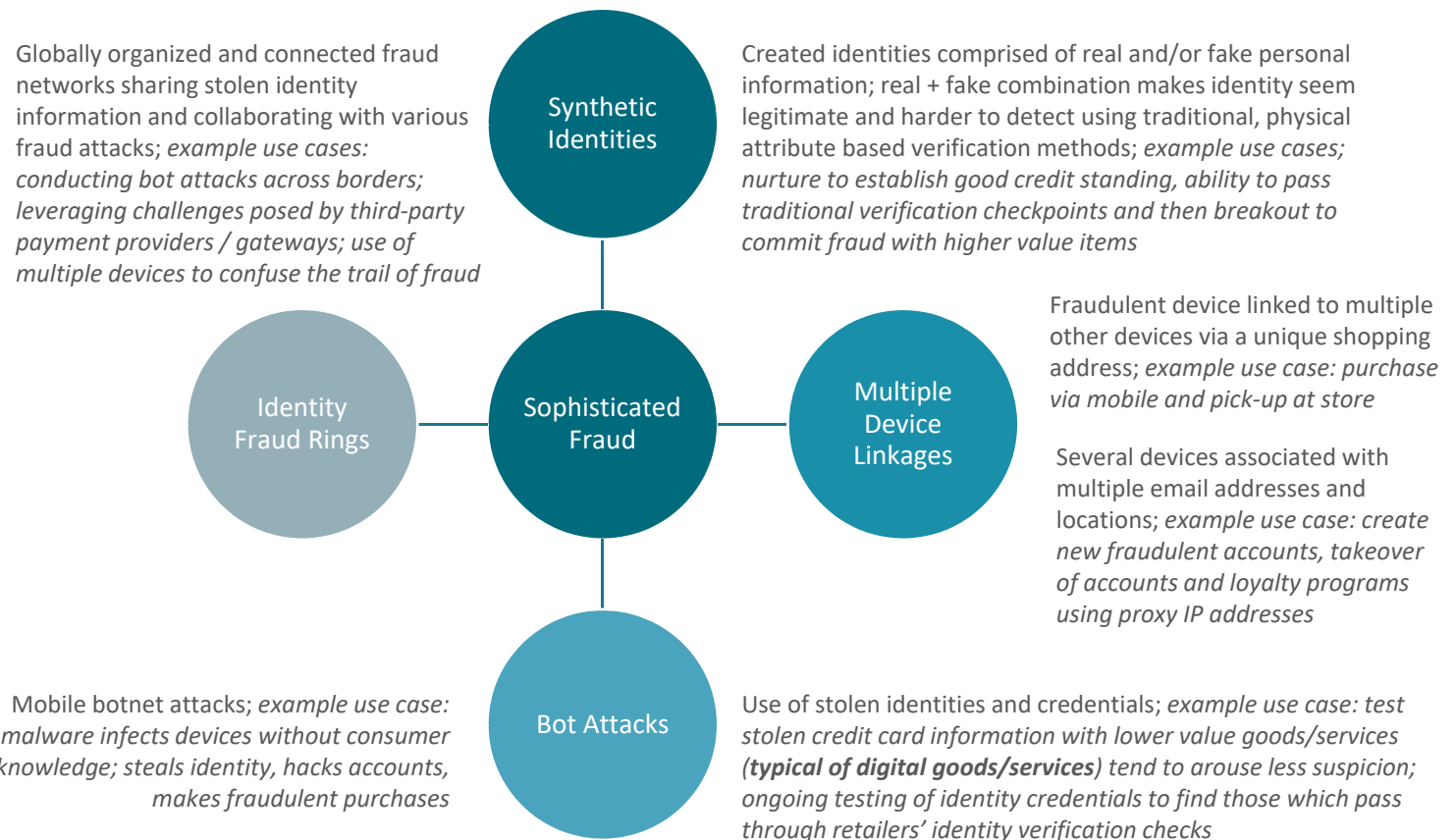


Recommendations

Fraud is becoming more sophisticated and complex.

Traditional verification checkpoints, using physical attributes (physical address, date of birth, social security number, etc...), are less effective at detecting and preventing these types of organized fraud. This is particularly challenging for transactions conducted online or through m-commerce.

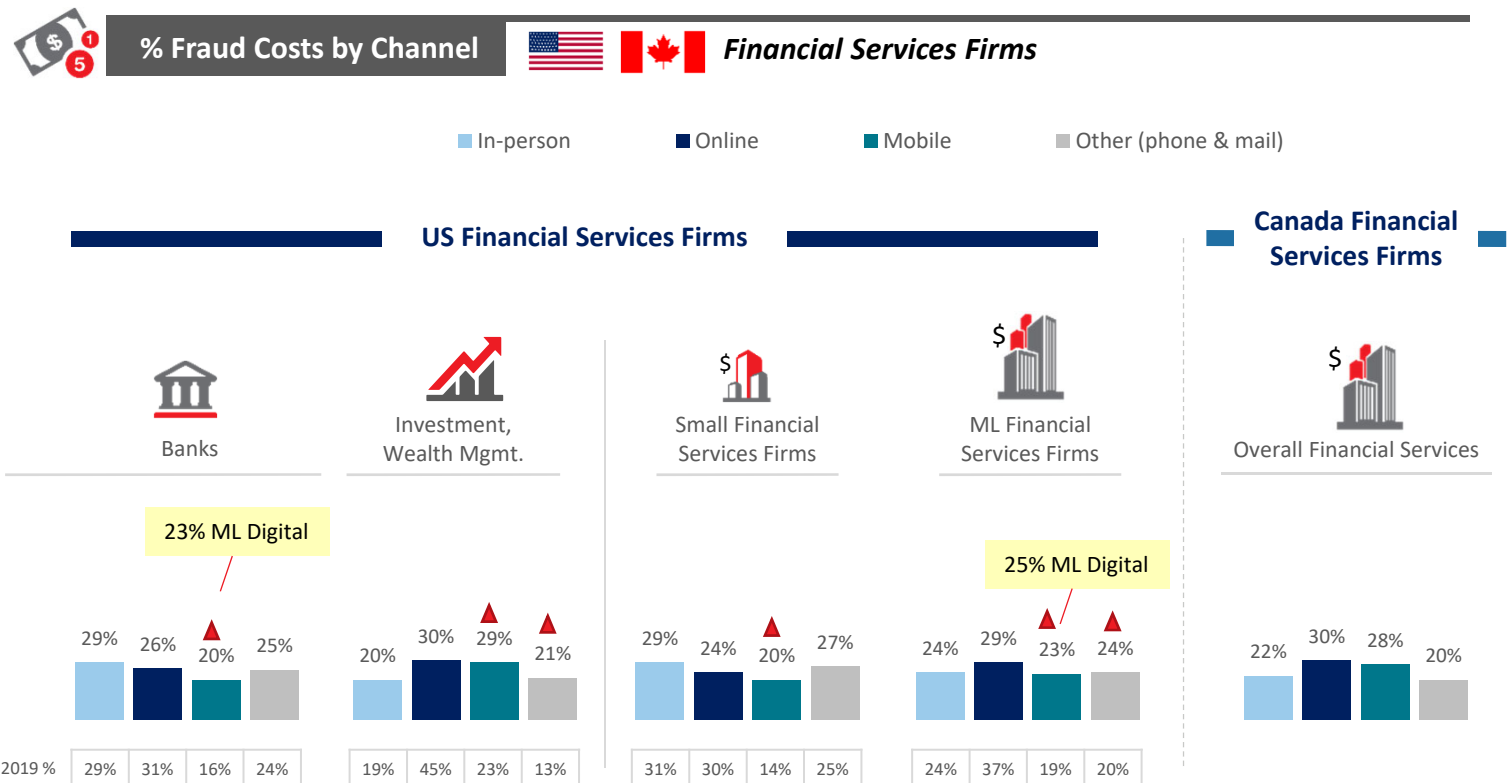
Sophisticated methods shown below not only impact identity risk assessment, but also transactional risk. One of these impacts is the limited ability to determine the transaction source / location.



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Question: Q15. Please indicate the percent of fraud costs generated through each of the following transaction channels used by your company.	

Mobile channel transactions account for a somewhat larger percent of financial services fraud costs compared to 2019.

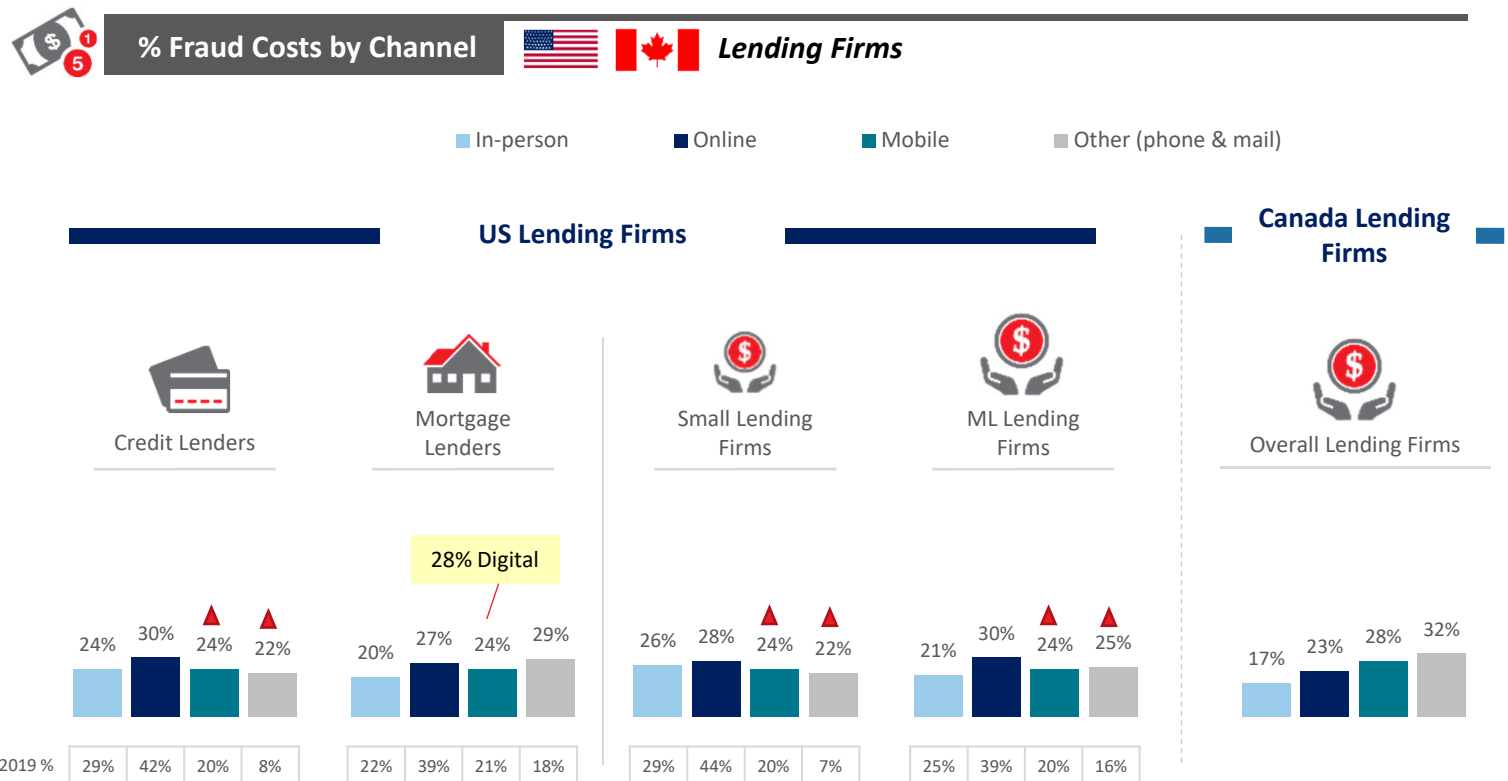
Mobile represents an even larger share of fraud costs among larger digital firms. Some of this can be attributed to the shifting of transactions to remote channels during COVID-19. But it also relates to particular mobile channel challenges regarding digital identity attributes (email, phone verification/risk), as well as increased botnet activity, identity spoofing and multiple device linkages emerging within globally connected fraud networks.



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
<p>Survey Question: Q15. Please indicate the percent of fraud costs generated through each of the following transaction channels used by your company.</p>	

Mobile channel transactions also account for a somewhat larger percent of lending firm fraud costs compared to 2019.

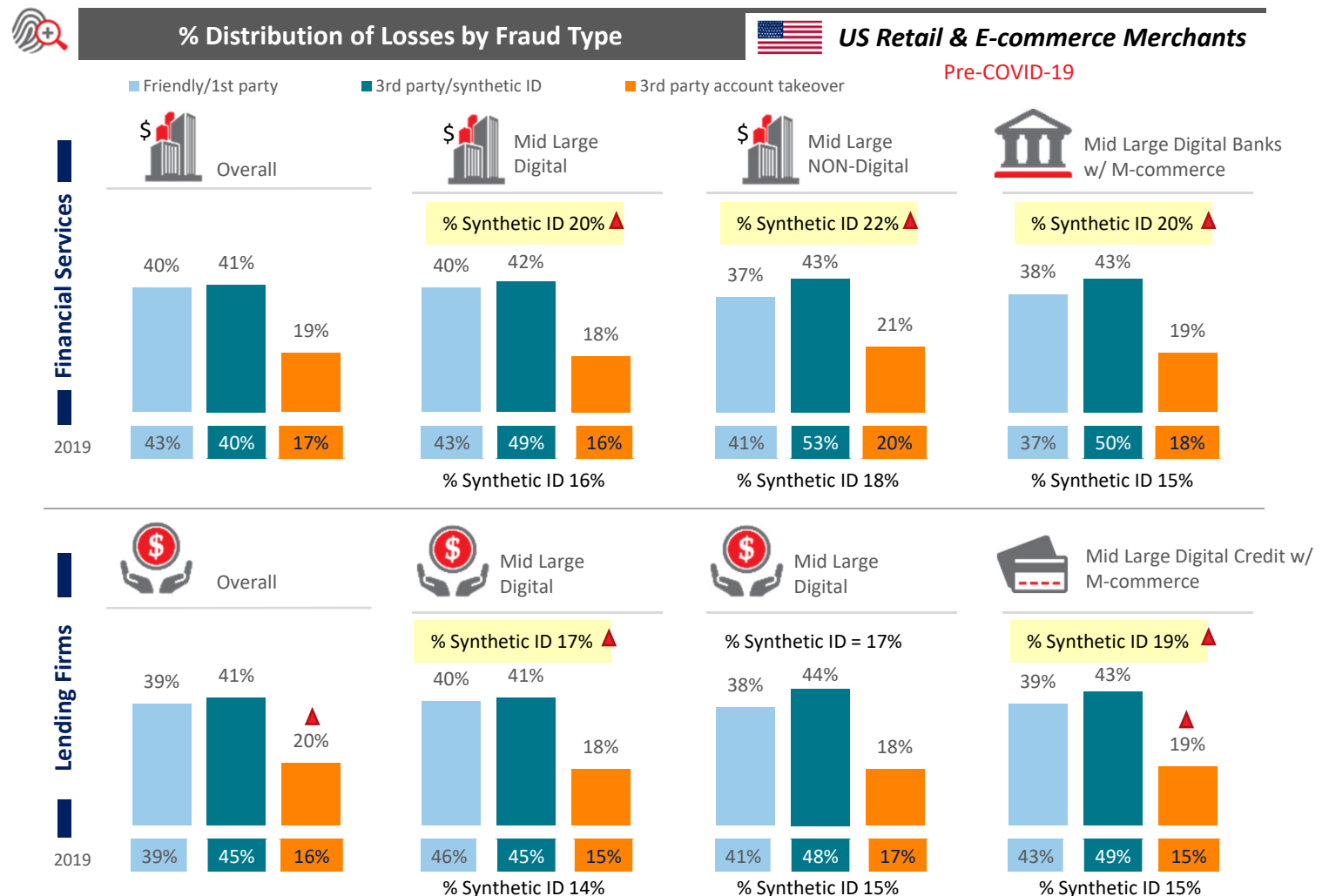
There is a similar story with lending as noted with financial services firms.



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations

Survey Question:
Q12: Please indicate the percentage distribution of the following fraud methods, as they are attributed to your total annual fraud loss over the past 12 months.

Prior to COVID-19, identity fraud had continued to be a sizeable portion of fraud losses for U.S. financial services and lending firms, with synthetic identity fraud growing among mid/large firms and those using the mobile channel.



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Question: Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?	

While account-related takeover remains a sizeable portion of identity-related fraud, the creation of fraudulent accounts has increased as a portion of these pre-COVID-19 losses for U.S. mid/large financial services and lending firms.

This coincides with increased fraud related to mobile phones and fraudulent account creation mentioned earlier.

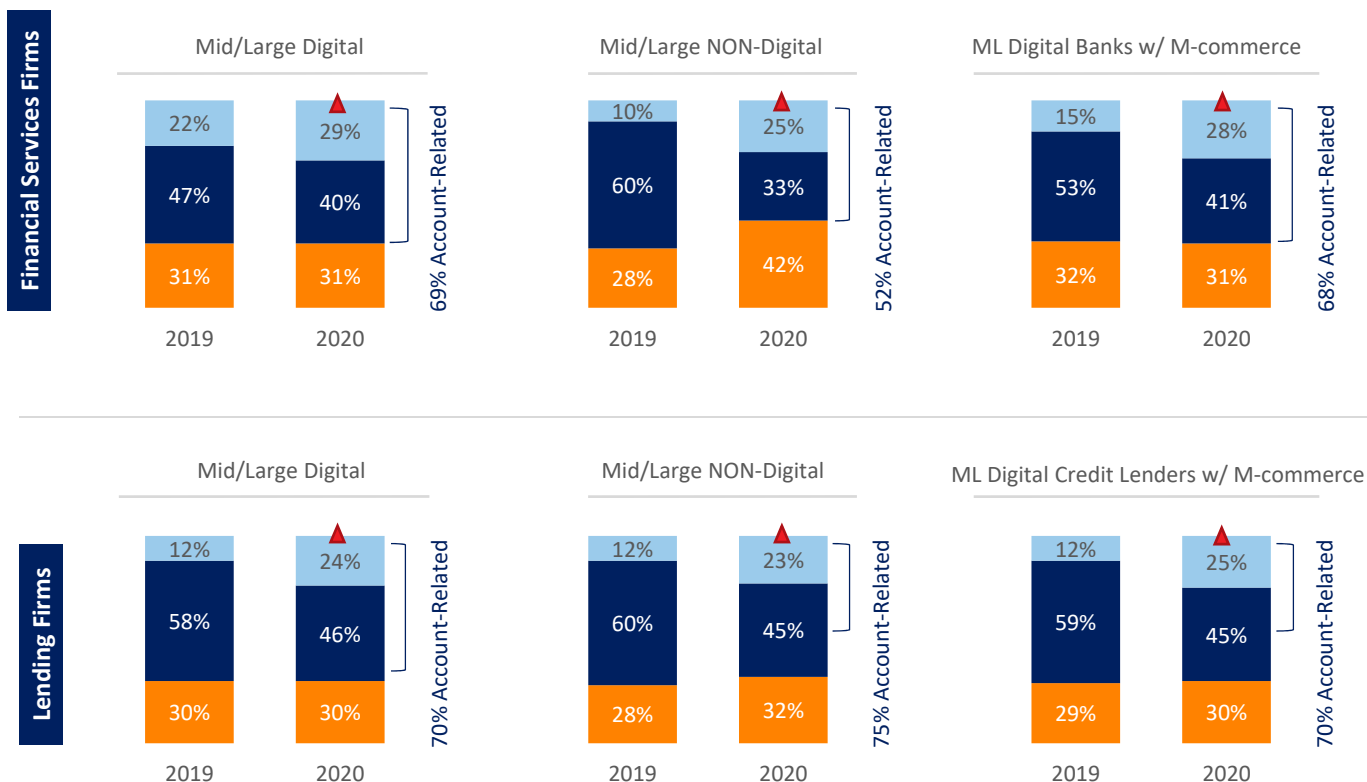


Identity-Related Fraud: % Distribution by Activity



US Financial Services & Lending Firms Pre-COVID-19

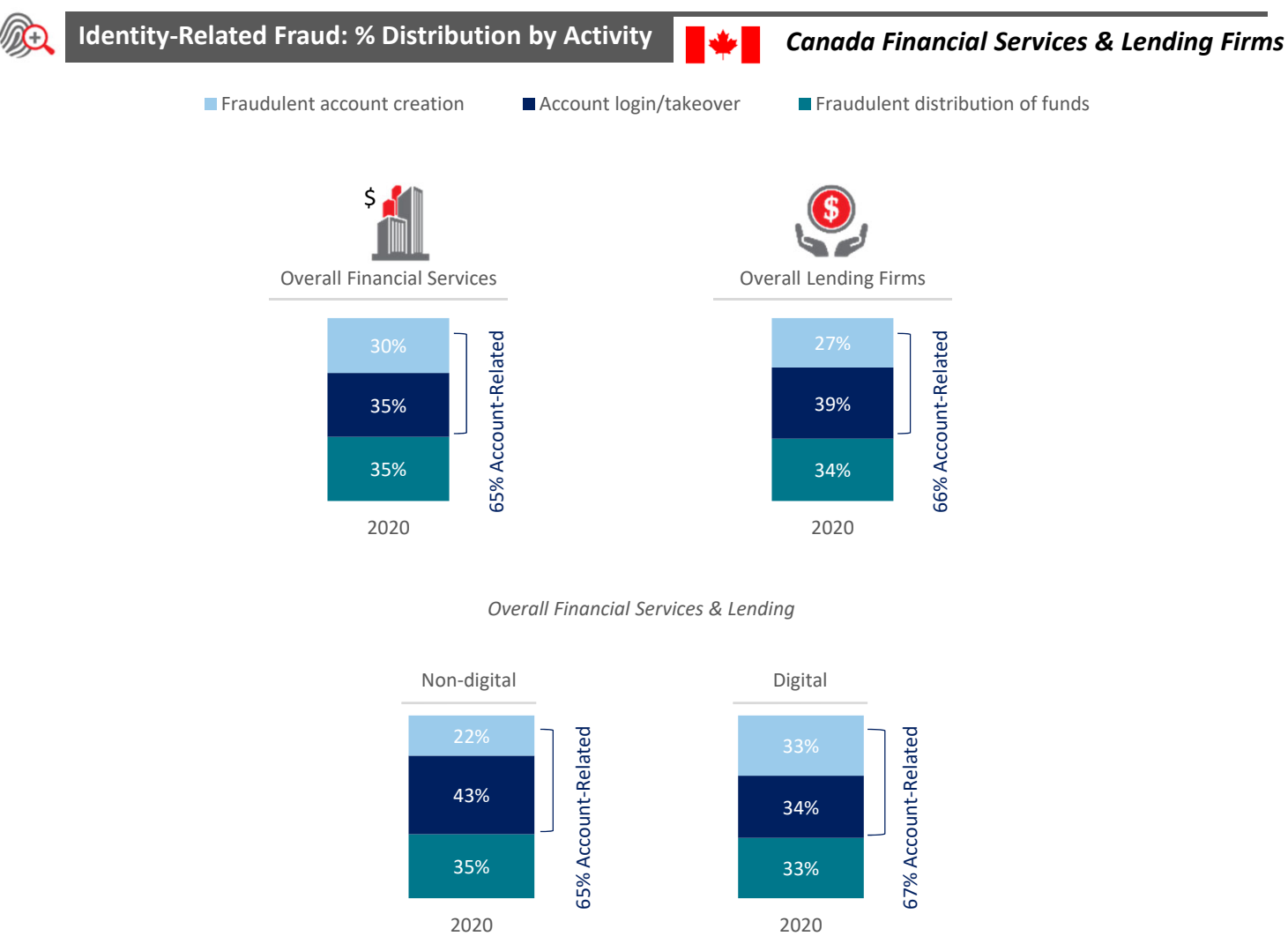
■ Fraudulent account creation
 ■ Account login/takeover
 ■ Fraudulent distribution of funds



▲ = significantly higher than 2019

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Question: Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?	

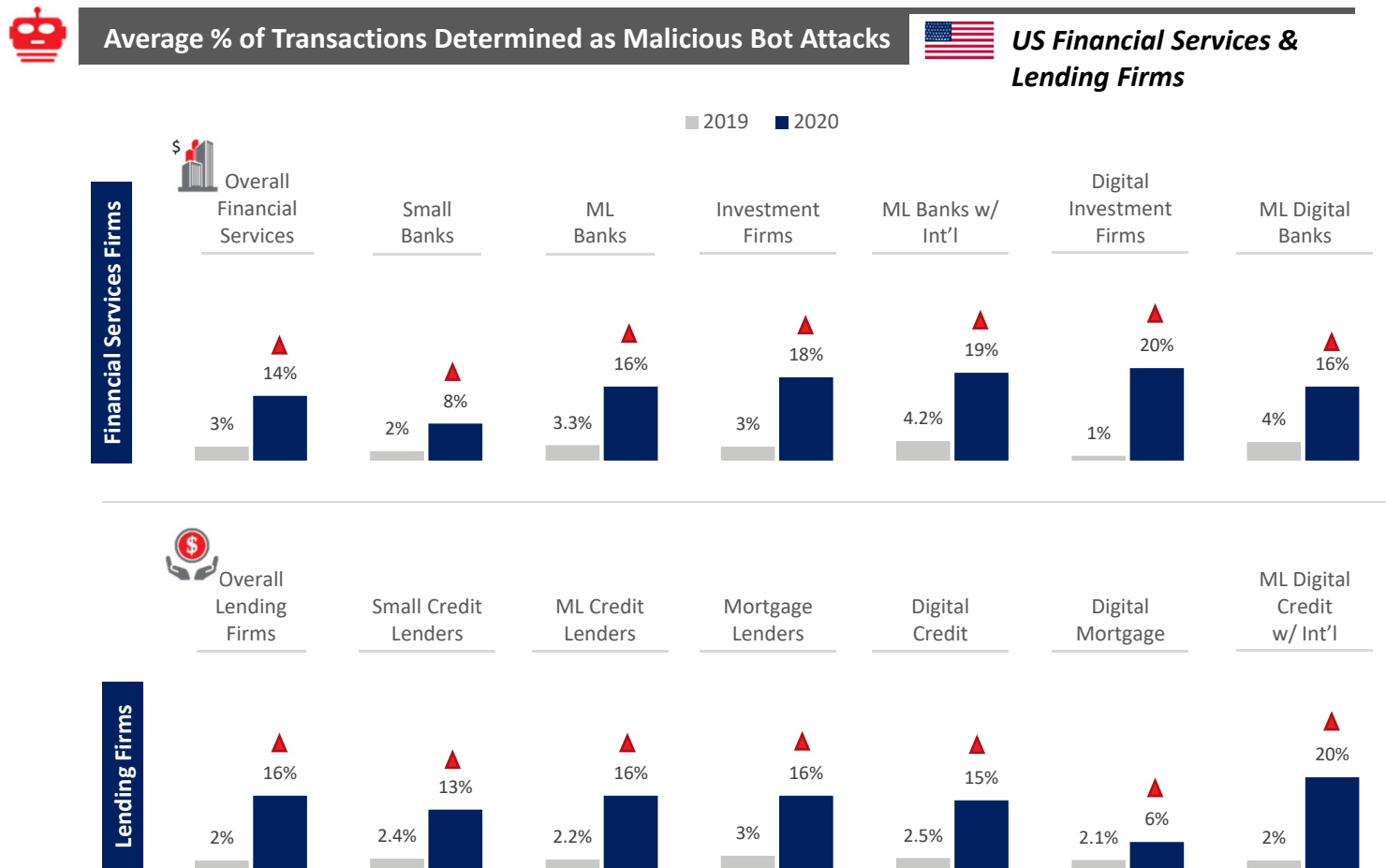
Account-related takeover / fraudulent creation also represents a sizeable portion of identity-based fraud for Canadian firms as well.



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
<p>Survey Question: B1: In a typical month, what percent of your transactions are determined to be malicious automated bot attacks (i.e. rapid creation and placement of hundreds of orders / transactions by fraudulent automated Bots at the same time)?</p>	

Bot attacks represent a sizeable portion of U.S. financial services and lending firms' monthly transactions.

Firms indicate this as a significant increase over the previous period, which is consistent with reported increased mobile botnet attacks in the LexisNexis® Risk Solutions Cybercrime Report. The volumes are similar to the level found among larger retailers in the LexisNexis® Risk Solutions 2020 True Cost of Fraud Retail edition.



2020

TRUE COST OF FRAUD™
FINANCIAL SERVICES &
LENDING STUDY

Even higher botnet representation is cited by Canadian financial services and lending firms, particularly by digital firms.



Overview



Key Findings



Attacks & Costs



Trends



Challenges & Impacts



Potential COVID-19
Impacts



Solutions Use



Strategic Approaches



Recommendations

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

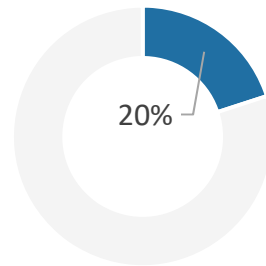


Average % of Transactions Determined as Malicious Bot Attacks

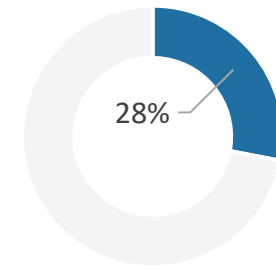


Canada Financial Services
& Lending Firms

Financial Services Firms

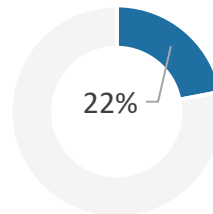


Lending Firms

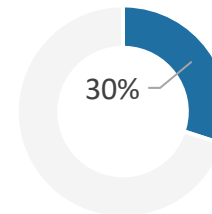


Overall Financial Services & Lending

Non-digital



Digital





Overview



Key Findings



#1 Attacks & Costs



#2 Trends



#3 Challenges & Impacts

#4 Potential COVID-19
Impacts

#5 Solutions Use

#6 Strategic
Approaches

Recommendations

Key Finding #3: In addition to identity verification, the ability to balance fraud prevention with minimal customer friction is becoming harder as fraud becomes more digitally complex.



- Identity verification remains a top challenge with online and mobile channel transactions.
 - Larger banks and credit lenders are also having to battle a broader set of challenges in these channels.
 - Digital identity verification is a particularly increasing challenge regarding email, device and phone number data. This is a challenge to both digital and non-digital firms.
- Balancing fraud prevention with minimizing customer friction has grown as a mobile channel challenge, particularly among non-digital financial services firms which are less likely to have invested in digital-based risk mitigation solutions uniquely designed for these issues.
- The rise of synthetic identities, increased botnet attacks, limited ability to confirm transaction location, limited access to real-time risk assessment data and tools, and non-bank payment providers are behind the issues related to identity verification.

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Question: Q42a: To what degree have non-bank payment service providers and systems created challenges to your business's fraud detection and prevention processes/operations during the past year?	

A sizeable portion of U.S. and Canadian financial services and lending firms have challenges with transactions flowing through third-party, non-bank payment providers, particularly for digital lending firms.

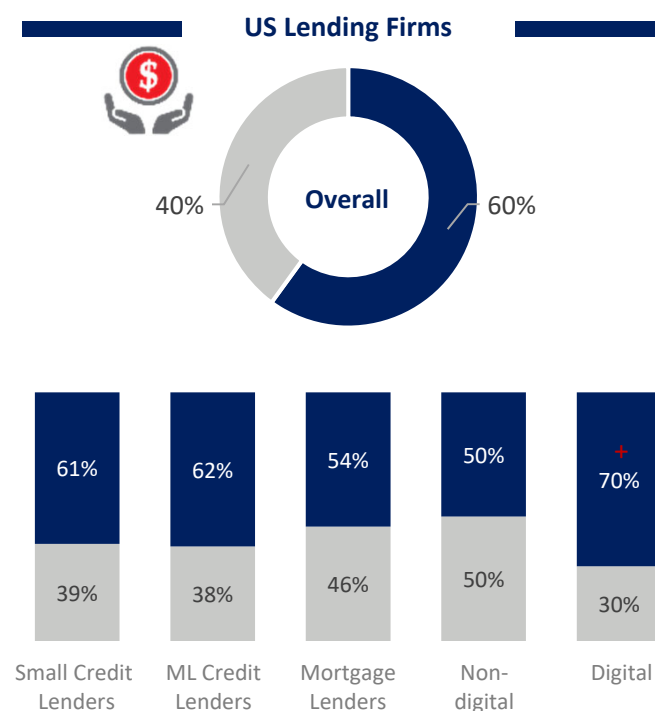
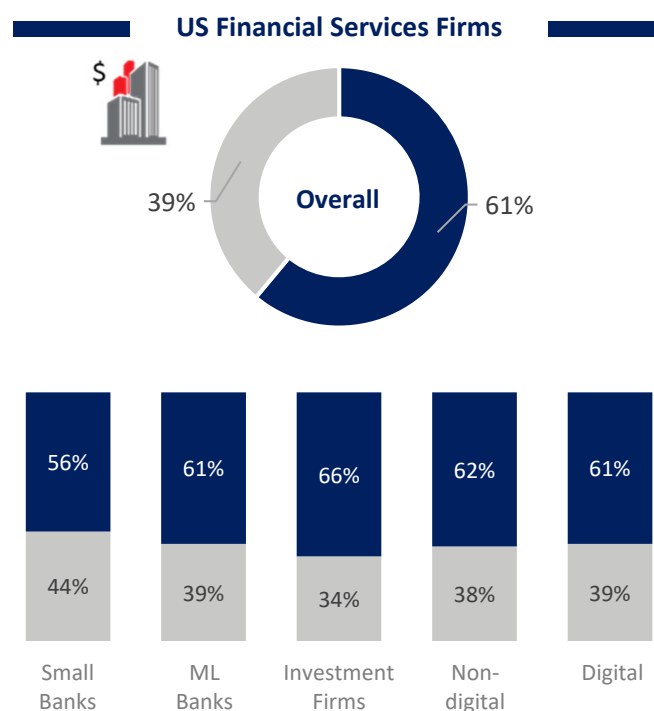


Impact of Non-Bank/3rd Party Payment Providers*



US Financial Services & Lending Firms

■ No or Minimal Degree of Challenges ■ Moderate/Large Degree of Challenges

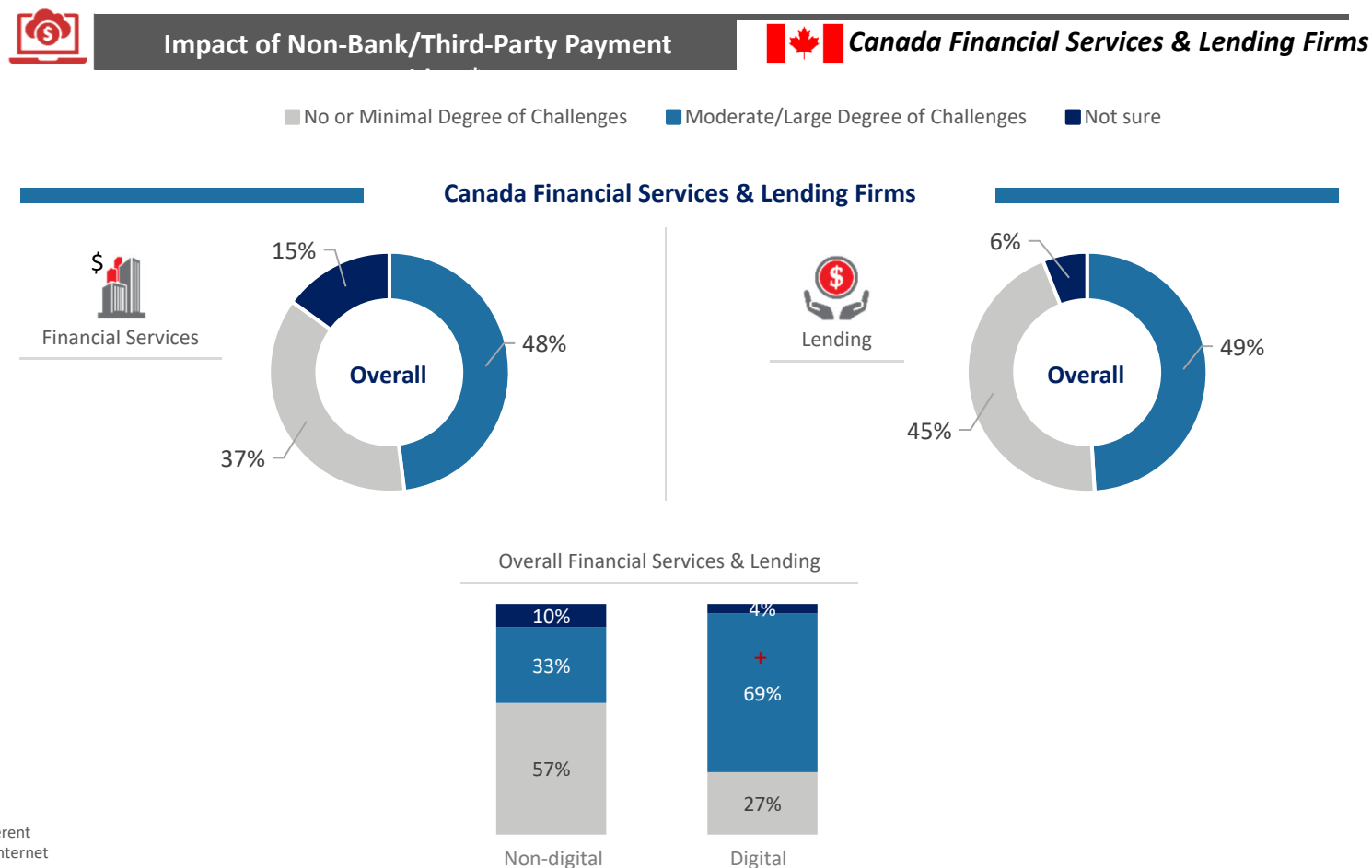


* Non-bank payment can involve a variety of different provider and systems types, such as Mobile and Internet Payment Systems (i.e. mobile wallets, peer-to-peer payments, and social media payments), payment services providers (i.e., PayPal, Stripe, Amazon Payments, Authorize.net, etc.) and FinTech companies. First asked in 2020.

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
<p>Survey Question: Q42a: To what degree have non- bank payment service providers and systems created challenges to your business's fraud detection and prevention processes/operations during the past year?</p>	

Nearly half of Canadian financial services and lending firms have also been negatively impacted by third-party, non-bank payment providers, particularly for digital firms.

Overall, significantly more U.S. firms report this type of challenge compared to Canadian firms.



* Non-bank payment can involve a variety of different provider and systems types, such as Mobile and Internet Payment Systems (i.e. mobile wallets, peer-to-peer payments, and social media payments), payment services providers (i.e., PayPal, Stripe, Amazon Payments, Authorize.net, etc.) and FinTech companies. First asked in 2020.

	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations

Survey Questions:
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online/mobile channel.

Identity verification is a key online channel challenge for mid/large U.S. banks, but they also face a variety of other challenges.

Since the survey question allows for selecting only three choices as top challenges, lower percentages for other challenges do not necessarily mean that they are less of an issue. Rather, mid/large banks did not coalesce around the second and third top challenge, indicating that they each experience various unique challenges – which speaks to ways in which more sophisticated fraud tactics have created more types of concerns.

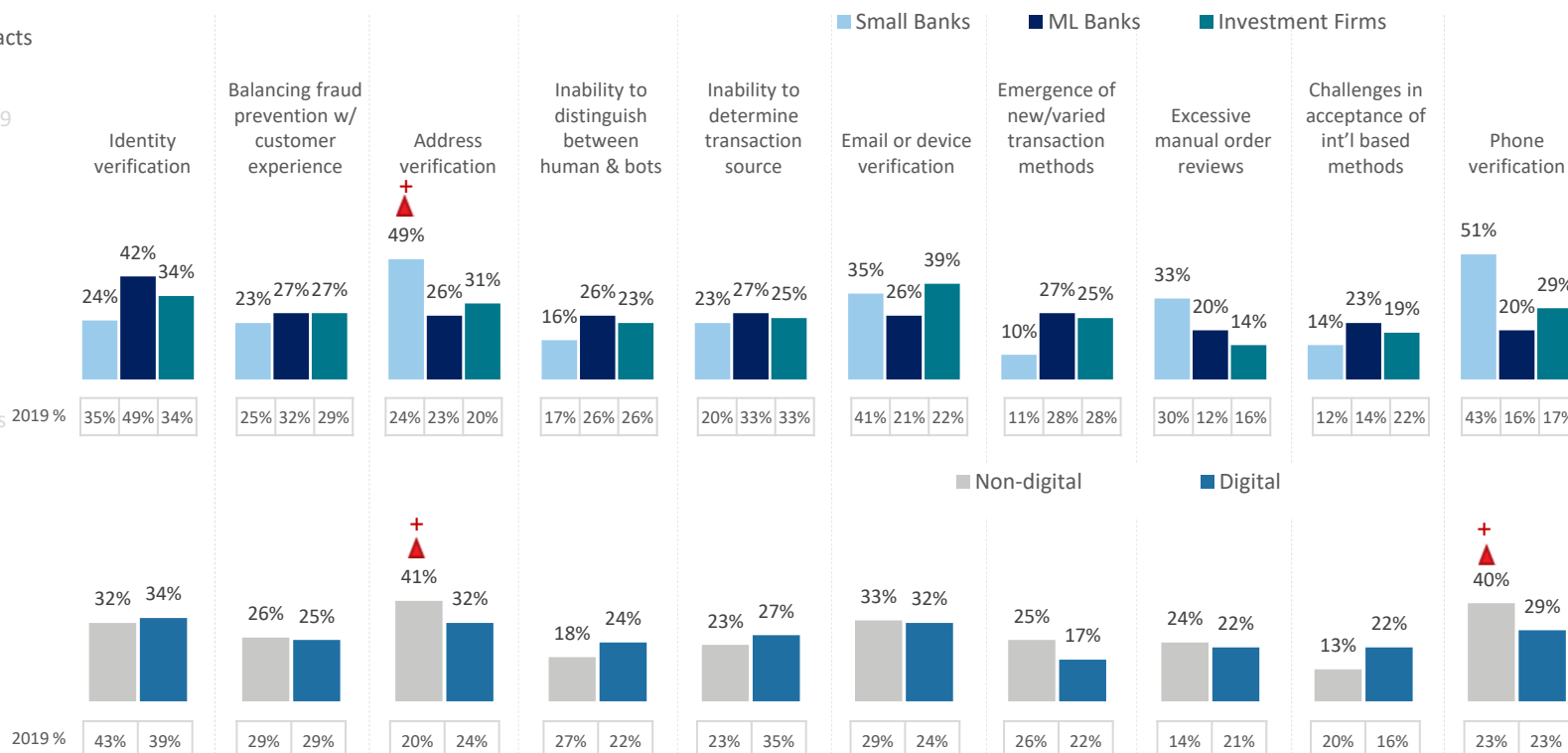
Non-digital firms have experienced increased challenges with phone and address verification, though are also less likely to be using solutions that can assess the risk associated with these identity attributes.



Fraud Challenges by ONLINE Channel (Top 3 ranked)



US Financial Services Firms



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Questions: Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online/mobile channel.	

Identity verification, including through address, phone and email, are top ranked online channel challenges for mortgage lenders and smaller creditors. As with mid/large banks, larger credit lenders face a broader scope of online channel challenges.

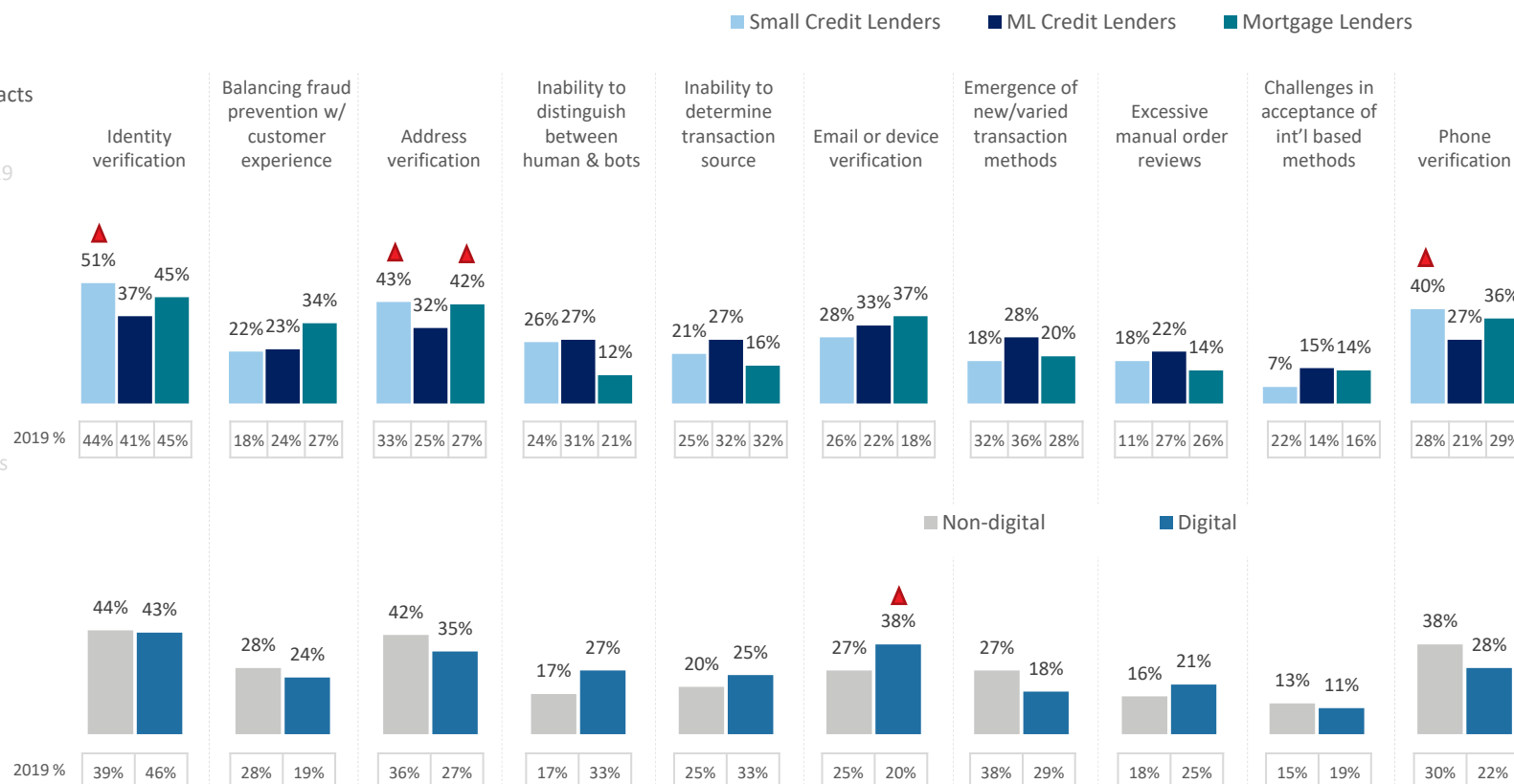
Non-digital lending firms are somewhat more likely to mention phone and address verification and are also less likely to be using solutions that can assess the risk associated not only with identity but transaction risk as well.



Fraud Challenges by ONLINE Channel (Top 3 ranked)



US Lending Firms



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Questions: Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online/mobile channel.	

Identity verification, including for email/device, are top online channel challenges for digital and non-digital Canadian firms as well.

Lending firms rank these among their top challenges somewhat more than do financial services firms, followed by inability to determine transaction source and balancing fraud prevention with customer experience.

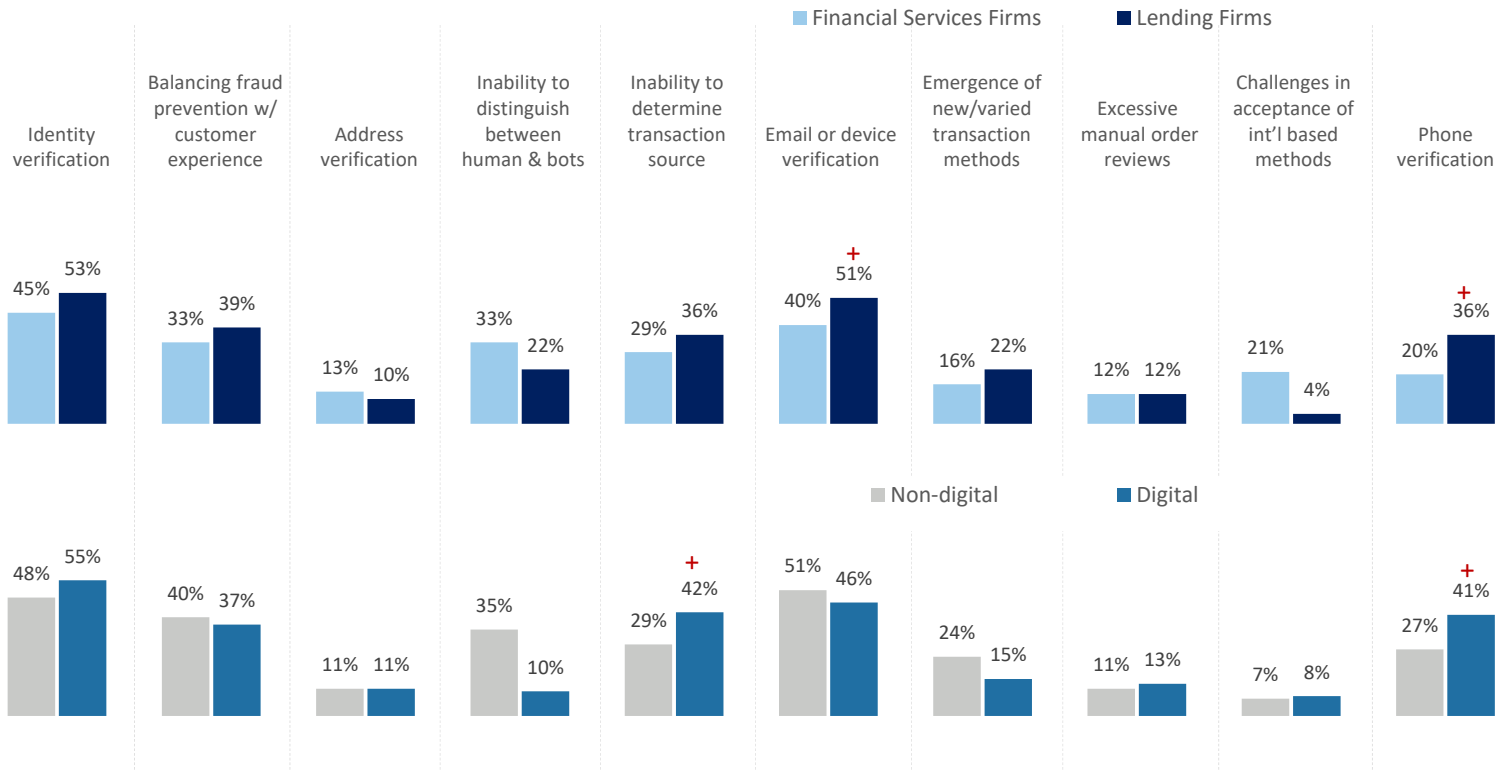
Digital firms are particularly challenged with device verification and transaction source, made more difficult by operating largely through anonymous remote channels.



Fraud Challenges by ONLINE Channel (Top 3 ranked)



Canada Financial Services & Lending Firms

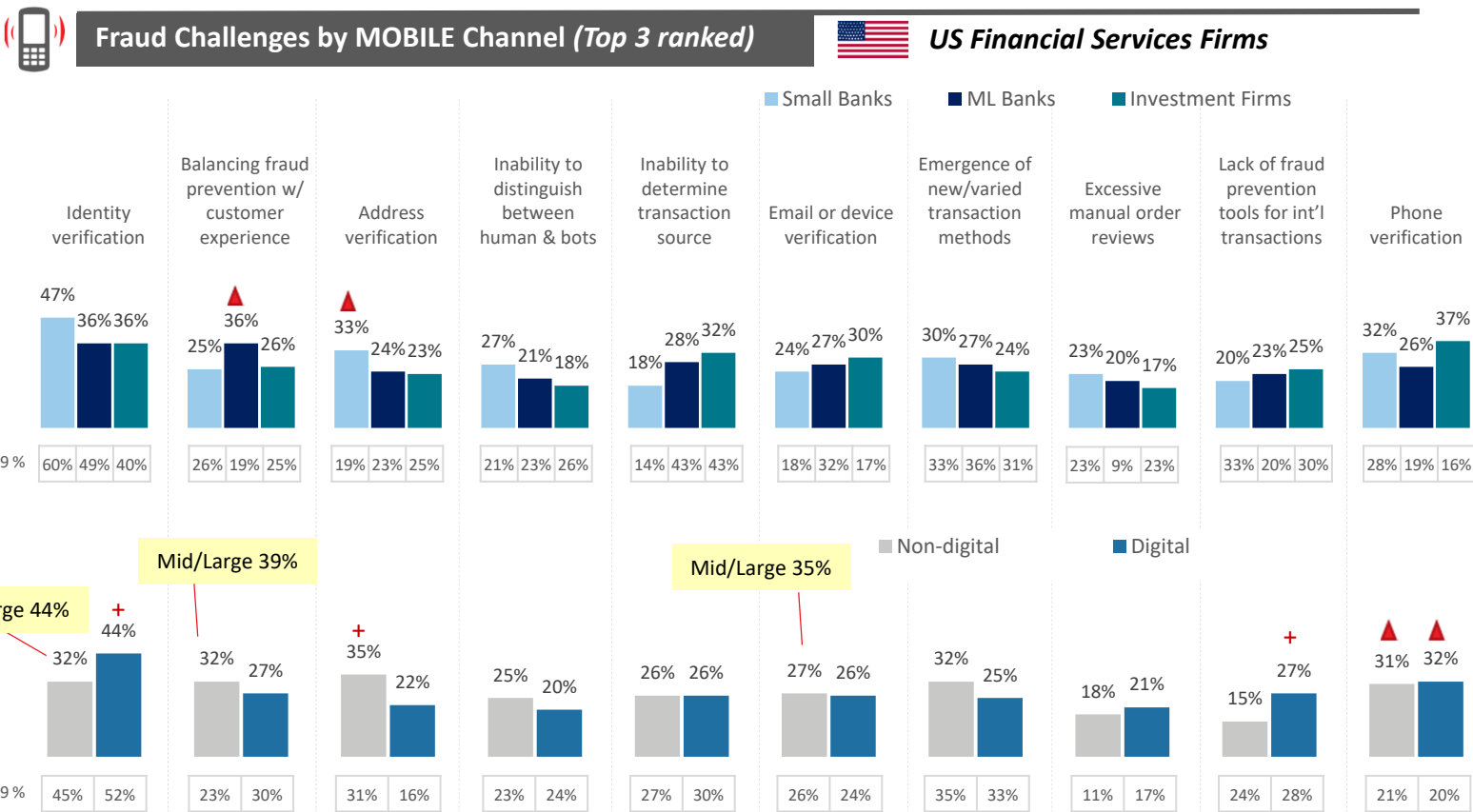


- Overview
- Key Findings
- #1 Attacks & Costs
- #2 Trends
- #3 Challenges & Impacts
- #4 Potential COVID-19 Impacts
- #5 Solutions Use
- #6 Strategic Approaches
- Recommendations

Survey Questions:
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online/mobile channel.

Balancing fraud prevention with friction has become more of a mobile channel challenge for mid/large U.S. banks, while address verification increases for small banks.

Of note is the degree to which identity verification, including through email/device/phone, and balancing fraud detection with prevention are top challenges among mid/large non-digital firms compared to digital ones. This segment continues to be slower to adopt the mobile channel; those which have are less likely to have implemented solutions to address the unique risks from these transactions and more likely to be using legacy/traditional authentication solutions across different channels.



2020

TRUE COST OF FRAUD™
FINANCIAL SERVICES &
LENDING STUDY

Overview



Key Findings



#1

Attacks & Costs



#2

Trends



#3

Challenges & Impacts



#4

Potential COVID-19
Impacts

#5

Solutions Use



#6

Strategic
Approaches

Recommendations

Survey Questions:
Q20: Please rank the top 3
challenges related to fraud
faced by your company
when serving customers
using the online/mobile
channel.

Digital-based verification (email/device/phone) through the mobile channel is becoming more challenging for credit and mortgage lenders.

This is also an issue for non-digital firms. As mentioned earlier, “non-digital” doesn’t mean “no digital”, but rather a business model that doesn’t generate a majority of revenues remotely. As such, “non-digital” firms are often multi-channel and can therefore experience the same digital channel challenges.



Fraud Challenges by MOBILE Channel (Top 3 ranked)

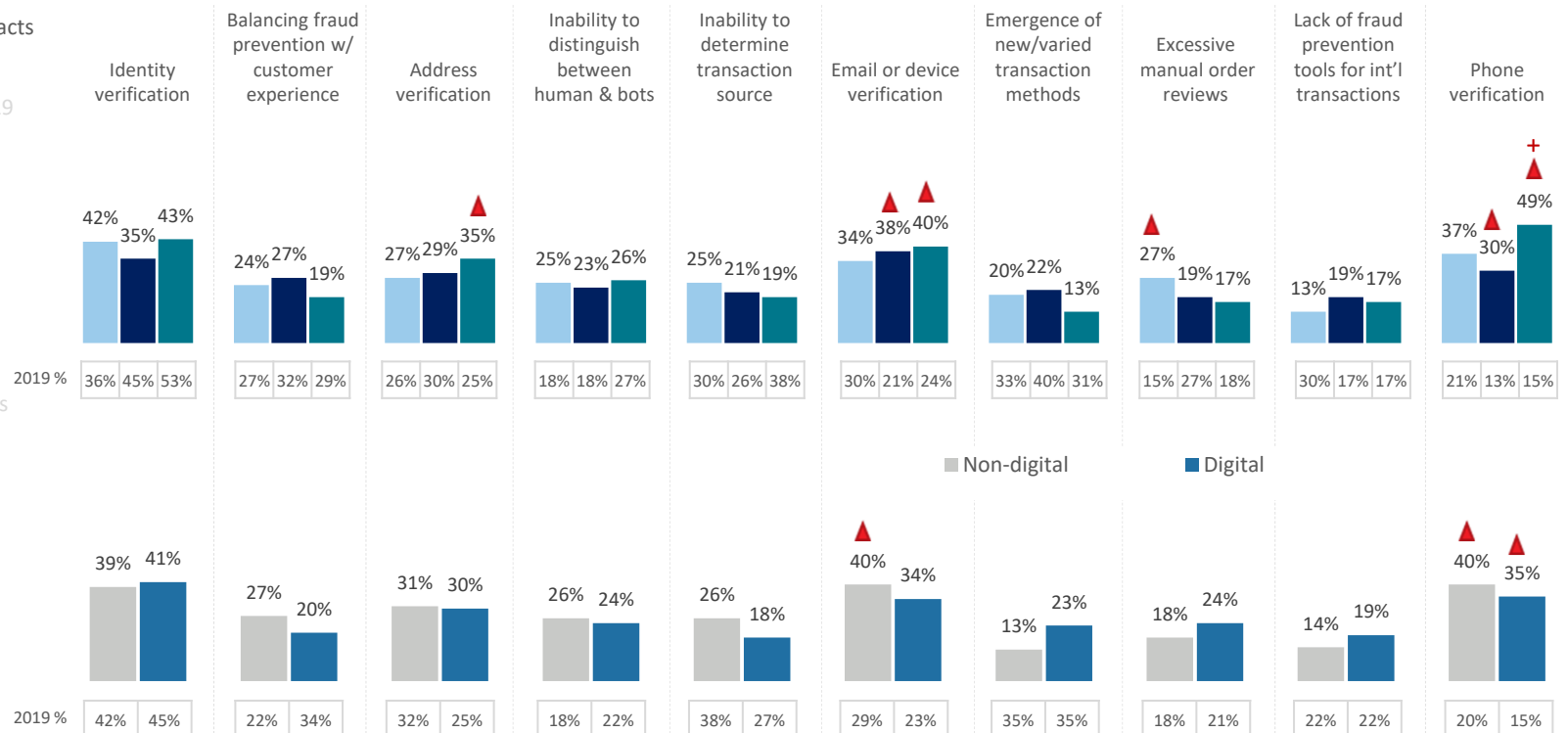


US Lending Firms

■ Small Credit Lenders

■ ML Credit Lenders

■ Mortgage Lenders

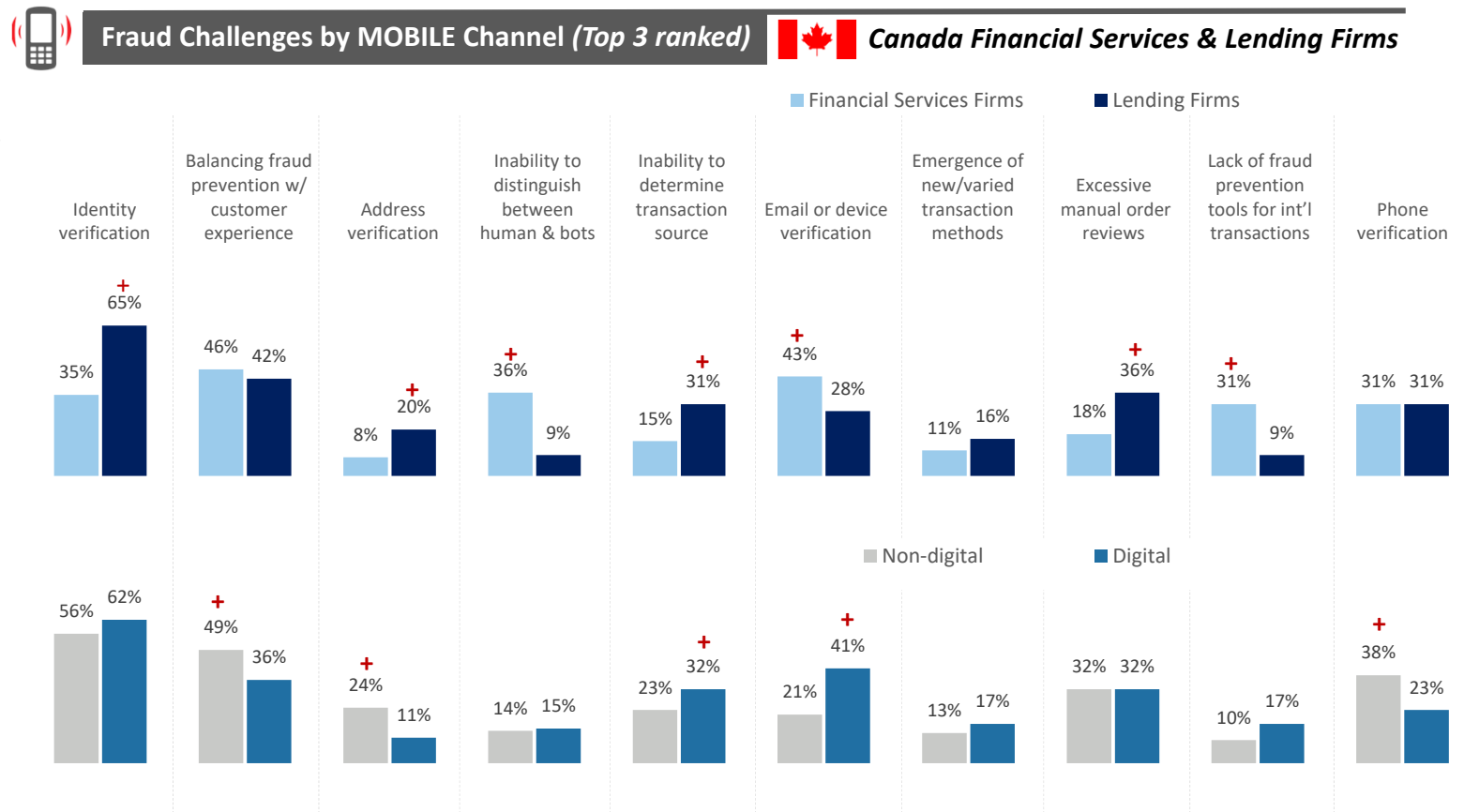


2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Questions: Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online/mobile channel.	

Top mobile channel challenges vary between Canadian financial services and lending firms, as well as by digital and non-digital organizations.

Identity verification is a significant challenge for Canadian lending firms, which can be impacted by other challenges involving inability to determine transaction source and needing to avoid too much customer friction. For some, this has translated into excessive manual reviews.

Financial services firms varied when ranking their top 3 mobile channel challenges, but with a number selecting verification (identity, device) and inability to distinguish between legitimate transactions and bot attacks.



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
#1	Attacks & Costs
#2	Trends
#3	Challenges & Impacts
#4	Potential COVID-19 Impacts
#5	Solutions Use
#6	Strategic Approaches
	Recommendations

Survey Questions:
Q20c/d: Please rank the
top 3 factors that make
customer identity a
challenge when servicing
customers through the
online/mobile channel.

Common reasons for identity verification challenges among U.S. financial services and lending firms include the rise of synthetic identities, the increased volume of botnet attacks and limited ability to confirm order location.

A number, including non-digital firms, also pointed to a lack of real-time, third-party data sources and transaction tracking tools. The need for real-time transaction tracking tools also underscores the importance of not just assessing individual identities, but also the risk of the transaction and prior behavioral patterns of transaction entities.


Top Identity Verification-Related Challenges		US Financial Services & Lending Firms	
		When Serving Customers Through the Online Channel	When Serving Customers Through the Mobile Channel
	Overall Financial Services	<ul style="list-style-type: none"> Volume of malicious Botnet orders (50%) Limited ability to confirm location of order (47%) Rise of synthetic identities (46%) Use of the mobile channel (45%) 	<ul style="list-style-type: none"> Use of the mobile channel (53%) Volume of malicious Botnet orders (46%) Rise of synthetic identities (46%)
	Non-digital	<ul style="list-style-type: none"> Volume of malicious Botnet orders (53%) Limited ability to confirm location of order (49%) Limited/no real-time transaction tracking tools (48%) 	<ul style="list-style-type: none"> Limited ability to confirm location of order (55%) Use of the mobile channel (53%) Limited/no access to real-time 3rd party data sources (45%)
	Digital	<ul style="list-style-type: none"> Rise of synthetic identities (52%) Use of the mobile channel (50%) Volume of malicious Botnet orders (48%) Limited ability to confirm location of order (46%) 	<ul style="list-style-type: none"> Use of the mobile channel (53%) Rise of synthetic identities (49%) Volume of malicious Botnet orders (48%) (ML Banks) Limited/no real-time transaction tracking tools (44%)
	Overall Lending	<ul style="list-style-type: none"> Rise of synthetic identities (64%) Limited/no access to real-time 3rd party data sources (48%) Use of the mobile channel (45%) 	<ul style="list-style-type: none"> Use of the mobile channel (59%) Rise of synthetic identities (54%)
	Non-digital	<ul style="list-style-type: none"> Rise of synthetic identities (63%) Limited/no access to real-time 3rd party data sources (50%) 	<ul style="list-style-type: none"> Use of the mobile channel (62%) Rise of synthetic identities (52%) Limited/no access to real-time 3rd party data sources (43%)
	Digital	<ul style="list-style-type: none"> Rise of synthetic identities (65%) Use of the mobile channel (57%) Limited/no access to real-time 3rd party data sources (46%) 	<ul style="list-style-type: none"> Use of the mobile channel (56%) Rise of synthetic identities (55%) Limited ability to confirm location of order (50%)

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations

Survey Questions:
Q20c/d: Please rank the
top 3 factors that make
customer identity a
challenge when servicing
customers through the
online/mobile channel.

Similar identity-verification challenges were cited by Canadian financial services and lending firms, though there was more mention of balancing speed against customer friction.

More Canadian firms cited the rise of synthetic identities and lack of real-time data sources as identity-verification challenges compared to U.S. firms.

Top Identity Verification-Related Challenges		 <i>Canada Financial Services & Lending Firms</i>
	When Serving Customers Through the Online Channel	When Serving Customers Through the Mobile Channel
<i>Overall Financial Services</i>	<ul style="list-style-type: none"> Rise of synthetic identities (71%) Use of the mobile channel (61%) 	<ul style="list-style-type: none"> Rise of synthetic identities (82%) Limited/no access to real-time 3rd party data sources (66%) Use of the mobile channel (59%)
<i>Overall Lending</i>	<ul style="list-style-type: none"> Rise of synthetic identities (81%) Use of the mobile channel (60%) Limited/no access to real-time 3rd party data sources (52%) 	<ul style="list-style-type: none"> Balancing approval speed against customer friction/abandonment (60%) Limited/no access to real-time 3rd party data sources (55%) Rise of synthetic identities (52%)
<i>Non-digital</i>	<ul style="list-style-type: none"> Rise of synthetic identities (69%) Use of the mobile channel (64%) Limited/no access to real-time 3rd party data sources (59%) Balancing approval speed against customer friction/abandonment (54%) 	<ul style="list-style-type: none"> Balancing approval speed against customer friction/abandonment (77%) Limited/no access to real-time 3rd party data sources (65%) Use of the mobile channel (55%)
<i>Digital</i>	<ul style="list-style-type: none"> Rise of synthetic identities (93%) Use of the mobile channel (55%) 	<ul style="list-style-type: none"> Rise of synthetic identities (84%)

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations

Survey Question:
Q42b: Over the past year, to what degree have the following been challenging to your fraud detection and prevention processes/operations when receiving transactions made through non-bank payment service providers and systems?

* Non-bank payment can involve a variety of different provider and systems types, such as Mobile and Internet Payment Systems (i.e. mobile wallets, peer-to-peer payments, and social media payments), payment services providers (i.e., PayPal, Stripe, Amazon Payments, Authorize.net, etc.) and FinTech companies. First asked in 2020.

A significant majority of U.S. financial services firms, both digital and non-digital, experience a number of negative impacts from non-bank/third-party payment providers.

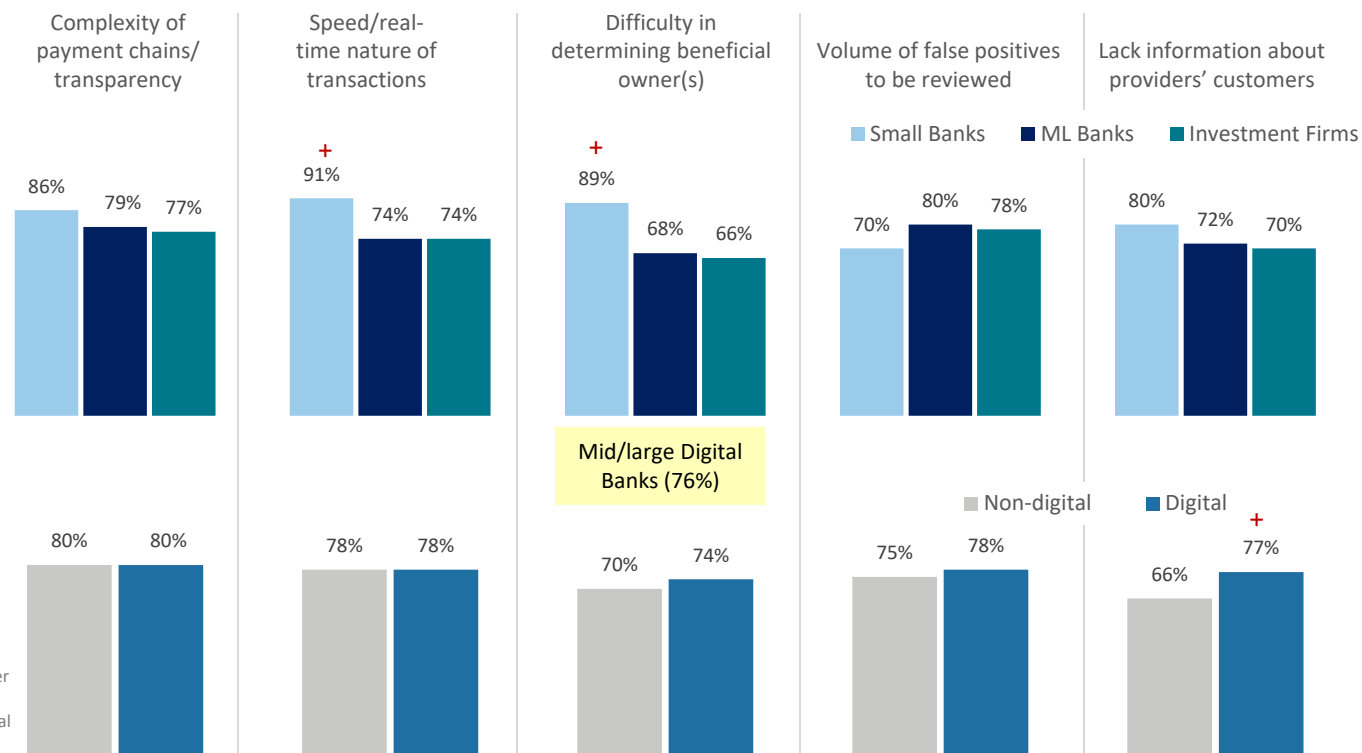
These range from added work (false positives), blind spots with assessing risk (lack of providers' customers' profile, UBO) and complexity (with payment chains and speed of transactions).



Impact of Non-Bank / Third-Party Payment Providers* (% to a large degree)



US Financial Services Firms



+ = significantly higher than the segment counterpart

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations

Survey Question:
Q42b: Over the past year, to what degree have the following been challenging to your fraud detection and prevention processes/operations when receiving transactions made through non-bank payment service providers and systems?

* Non-bank payment can involve a variety of different provider and systems types, such as Mobile and Internet Payment Systems (i.e. mobile wallets, peer-to-peer payments, and social media payments), payment services providers (i.e., PayPal, Stripe, Amazon Payments, Authorize.net, etc.) and FinTech companies. First asked in 2020.

A significant majority of U.S. lending firms, both digital and non-digital, experience the same type of non-bank/third-party payment provider negative impacts as their financial services counterparts.

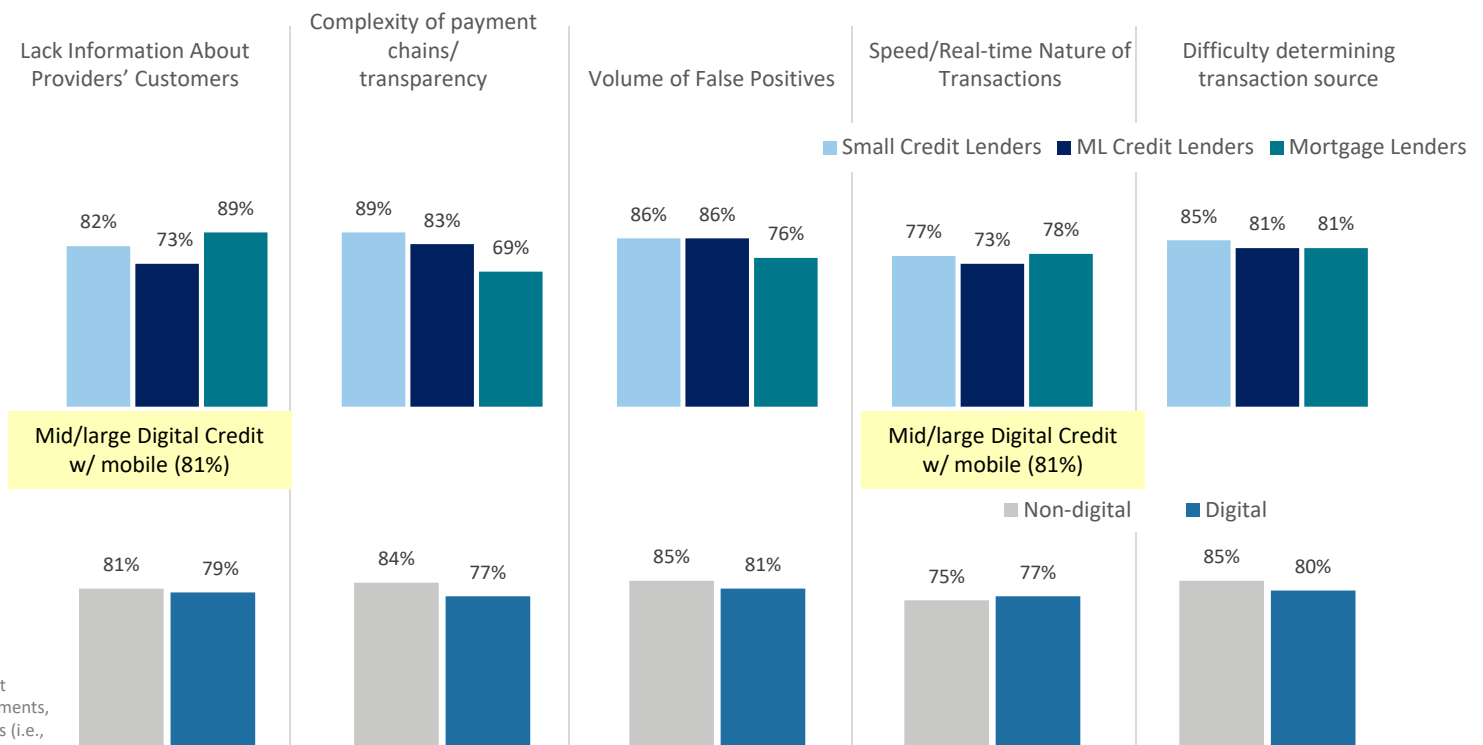
Mid/large digital credit lenders with mobile transactions are particularly challenged with assessing the risk of providers' customers' within a fast/real-time nature of the transactions.



Impact of Non-Bank / Third-Party Payment Providers* (% to a large degree)



US Lending Firms



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
<p>Survey Question: Q42b: Over the past year, to what degree have the following been challenging to your fraud detection and prevention processes/operations when receiving transactions made through non-bank payment service providers and systems?</p>	

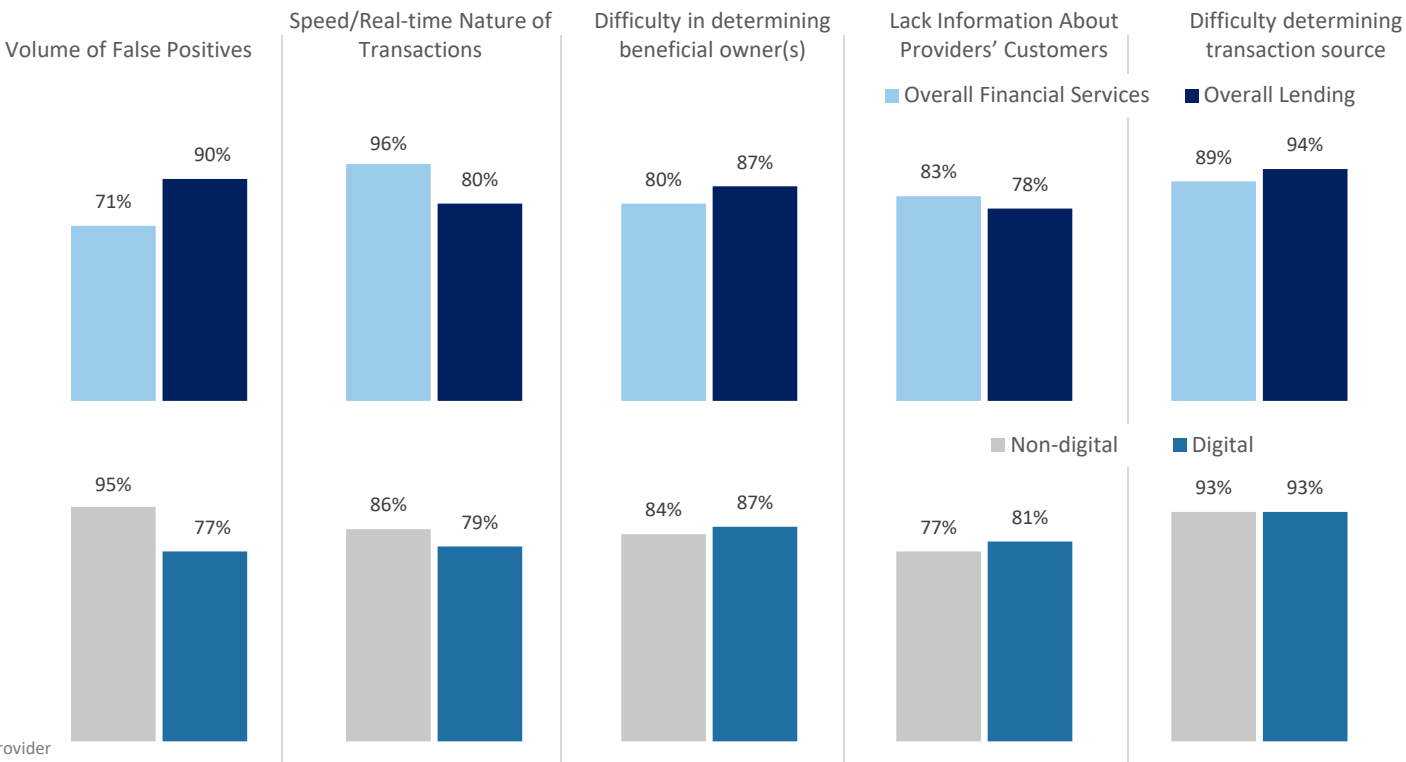
As with U.S. firms, a significant majority of Canadian financial services and lending firms cite challenges related to added work and blind spots with risk assessment.



Impact of Non-Bank / 3rd Party Payment Providers* (% to a large degree)



Canada Financial Services & Lending Firms



* Non-bank payment can involve a variety of different provider and systems types, such as Mobile and Internet Payment Systems (i.e. mobile wallets, peer-to-peer payments, and social media payments), payment services providers (i.e., PayPal, Stripe, Amazon Payments, Authorize.net, etc.) and FinTech companies. First asked in 2020.



Overview



Key Findings



#1 Attacks & Costs



#2 Trends



#3 Challenges & Impacts

#4 Potential COVID-19
Impacts

#5 Solutions Use



#6 Strategic Approaches



Recommendations

Key Finding #4: The COVID-19 pandemic has had a significantly negative impact on financial services and lending firms.



- Across segments, the volume of successful attacks have risen, but most dramatically among larger institutions.
- Similarly, this has caused a spike in the cost of fraud. That said, this spike may level off or pull back at some point as firms further implement solutions and approaches to adapt to the COVID or post-COVID world.
- The negative impact has been felt among both digital and non-digital firms, particularly banks and credit lenders which would have been involved with PPP applications.

	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations

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?

3 <https://www.infosecurity-magazine.com/news/attacks-on-banks-spike-238-during/>
4 <https://www.carbonblack.com/blog/modern-bank-heists-threat-report-finds-dramatic-increase-in-cyberattacks-against-financial-institutions-amid-covid-19/>

The COVID-19 shutdown, and movement of more transactions remotely, increased overall and successful monthly fraud attacks on mid/large financial services firms, particularly banks.

That doesn't mean that smaller and non-digital firms did not get negatively impacted, but the larger digital ones got hit comparably harder. This aligns with reports of significant increased attacks on banks during this period, particularly cyber attacks.^{3,4}

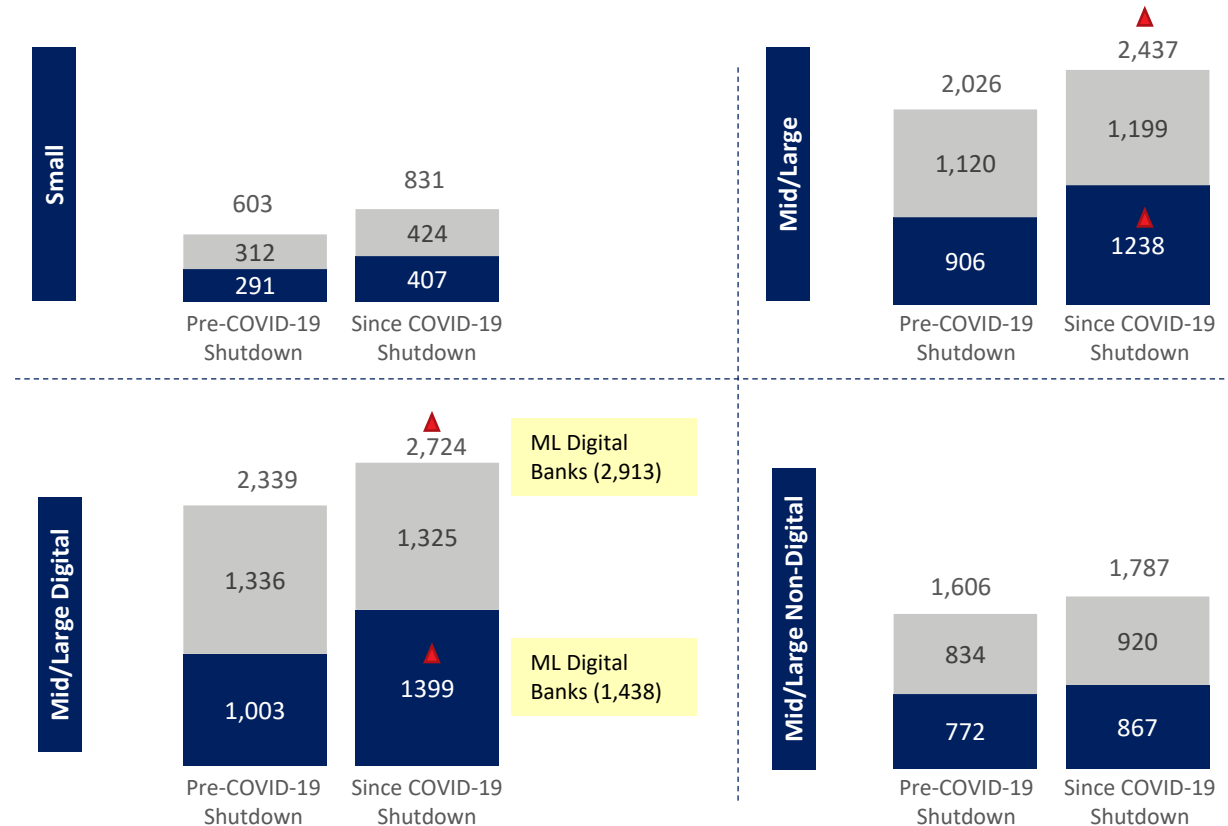


Average Monthly Fraud Attempts: Pre & During COVID-19 Shutdown



US Financial Services Firms

■ Average Number of Fraudulent Attempts PREVENTED per Month
■ Average Number of Fraudulent Attempts That SUCCEEDED per Month



▲ = significantly higher than 2020 Pre-Shutdown

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
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?	

U.S. lending firms were also hit hard by the COVID-19 shutdown, particularly larger credit lending firms – both digital and non-digital.

Federal watchdogs have reported on fraud occurring with some portion of PPP applications.⁵ Findings from the LexisNexis® Risk Solutions 2020 SMB Lending Fraud study also show an increase in the prevalence of stolen business and consumer identity occurring during this period. While successful attacks increased, so too did prevented ones – showing that lenders were effectively stopping some of this increased volume

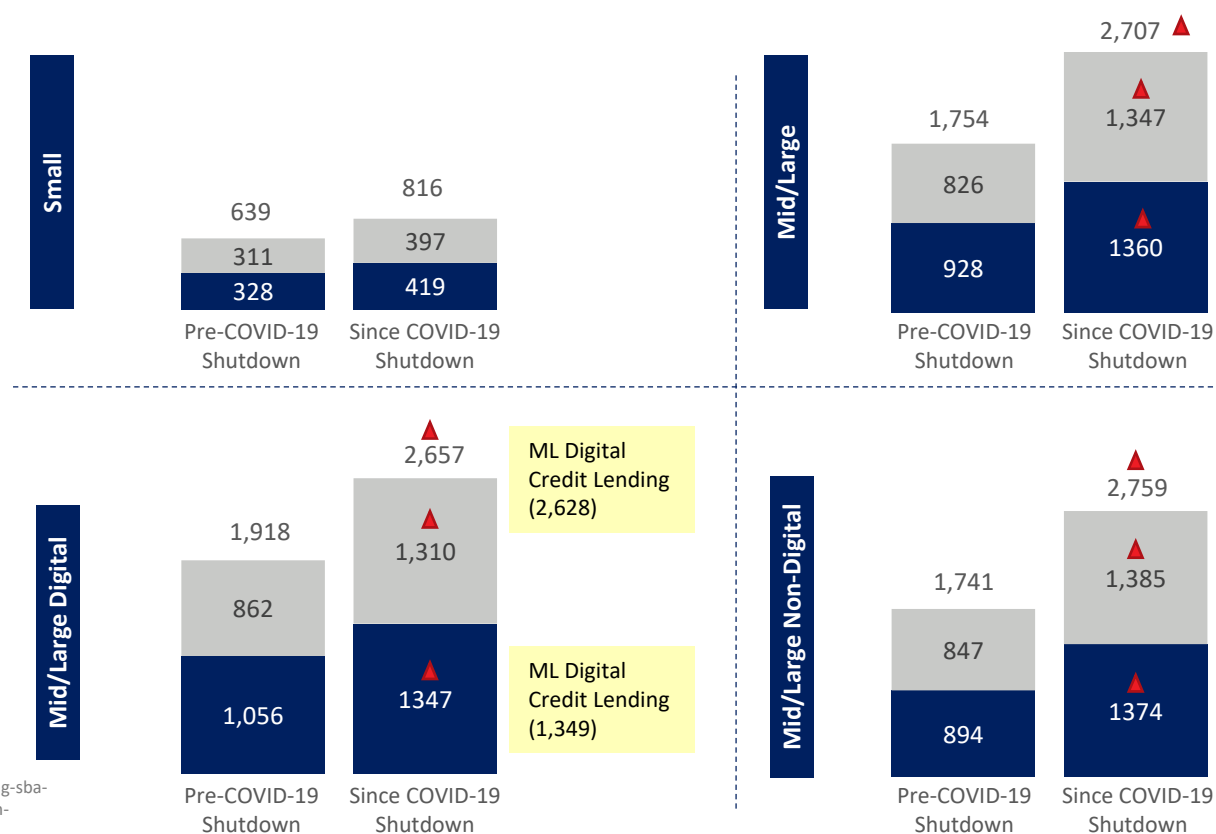


Average Monthly Fraud Attempts: Pre & During COVID-19 Shutdown



US Lending Firms

Average Number of Fraudulent Attempts PREVENTED per Month
 Average Number of Fraudulent Attempts That SUCCEEDED per Month



▲ = significantly higher than 2020 Pre-Shutdown

⁵ <https://www.washingtonpost.com/business/2020/07/28/scathing-sba-watchdog-report-details-pervasive-fraud-coronavirus-disaster-loan-program/>

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
#1	Attacks & Costs
#2	Trends
#3	Challenges & Impacts
#4	Potential COVID-19 Impacts
#5	Solutions Use
#6	Strategic Approaches
	Recommendations
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?	

Canadian financial services and lending firms experienced increased fraud attacks since the beginning of COVID-19.

This was felt across organization type and size, though particularly among larger firms.



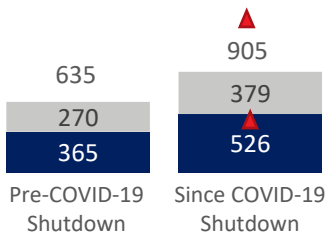
Average Monthly Fraud Attempts: Pre & During COVID-19 Shutdown



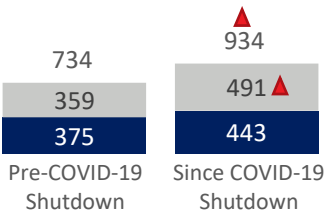
Canada Financial Services & Lending Firms

■ Average Number of Fraudulent Attempts PREVENTED per Month
■ Average Number of Fraudulent Attempts That SUCCEED per Month

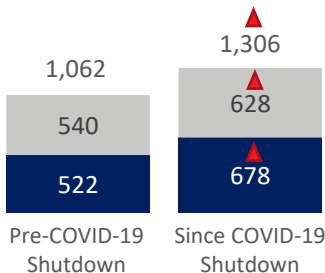
Overall Financial Services



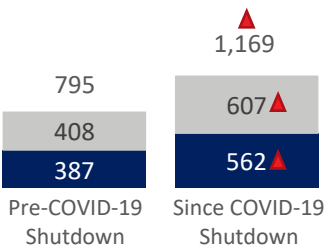
Overall Lending



ML Financial Services & Lending



Digital





Overview



Key Findings



#1

Attacks & Costs



#2

Trends



#3

Challenges & Impacts



#4

Potential COVID-19
Impacts

#5

Solutions Use



#6

Strategic Approaches



Recommendations

Key Finding #5: As fraud becomes more sophisticated, there has been some adoption of solutions designed to address unique digital/online/mobile risks, though that is still limited for the most part.



- U.S. lending firms and some digital financial services firms have further implemented solutions.
- Fraud is not a one-size fits all.
 - The ability to detect fraud in the remote channels, particularly mobile, is harder than doing so in-person.
 - The ability to distinguish between a legitimate customer and fraudster is very difficult when the criminal is using a synthetic identity with real personally identifiable information.
- Different solutions need to be applied for different channels and types of transactions. These should assess fraud for both the identity and the transaction, using physical and digital identifying information.



Overview



Key Findings



#1

Attacks & Costs



#2

Trends



#3

Challenges & Impacts



#4

Potential COVID-19
Impacts

#5

Solutions Use



#6

Strategic Approaches



Recommendations

Fraud has become more complex; various risks can occur at the same time with no single solution. Fraud tools need to authenticate both digital and physical criteria, as well as both identity and transaction risk.

FRAUD ISSUES



DIGITAL SERVICES

fast transactions, easy synthetic identity and botnet targets; **need velocity checking to determine transaction risk along with data and analytics to authenticate the individual**



ACCOUNT-RELATED FRAUD

breached data **requires more levels of security, as well as authenticating the person from a bot or synthetic ID**



SYNTHETIC IDENTITIES

need to authenticate the whole individual behind the transaction to distinguish from a fake identity based on partial real data



BOTNET ATTACKS

mass human or automated attacks often to test cards, passwords/credentials or infect devices



MOBILE CHANNEL

source origination and infected devices add risk; mobile bots and malicious malware makes authentication difficult; **need to assess the device and the individual**

SOLUTION OPTIONS

ASSESSING THE TRANSACTION RISK

Velocity checks/transaction scoring:

monitors historical transaction patterns of an individual against their current transactions to detect if volume by the cardholder matches up or if there appears to be an irregularity. **Solution examples:** real-time transaction scoring; automated transaction scoring

▶ AUTHENTICATING THE PHYSICAL PERSON

Basic Verification: verifying name, address, DOB or providing a CVV code associated with a card. **Solution examples:** check verification services; payment instrument authentication; name/address/DOB verification

Active ID Authentication: use of personal data known to the customer for authentication; or where a user provides two different authentication factors to verify themselves. **Solution examples:** authentication by challenge or quiz; authentication using OTP/ 2 factor

▶ AUTHENTICATING THE DIGITAL PERSON

Digital identity/behavioral biometrics:

analyzes human-device interactions and behavioral patterns, such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognizing normal user and fraudster behavior. **Solution examples:** authentication by biometrics; email/phone risk assessment; browser/malware tracking; device ID / fingerprinting

Device assessment: uniquely identify a remote computing device or user. **Solution examples:** device ID/ fingerprint; geolocation

2020

TRUE COST OF FRAUD™
FINANCIAL SERVICES &
LENDING STUDY

Overview



Key Findings



#1

Attacks & Costs



#2

Trends



#3

Challenges & Impacts



#4

Potential COVID-19
Impacts

#5

Solutions Use

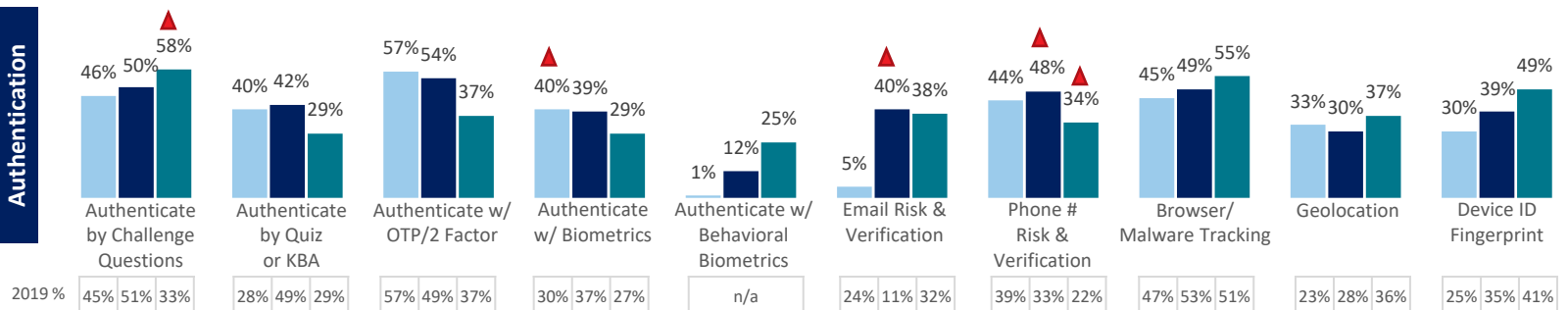


#6

Strategic Approaches



Recommendations

Survey Question:
Q27: Which of the
following fraud
solutions does
your company
currently use?Advanced ID
Authentication

The limited use of solutions to identify digital behavior threats are found across types of financial services firms, though there has been some further adoption since the prior period.

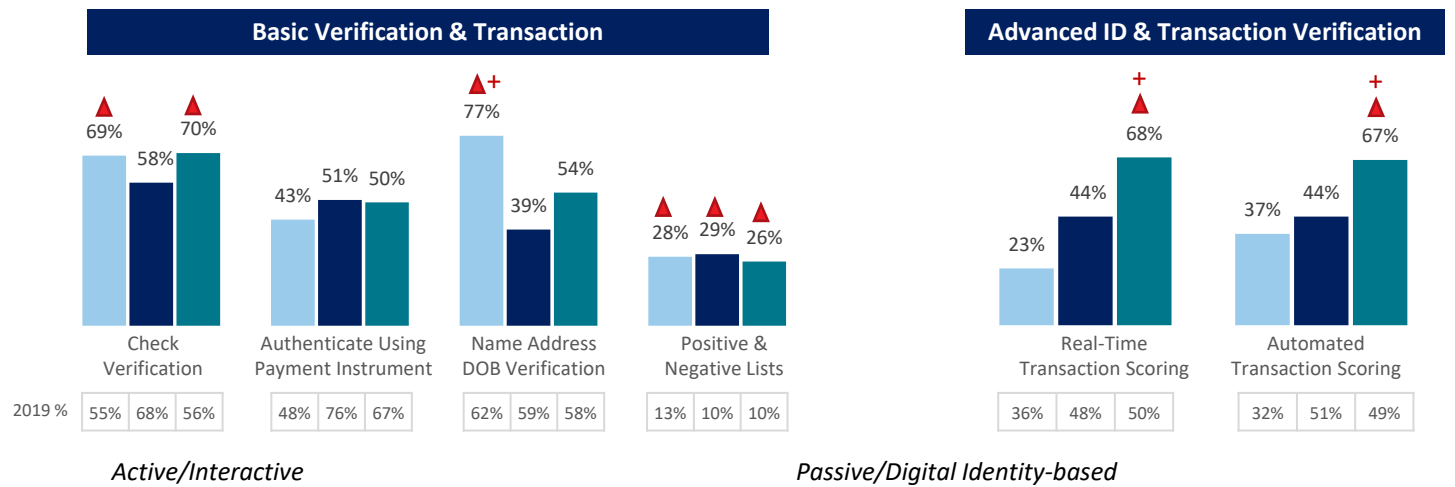
Investment firms have particularly made investments in transaction verification solutions; these are just as important as those assessing the individual risks. The complexity of synthetic identity fraud and botnet attacks requires more sophisticated solutions to assess the whole person from a digital behavior and physical identity perspective, as well as the risk of the transaction itself.

Fraud Mitigation Solutions Usage



US Financial Services Firms

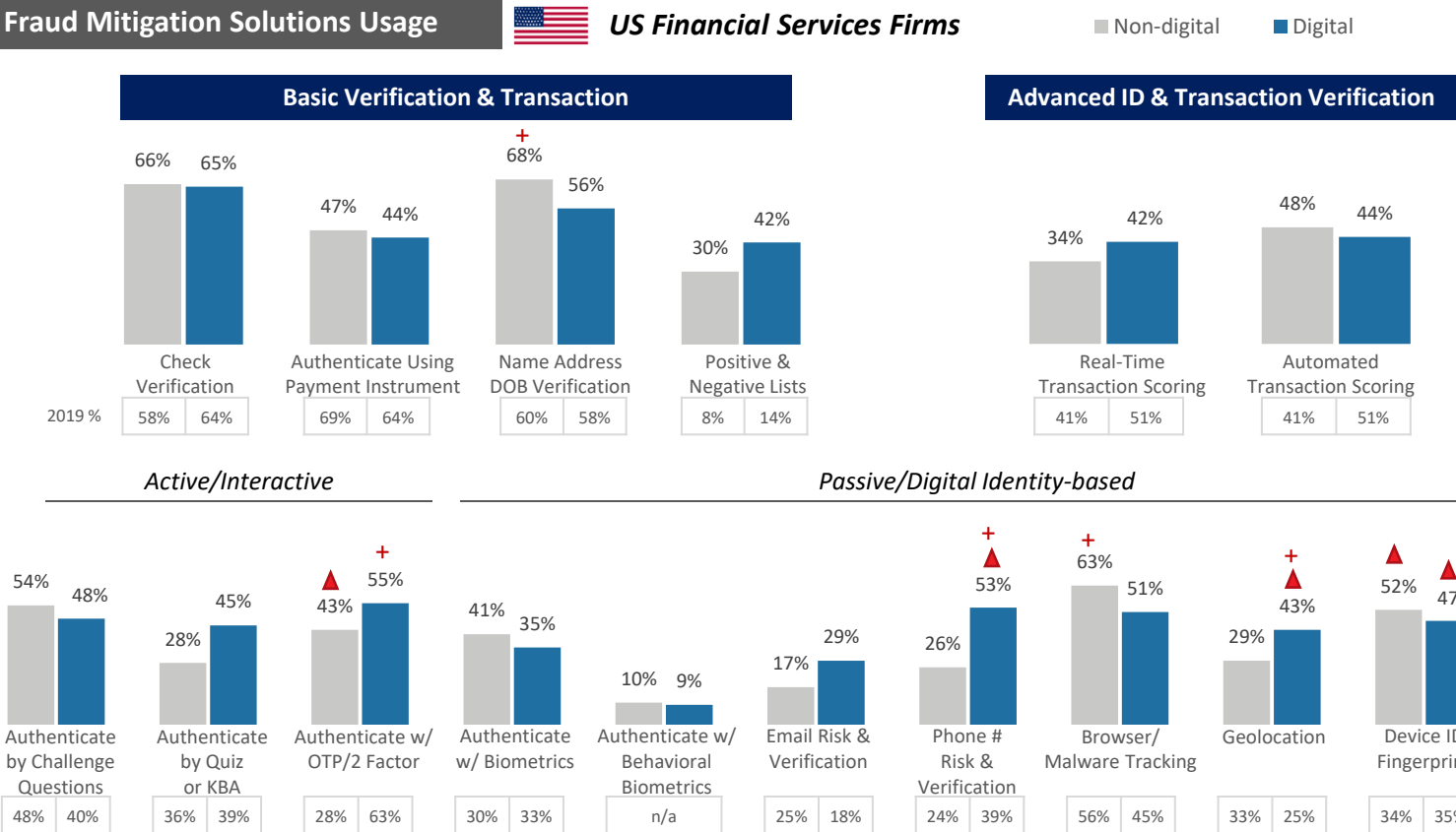
Small Banks ML Banks Investment Firms



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	#1 Attacks & Costs
	#2 Trends
	#3 Challenges & Impacts
	#4 Potential COVID-19 Impacts
	#5 Solutions Use
	#6 Strategic Approaches
	Recommendations
Survey Question: Q27: Which of the following fraud solutions does your company currently use?	

As fraud becomes more sophisticated, digital and non-digital financial services firms battle similar challenges around identity verification in the online and mobile channels.

There has been some increased adoption of passive/digital-based solutions among digital firms; adoption lags among non-digital firms even though they are challenged by digital-based identity attributes in the online and mobile channels. These solutions are designed to provide a fast, behind-the-scenes fraud assessment, reducing customer effort; this could help for those larger non-digital firms that cited balancing fraud detection with customer friction as a mobile channel issue.



2020

TRUE COST OF FRAUD™
FINANCIAL SERVICES &
LENDING STUDY

Overview



Key Findings



#1 Attacks & Costs



#2 Trends



#3 Challenges & Impacts

#4 Potential COVID-19
Impacts

#5 Solutions Use



#6 Strategic Approaches



Recommendations

Survey Question:
Q27: Which of the
following fraud
solutions does
your company
currently use?There is some increased adoption of advanced identity authentication
solutions among U.S. lending firms.

Lending firms are more likely to have implemented quiz/challenge-based identity verification solutions than their financial services counterparts. That said, a sizeable number of firms are not using these nor the advanced transaction verification solutions, compared to U.S. investment firms.

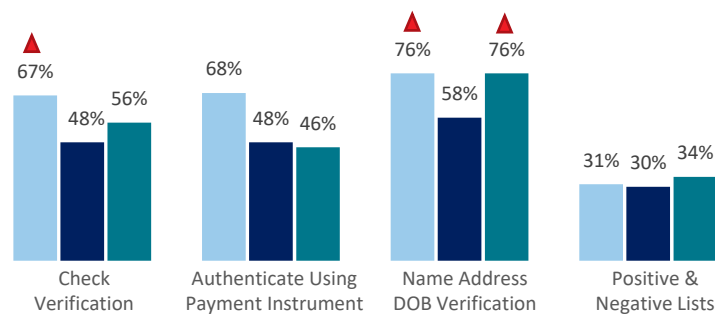
Fraud Mitigation Solutions Usage



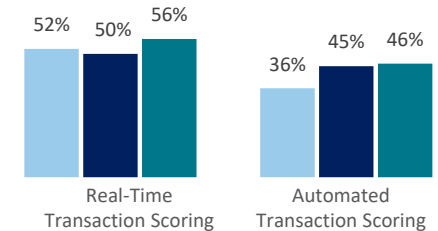
US Lending Firms

■ Small Credit Lenders ■ ML Credit Lenders ■ Mortgage Lenders

Basic Verification & Transaction



Advanced ID & Transaction Verification



2019 %

47% 66% 57%

60% 71% 66%

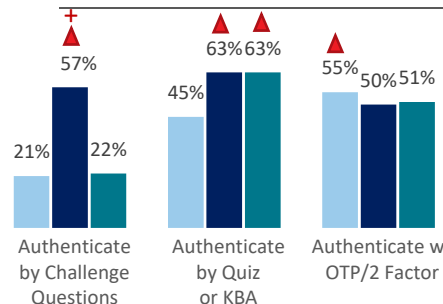
54% 59% 57%

48% 37% 41%

44% 51% 59%

46% 58% 56%

Active/Interactive



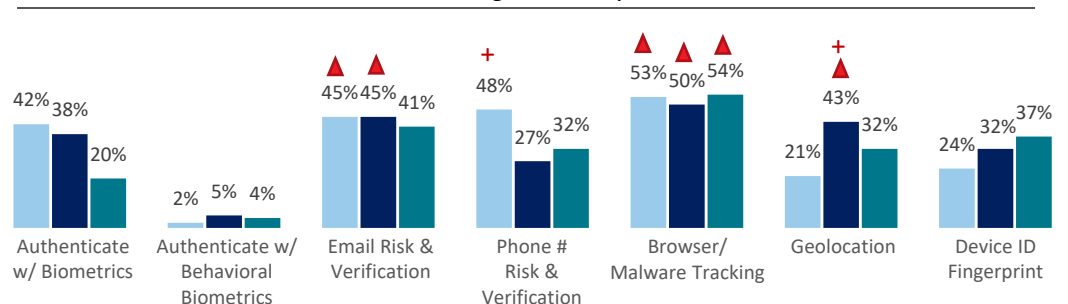
2019 %

36% 37% 24%

35% 42% 42%

32% 47% 44%

Passive/Digital Identity-based



n/a

24% 33% 33%

51% 26% 33%

36% 35% 37%

23% 28% 28%

30% 34% 36%

2020

TRUE COST OF FRAUD™
FINANCIAL SERVICES &
LENDING STUDY

Overview



Key Findings



#1

Attacks & Costs



#2

Trends



#3

Challenges & Impacts



#4

Potential COVID-19
Impacts

#5

Solutions Use



#6

Strategic Approaches



Recommendations

Survey Question:
Q27: Which of the
following fraud
solutions does
your company
currently use?Advanced ID
AuthenticationIncreased solutions adoption has occurred for both digital and non-digital
lending firms.

This has occurred more among lending than financial services firms.

Fraud Mitigation Solutions Usage

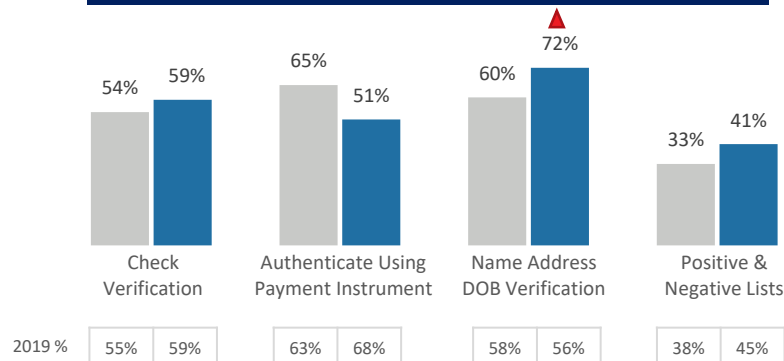


US Lending Firms

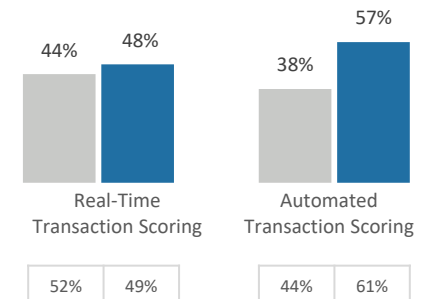
■ Non-digital

■ Digital

Basic Verification & Transaction

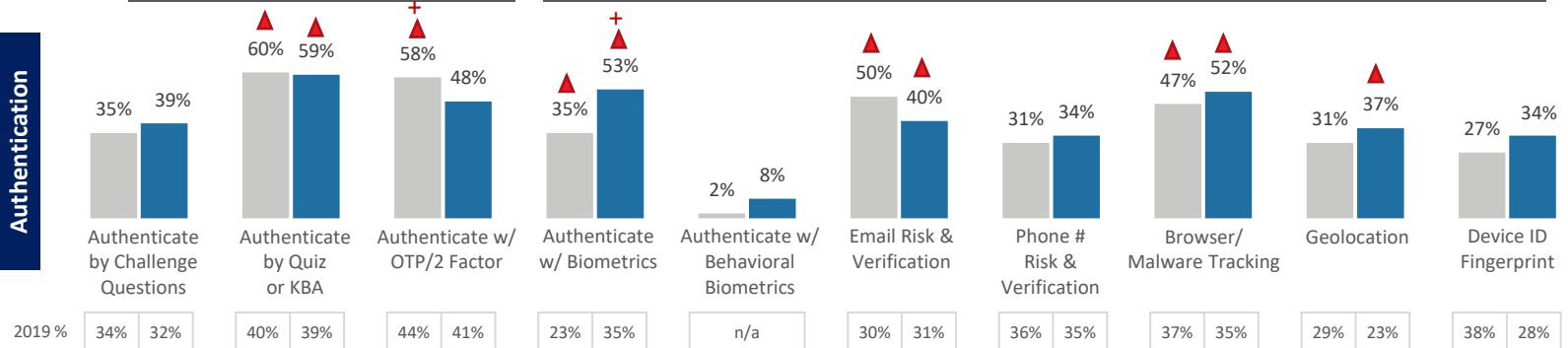


Advanced ID & Transaction Verification



Active/Interactive

Passive/Digital Identity-based



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
#1	Attacks & Costs
#2	Trends
#3	Challenges & Impacts
#4	Potential COVID-19 Impacts
#5	Solutions Use
#6	Strategic Approaches
	Recommendations

Advanced identity authentication and transaction verification solutions use is very limited among Canadian financial services and lending firms.

While many use email/phone risk and verification, there is more widespread use of traditional solutions.

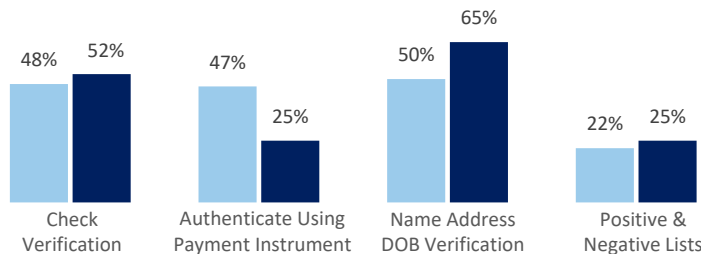
Fraud Mitigation Solutions Usage



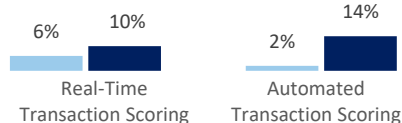
Canada Financial Services & Lending Firms

Overall Financial Services Overall Lending

Basic Verification & Transaction

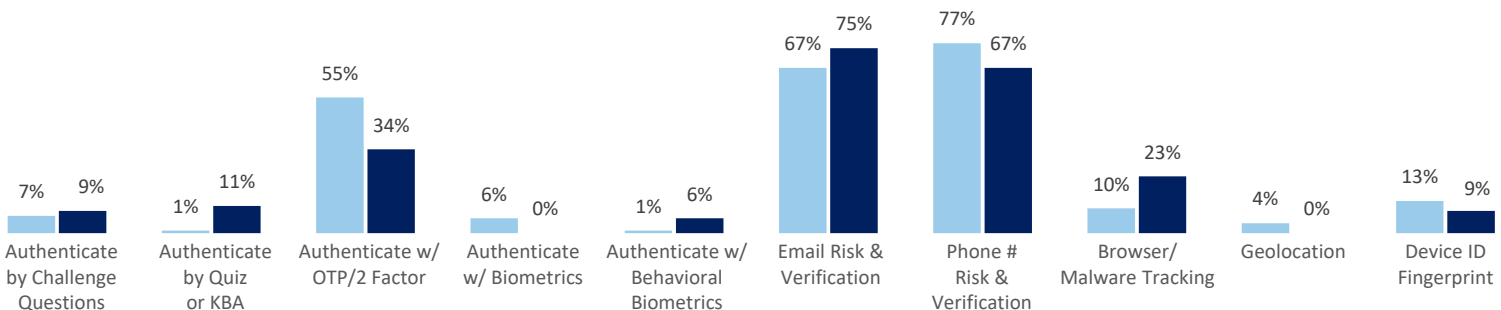


Advanced ID & Transaction Verification



Active/Interactive

Passive/Digital Identity-based



Advanced ID Authentication

Survey Question:
Q27: Which of the
following fraud
solutions does
your company
currently use?

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
#1	Attacks & Costs
#2	Trends
#3	Challenges & Impacts
#4	Potential COVID-19 Impacts
#5	Solutions Use
#6	Strategic Approaches
	Recommendations

Survey Question:
Q27: Which of the
following fraud
solutions does
your company
currently use?

Advanced ID
Authentication

Limited solutions use is similar among digital and non-digital firms.

As mentioned earlier, the complexity of synthetic identity fraud and botnet attacks requires more sophisticated solutions to assess the whole person from a digital behavior and physical identity perspective. The limited use of these explains the challenges highlighted earlier with identity verification, botnet attacks, and account-related fraud.

Fraud Mitigation Solutions Usage

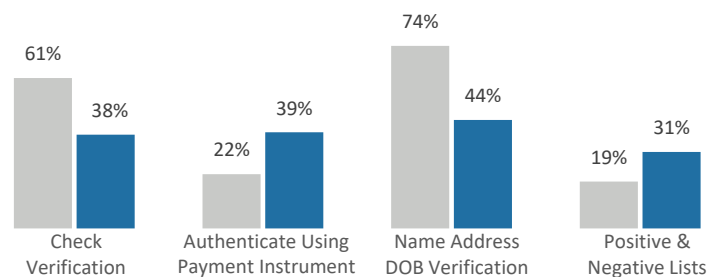


**Canada Financial Services
& Lending Firms**

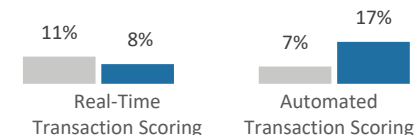
■ Non-digital

■ Digital

Basic Verification & Transaction

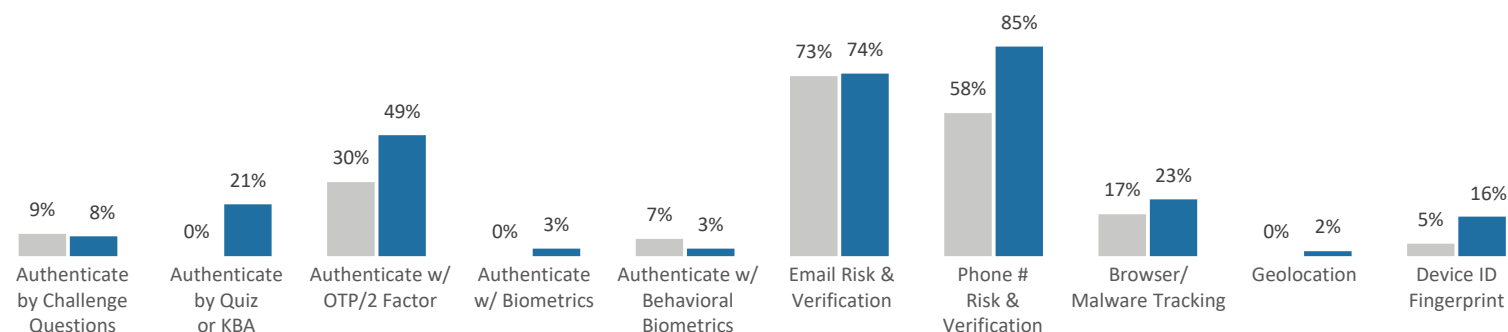


Advanced ID & Transaction Verification



Active/Interactive

Passive/Digital Identity-based



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Questions: Q28b: In addition to solutions, what supportive capabilities is your company using to help fight fraud?	

In addition to risk mitigation solutions, a number of U.S. investment firms and larger banks also use crowdsourcing, cybersecurity alerts and rules-based approaches. Just under half of larger banks also use AI/ML models.

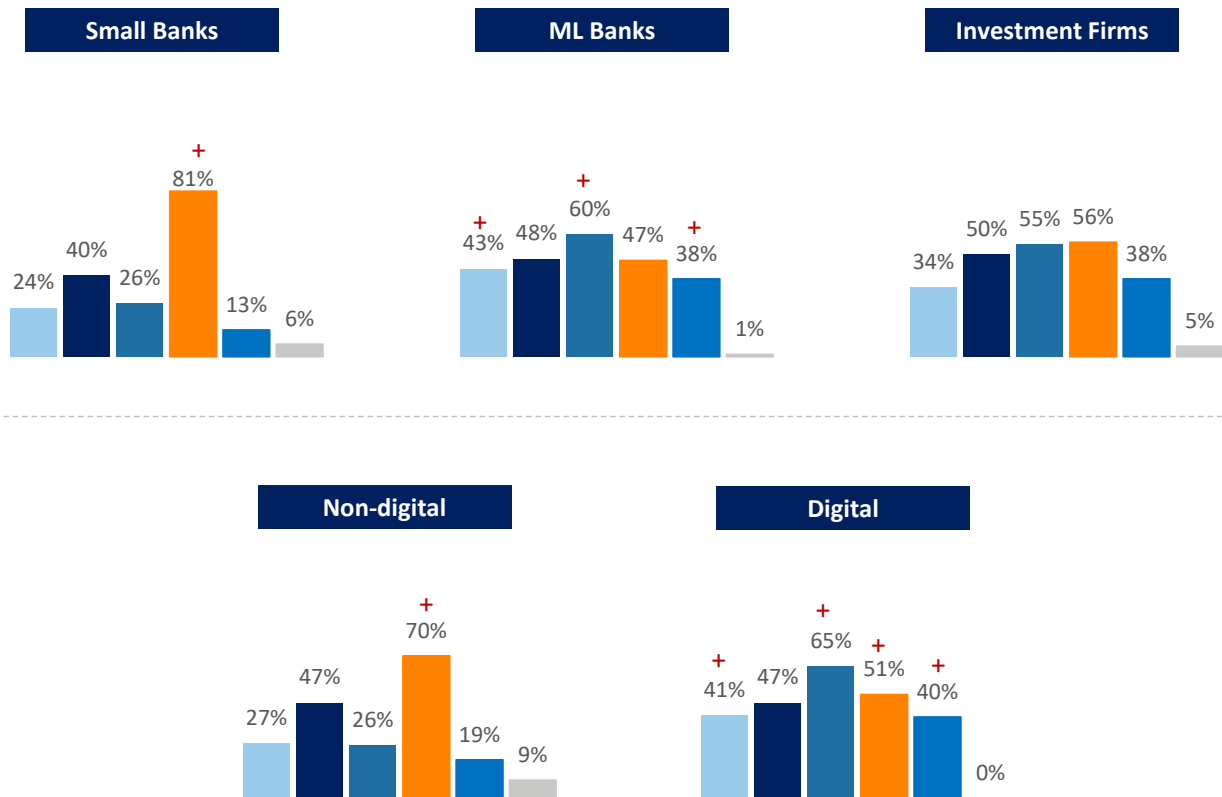
These capabilities are found more among digital than non-digital firms, which can contribute to earlier cited online and mobile channel challenges among non-digital firms.

Supportive Capabilities Usage



US Financial Services Firms

■ AI/ML models ■ Crowdsourcing ■ Cybersecurity alerts ■ Rules-based approaches ■ Social media intelligence ■ Not sure



+ = significantly higher than the segment counterpart

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
#1	Attacks & Costs
#2	Trends
#3	Challenges & Impacts
#4	Potential COVID-19 Impacts
#5	Solutions Use
#6	Strategic Approaches
	Recommendations
Survey Questions: Q28b: In addition to solutions, what supportive capabilities is your company using to help fight fraud?	

Rules-based approaches are prevalent across U.S. lending firms, while crowdsourcing and social media intelligence is limited.

Larger credit lenders are more likely than others to rely on cybersecurity alerts and AI/ML models.

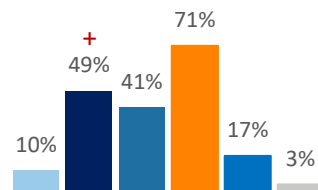
Supportive Capabilities Usage



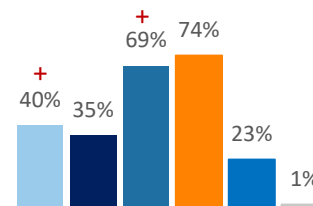
US Lending Firms

AI/ML models
 Crowdsourcing
 Cybersecurity alerts
 Rules-based approaches
 Social media intelligence
 Not sure

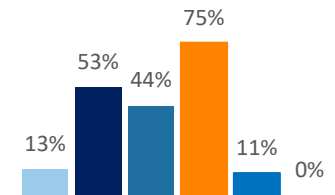
Small Credit Lenders



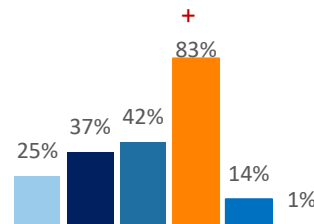
ML Credit Lenders



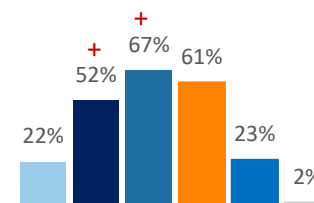
Mortgage Lenders



Non-digital



Digital



⁺ = significantly higher than the segment counterpart

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Questions: Q28b: In addition to solutions, what supportive capabilities is your company using to help fight fraud?	

Rules-based approaches are also prevalent across Canadian financial services and lending firms, with digital financial services organizations also relying on cybersecurity alerts.

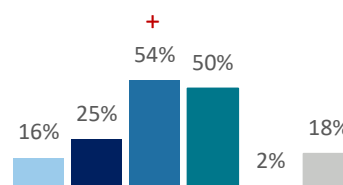
Supportive Capabilities Usage



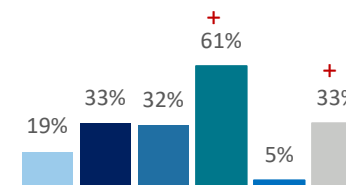
Canada Financial Services & Lending Firms

AI/ML models
 Crowdsourcing
 Cybersecurity alerts
 Rules-based approaches
 Social media intelligence
 Not sure

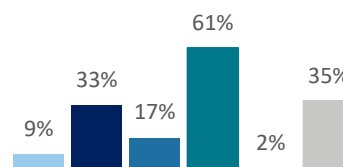
Overall Financial Services



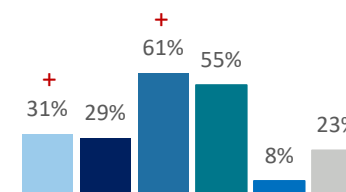
Overall Lending



Non-digital



Digital





Overview



Key Findings



#1

Attacks & Costs



#2

Trends



#3

Challenges & Impacts



#4

Potential COVID-19
Impacts

#5

Solutions Use



#6

Strategic Approaches



Recommendations

Key Finding #6: There is movement towards cloud-based solutions and the integration of cybersecurity, the digital customer experience and fraud prevention efforts.

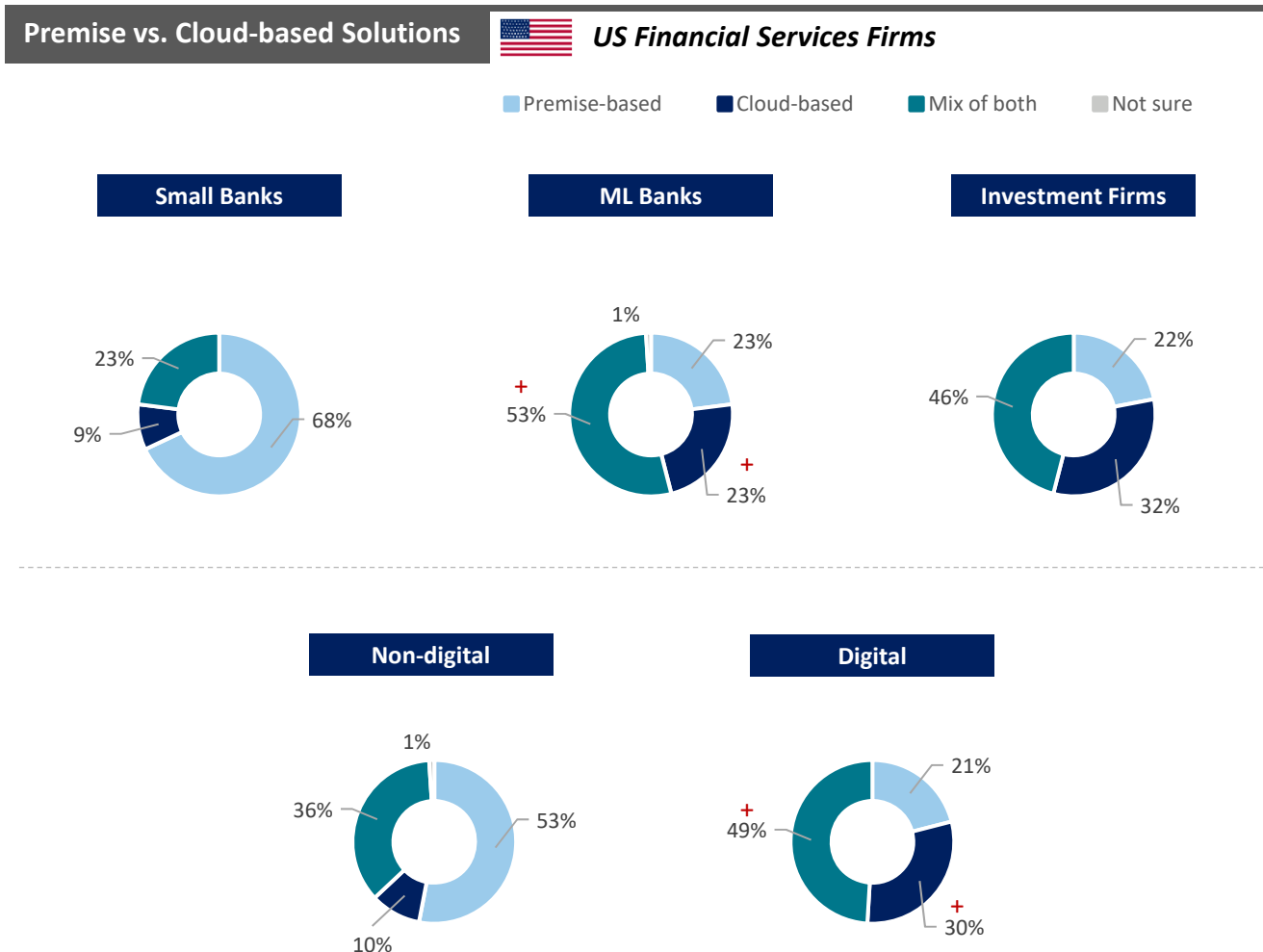


- Cloud-based solutions are more likely to be implemented by larger firms with a digital business model at this stage.
- The integration of fraud prevention with cybersecurity and the digital customer experience is occurring across a broader range of organizations small-to-large and digital and non-digital. That said, this is more often found among U.S. than Canadian firms at this point.

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
#1	Attacks & Costs
#2	Trends
#3	Challenges & Impacts
#4	Potential COVID-19 Impacts
#5	Solutions Use
#6	Strategic Approaches
	Recommendations
Survey Questions: Q28a: Are your fraud solutions:	

Cloud-based fraud mitigation solutions are prevalent among larger digital banks and investment firms. That said, this often is comprised of a mix of cloud and on-premises solutions.

Smaller and non-digital U.S. financial services firms lean towards premise-based solutions, many of which are likely legacy ones.



+ = significantly higher than the segment counterpart

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
#1	Attacks & Costs
#2	Trends
#3	Challenges & Impacts
#4	Potential COVID-19 Impacts
#5	Solutions Use
#6	Strategic Approaches
	Recommendations
Survey Questions: Q28a: Are your fraud solutions:	

Mortgage lending and larger digital U.S. credit lending firms are likely to also have a mix of cloud and on-premises risk mitigation solutions.

Smaller and non-digital U.S. lending firms also lean towards premise-based solutions, many of which are likely legacy ones.

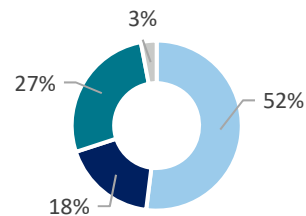
Premise vs. Cloud-based Solutions



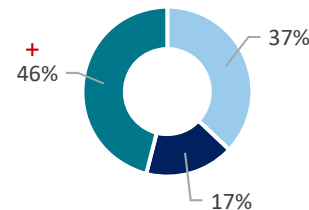
US Lending Firms

■ Premise-based
 ■ Cloud-based
 ■ Mix of both
 ■ Not sure

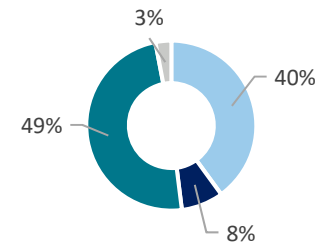
Small Credit Lenders



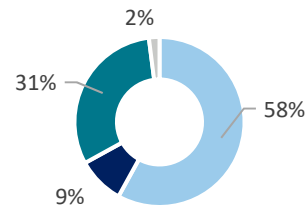
ML Credit Lenders



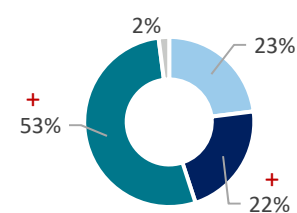
Mortgage Lenders



Non-digital



Digital



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Questions: Q28a: Are your fraud solutions:	

Digital Canadian financial services and lending firms are also likely to use a mix of cloud and premise-based solutions, more so compared to smaller, non-digital firms.

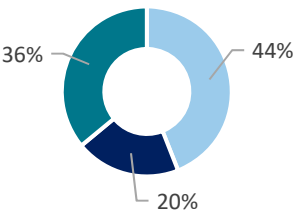
Premise vs. Cloud-based Solutions



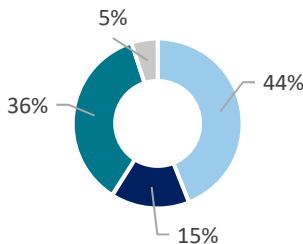
Canada Financial Services & Lending Firms

■ Premise-based
 ■ Cloud-based
 ■ Mix of both
 ■ Not sure

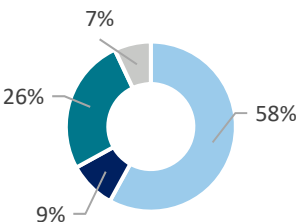
Overall Financial Services



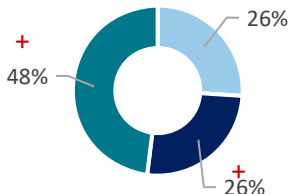
Overall Lending



Non-digital



Digital



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations

Survey Questions:
Q29: To what degree has your company integrated its cybersecurity operations with its fraud prevention efforts? Q30b: To what degree has your company integrated its digital/customer experience operations with its fraud prevention efforts?

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

There is movement among U.S. financial services firms toward integrating fraud prevention efforts with cybersecurity operations and the digital / customer experience, with most at a partially integrated stage.

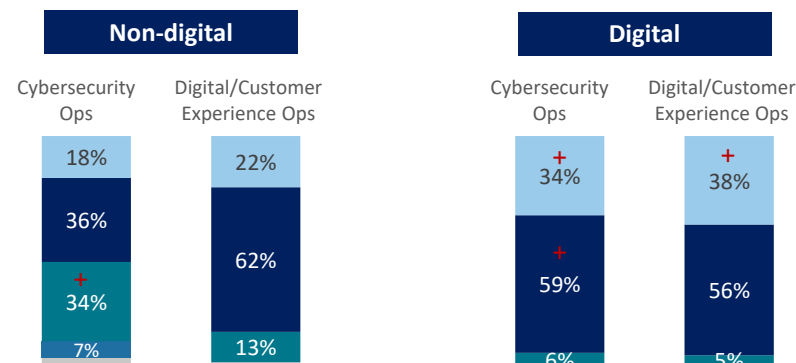
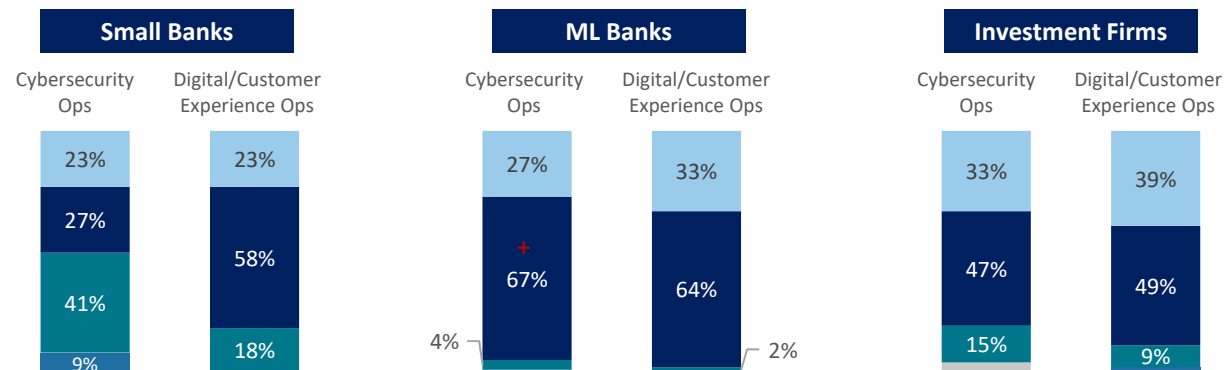
Given similar percentages for partial cybersecurity and digital CS integration among investment firms and mid/large banks that are digital, this would suggest that they are focusing on both at the same time.

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



US Financial Services Firms

■ Fully
 ■ Partially
 ■ Not at all
 ■ N/A; don't have formal operations
 ■ Not sure

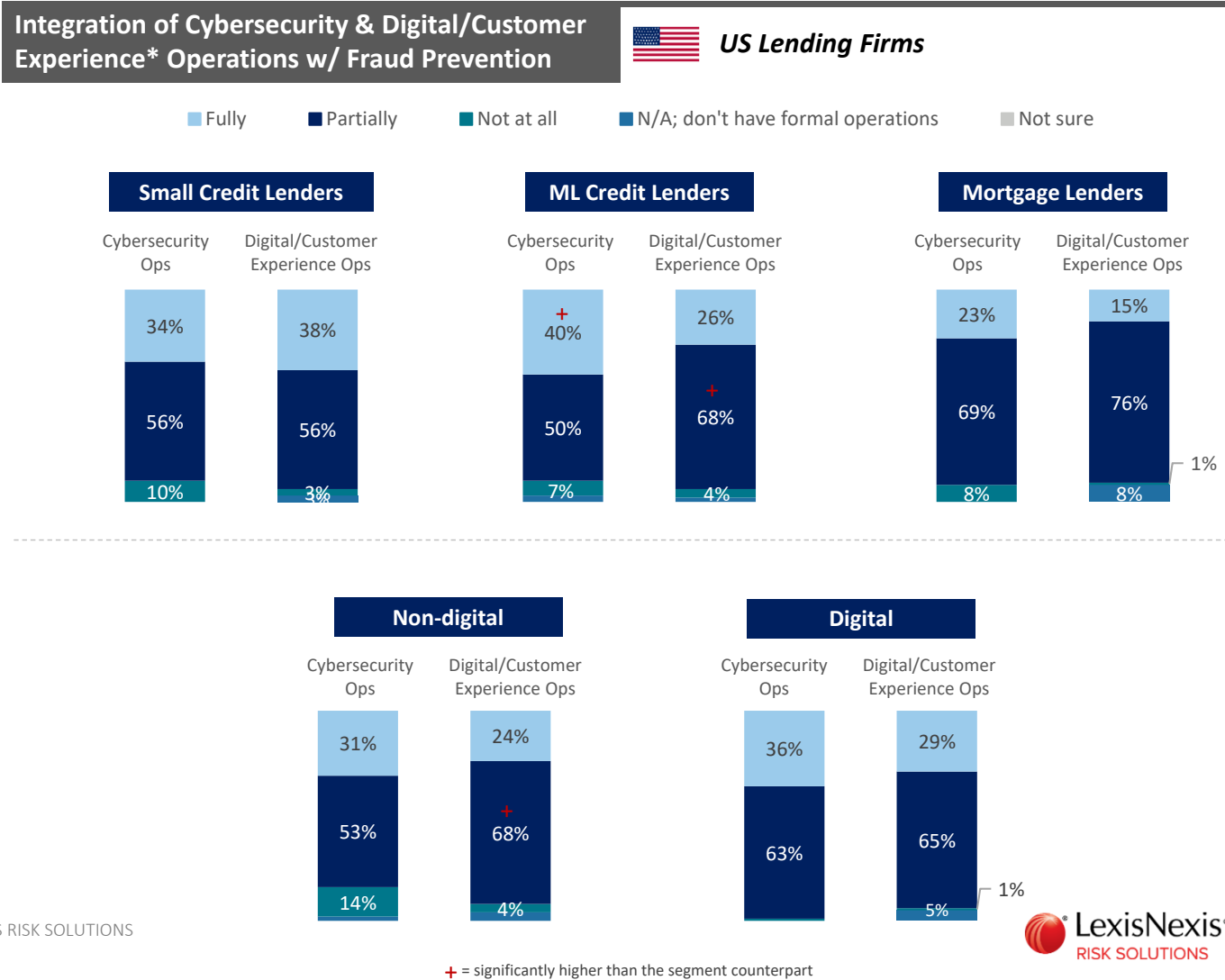


+ = significantly higher than the segment counterpart

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
#1	Attacks & Costs
#2	Trends
#3	Challenges & Impacts
#4	Potential COVID-19 Impacts
#5	Solutions Use
#6	Strategic Approaches
	Recommendations
Survey Questions: Q29: To what degree has your company integrated its cybersecurity operations with its fraud prevention efforts? Q30b: To what degree has your company integrated its digital/customer experience operations with its fraud prevention efforts?	

Somewhat more credit lending firms indicate full integration of cybersecurity and fraud prevention efforts compared to mortgage lenders and financial services firms.

While a majority of lending firms indicate being at least partially integrated with one or the other, there does not seem to be as much of a combined focus as found with financial services firms.



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

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations

Survey Questions:
Q29: To what degree has your company integrated its cybersecurity operations with its fraud prevention efforts? Q30b: To what degree has your company integrated its digital/customer experience operations with its fraud prevention efforts?

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

Just over half of Canadian financial services and lending firms are moving towards fraud prevention integration with the digital customer experience, but less fraud and cybersecurity integration at this point.

Many non-digital firms indicate that they don't have formal plans for integrating fraud prevention with cybersecurity, which puts them at risk given the rise of cybersecurity threats.

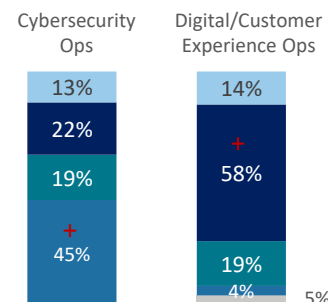
Integration of Cybersecurity & Digital/Customer Experience* Operations w/ Fraud Prevention



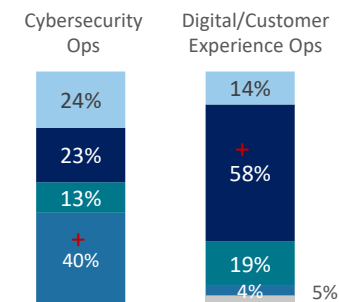
Canada Financial Services & Lending Firms

■ Fully
 ■ Partially
 ■ Not at all
 ■ N/A; don't have formal operations
 ■ Not sure

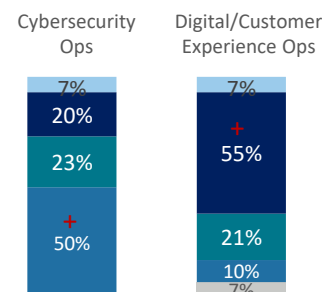
Overall Financial Services



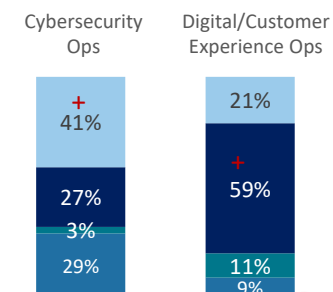
Overall Lending



Non-digital



Digital



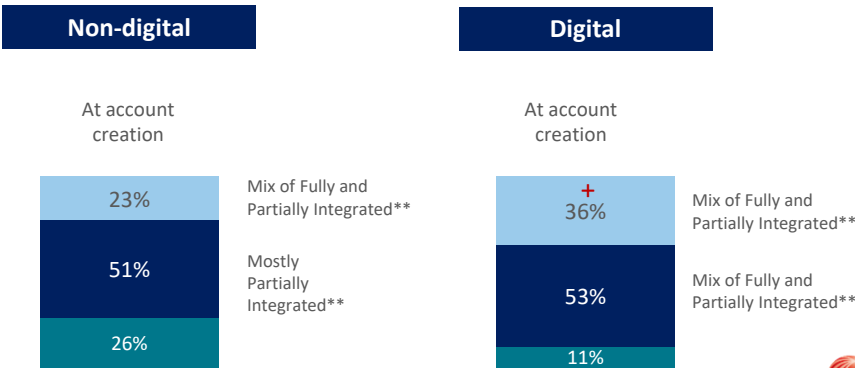
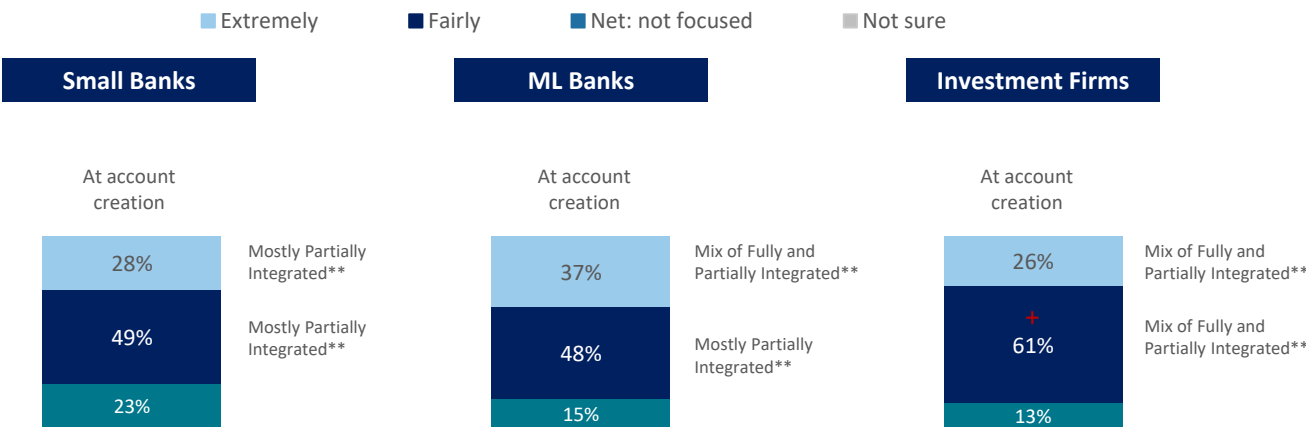
⁺ = significantly higher than the segment counterpart

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Questions: Q30: To what degree is your company focused on minimizing customer friction during an online/mobile transaction checkout? Q30a: To what degree is your company focused on minimizing customer friction during online/mobile account opening?	

A majority of U.S. financial services firms that have partially or fully integrated fraud prevention and the digital customer experience are at least fairly focused on minimizing customer friction in the remote channels.

That indicates that there are additional reasons for these integration efforts, such as improving identity verification efforts to reduce the risk of fraud and its associated costs.

Degree Company is Focused on Minimizing Customer Friction Through Online/Mobile Channels* US Financial Services Firms



*asked of those with online and/ or mobile channel translations
 ** Integration of digital / customer experience with fraud prevention

+ = significantly higher than the segment counterpart

2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
#1	Attacks & Costs
#2	Trends
#3	Challenges & Impacts
#4	Potential COVID-19 Impacts
#5	Solutions Use
#6	Strategic Approaches
	Recommendations
<p>Survey Questions: Q30: To what degree is your company focused on minimizing customer friction during an online/mobile transaction checkout? Q30a: To what degree is your company focused on minimizing customer friction during online/mobile account opening?</p>	

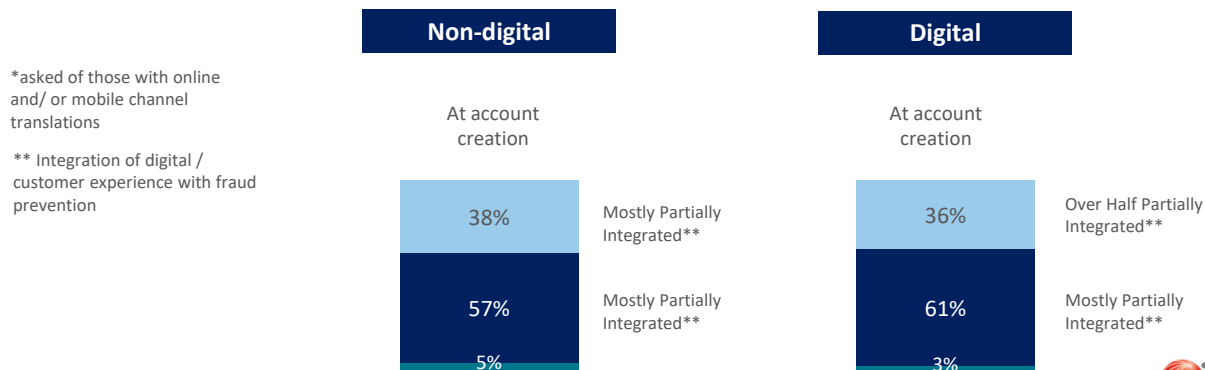
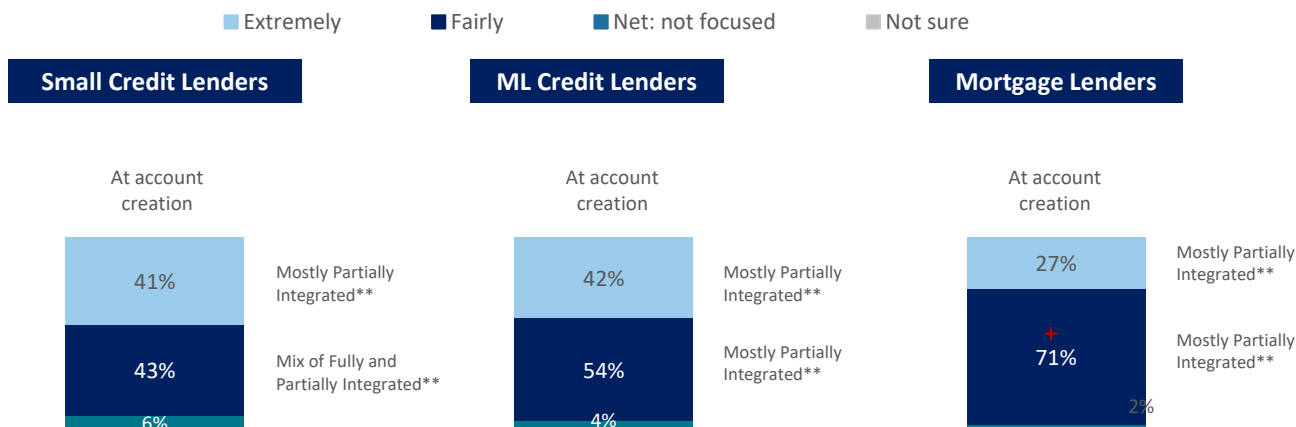
A majority of U.S. lending firms that have partially or fully integrated fraud prevention and the digital customer experience are also at least fairly focused on minimizing customer friction in the remote channels.

Again, this points to additional reasons for such integration.

Degree Company is Focused on Minimizing Customer Friction Through Online/Mobile Channels*



US Lending Firms



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

** Integration of digital / customer experience with fraud prevention

+ = significantly higher than the segment counterpart

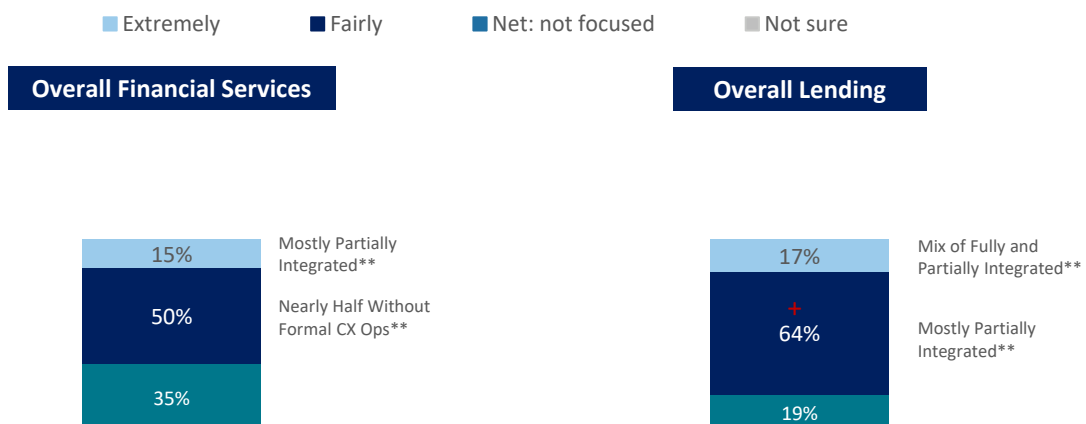
2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
#1	Attacks & Costs
#2	Trends
#3	Challenges & Impacts
#4	Potential COVID-19 Impacts
#5	Solutions Use
#6	Strategic Approaches
	Recommendations
<p>Survey Questions: Q30: To what degree is your company focused on minimizing customer friction during an online/mobile transaction checkout? Q30a: To what degree is your company focused on minimizing customer friction during online/mobile account opening?</p>	

Digital Canadian financial services and lending firms are fairly focused on minimizing customer friction through integration of fraud prevention and the digital experience.

Degree Company is Focused on Minimizing Customer Friction Through Online/Mobile Channels*



Canada Financial Services & Lending Firms



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

** Integration of digital / customer experience with fraud prevention

Recommendations



Overview



Key Findings



Attacks & Costs



Trends



Challenges & Impacts

Potential COVID-19
Impacts

Solutions Use



Strategic Approaches



Recommendations



- The combination of physical and digital identity analysis is essential.
- A multi-layered solution approach is most effective for fighting fraud across various channels and transaction types.
- Financial services and lending firms need to be very prepared for increased fraud attacks for the foreseeable future.
- Protecting the customer relationship and brand is an important part of fraud prevention; it isn't just about the cost of fraud.
- More sophisticated global crime networks require more real-time, third-party data and analysis to detect and prevent fraud and its collateral damage.



Overview



Key Findings



#1

Attacks & Costs



#2

Trends



#3

Challenges & Impacts



#4

Potential COVID-19
Impacts

#5

Solutions Use



#6

Strategic Approaches



Recommendations

Recommendations

1) To effectively fight fraud generated by botnets and synthetic identities, it is important to combine physical and digital identity data, and analysis to get the full view of the “customer”.

- These sophisticated threats are increasing, which negatively impacts financial services and lending firms with high fraud costs and potentially lost customers.
- Botnets and synthetic identities are difficult to detect using traditional risk mitigation solutions because they can mimic real persons and transactions. Using traditional identifiable data alone may miss these.
- Digital identity and behavioral biometrics data and analysis is essential for detecting anomalies based on device use, linkages, remote channel behaviors, locations and patterns. This will also support machine learning to prevent fraud before it occurs. Combining digital with physical identification data provides a comprehensive view for distinguishing between the real and synthetic or botnet “customer”.

2) A multi-layered solution approach is essential to protect financial services and lending firms throughout a single buyer experience. Each transaction channel and type carries unique risks.

- Using different solutions to support fraud detection at various points in the customer journey, including at onboarding, will strengthen overall protection.
- An example of this could involve:
 - Velocity checks / real-time scoring during onboarding to determine risk of the transaction; for account access, the use of multiple screening tools, including two-factor authentication, is important since fraudsters are experts at knowing the types of information that can get them through screening
 - Digital identity and behavioral biometrics can be used to distinguish legitimate customer from fraudster behavior
 - The use of passive, analytics-driven solutions will provide a more seamless and frictionless experience for the customer, including reducing the time involved for fraud assessment.



Overview



Key Findings



#1 Attacks & Costs



#2 Trends



#3 Challenges & Impacts

#4 Potential COVID-19
Impacts

#5 Solutions Use



#6 Strategic Approaches



Recommendations

Recommendations (cont.)

3) Financial services and lending firms very prepared for increased fraud attacks and costs for the foreseeable future.

- It is unclear what the landscape will look like over the next 1 -2 years as shaped by the COVID-19 pandemic.
- Will we see a return to pre-COVID-19 behaviors, or will there be a new normal that involves a higher level of online and mobile channel transactions than would have otherwise trended without the pandemic?
- If so, then firms could be faced with greater fraud spikes for at least for the foreseeable future. And since these will involve remote channels, the fraud techniques are more insidious and complex than those used with in-person transactions.
- Financial services and lending firms which have invested in digital identity and transaction fraud detection solutions cited earlier will be more prepared to deal with these sudden changes. As the cost of doing business rises in this COVID-19 environment, the *added cost* of fraud may become a negative tipping point for firms that haven't yet invested in these solutions.

4) As more transactions move to the online and mobile channels, the ability to compete becomes more challenging. Protecting customer relationships and your brand will become more important than ever.

- Consumers literally have more options at their fingertips, including abandoning a transaction that is burdensome. New customers may appreciate extra steps taken to verify their identity, such as providing passwords, answers to questions and one-time code numbers. Recurring customers may tire of this at some point based on the "you should know me by now" mindset. Not all transactions carry the same level of risk.
- Having risk mitigation solutions that allow you the flexibility of customizing verification efforts according to risk level can lessen friction.
- Customer relationships can be harmed if your customers become victims of fraud that is based on transactions with your business. Social media can further erode brand health where these grievances are shared.
- As a result, the investment in multi-layered solutions that assess both the digital and physical, individual and transactional attributes are important for not only protecting against fraud, but to also minimize the friction points and collateral damage caused by fraud.
- But there should be more to your fraud prevention strategy. It is crucial to have an approach that fully integrates these solutions with your cybersecurity and digital customer experience efforts as well, including the tracking of fraud by channel and transaction type.



Overview



Key Findings



Attacks & Costs



Trends



Challenges & Impacts

Potential COVID-19
Impacts

Solutions Use



Strategic Approaches



Recommendations

Recommendations (cont.)

5) Without more real-time, third-party data and analysis, financial services and lending will continue to struggle with various aspects for fraud, including identity verification and authentication.

- More online / mobile transaction will translate into faster customer experiences, with the need to quickly identify fraud and minimize friction.
- Those conducting international transactions will experience even further challenges without such real-time third-party data.
 - More complex and interconnected fraud rings using multiple devices and identity attributes can easily confuse the source of transaction origination.
 - Newer privacy regulations, such as GDPR, make it increasingly difficult for businesses to access and store customer data that is essential for effective identity verification and authentication.
- Payment gateways / providers can unknowingly be leveraged by fraudsters in order to hide behind complex transaction linkages, speed and volume of transactions hitting a firm and lack of transparency about the origination source and end customer.

2020

TRUE COST OF FRAUD™
FINANCIAL SERVICES &
LENDING STUDY

Appendix



Overview



Key Findings



Attacks & Costs



Trends



Challenges & Impacts



Potential COVID-19
Impacts



Solutions Use



Strategic Approaches



Recommendations



Appendix



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Questions: Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online/mobile channel.	

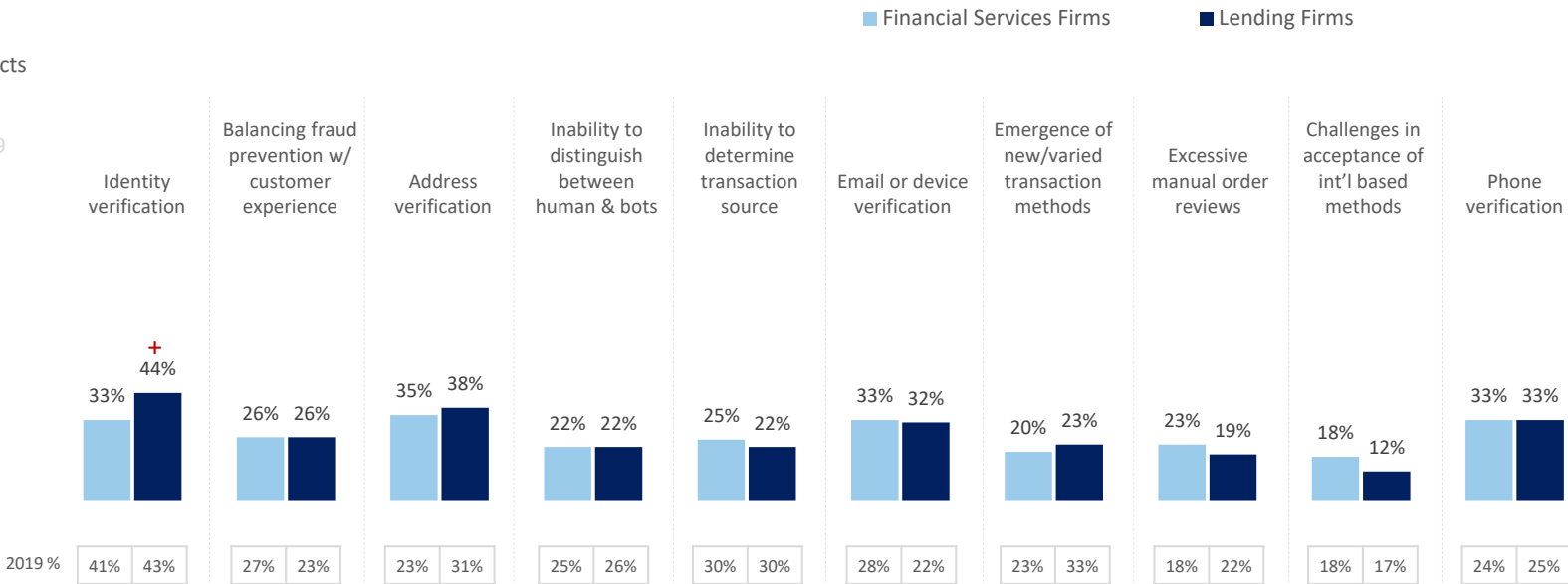
Identity verification, including those involving digital attributes (email/device, phone) are key online channel challenges at an overall level for U.S financial services and lending firms.



Fraud Challenges by ONLINE Channel (Top 3 ranked)



US Financial Services & Lending Firms



2020	TRUE COST OF FRAUD™ FINANCIAL SERVICES & LENDING STUDY
	Overview
	Key Findings
	Attacks & Costs
	Trends
	Challenges & Impacts
	Potential COVID-19 Impacts
	Solutions Use
	Strategic Approaches
	Recommendations
Survey Questions: Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online/mobile channel.	

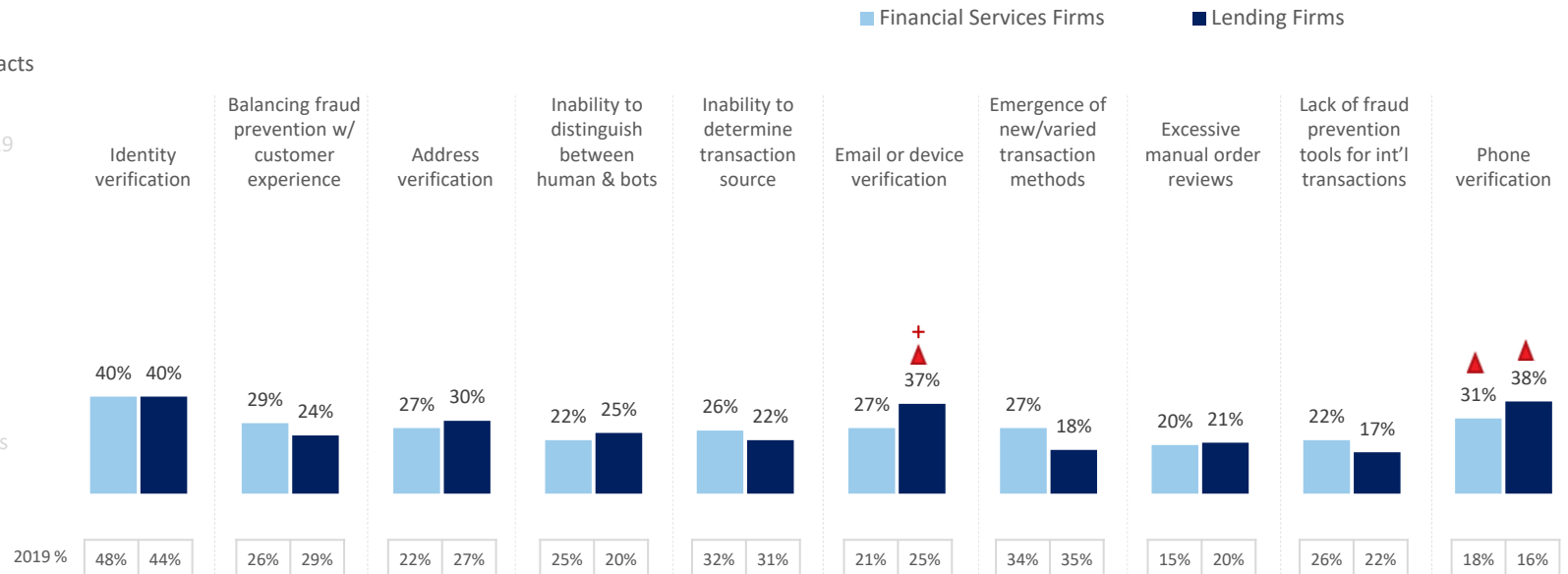
Identity verification, including those involving digital attributes (email/device, phone) are also key mobile channel challenges at an overall level for U.S. financial services and lending firms.



Fraud Challenges by MOBILE Channel (Top 3 ranked)



US Financial Services & Lending Firms



LexisNexis® Risk Solutions can help.

For more information:

risk.lexisnexis.com/FraudandIdentity

+1 800 953 2877



This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products identified. LexisNexis does not warrant this document is complete or error free. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. LexisNexis Fraud Multiplier is a service mark of RELX Inc. True Cost of Fraud is a trademark of LexisNexis Risk Solutions Inc. Copyright © 2020 LexisNexis. NXR14662-00-1020-EN-US