LexisNexis® Risk Solutions SMB Lending Fraud Study

February 2022

LexisNexis® RISK SOLUTIONS

Background

LexisNexis® Risk Solutions sought primary market research with lenders to understand small and midsize business (SMB) lending fraud. The intent is to generate insights in this area in order to create an industry benchmark to support lenders' efforts to stem SMB lending fraud and understand best practices.

Specific objectives included to understand:

- The volume of SMB lending fraud and through which channels;
- How SMB lending fraud is identified and tracked;
- The types of SMB fraud experienced;
- Priorities, internal activities, and levels of investment for curbing SMB lending fraud, including solutions usage; and
- Any differences in the above by size or type of organization.

Methodology

LexisNexis® Risk Solutions retained KS&R, a global market research firm, to conduct this research study.

- Data was collected by phone during August and September 2021. A total of 149 completions were obtained, broken out as follows:

Total	<$10B Asset Banks/Credit Unions	$10B+ Asset Banks/Credit Unions	Fintech/Digital Lenders	Payment Processors*
149	51	63	23	12

- Respondents included those with responsibility for making risk and fraud assessments/decisions for current and potential SMB customers.
- SMBs were defined as businesses earning up to $10,000,000 in annual revenue.
- LexisNexis® Risk Solutions was not identified as the sponsor of the research in order to lessen potential for brand bias.

*Though included in the data set and reflected in total-level findings, payment processors are not reported as a segment due to low N size.

Fraud Type Descriptions

The following descriptions of fraud types were presented in the survey:

Bogus business	Either an existent business entity fabricated to commit fraud, or a non-existent business fabricated to commit fraud
Stolen legitimate business	Takeover or misrepresentation of ownership of a business with the intent to commit fraud
Fake consumer identity	False/synthetic identity created to commit fraud
Stolen consumer identity	Identity theft using the true name of the owner/authorized representative of a business

Summary of Key Findings

1. SMB lending fraud has increased at a higher rate since 2019 and early 2020, costing lenders more as a percent of revenues and hitting larger banks and Fintech's most.

2. COVID-19 has significantly contributed to increased SMB lending fraud and costs.

3. Use of the mobile channel is also driving increased SMB lending fraud, some of which is also influenced by COVID-19.

4. SMB lenders expect to increase their investment in fraud mitigation prevention, with a focus on additional labor resources which will drive up costs.

5. Study findings show that lenders which use a multi-layered solutions approach to assess fraud risk by various transaction channels, by physical and digital identity attributes and by transaction have experienced a lower year-over-year (YOY) increase in SMB lending fraud.

Key Finding #1: SMB lending fraud has increased at a higher rate since 2019 and early 2020, costing lenders more as a percent of revenues and hitting larger banks and Fintech's most.

Fraud cost as a percent of revenues is highest for Fintech's, though has seen the sharpest year-over-year (YOY) rise among larger banks.

Significantly more fraud prevention costs have involved labor compared to early 2020, as lending faced increase loan requests based on PPP and battled more fraud related to bogus business credentials and fake or stolen consumer identities.

Identity fraud, based on scams stealing legitimate consumer and business identities, have particularly challenged larger banks.

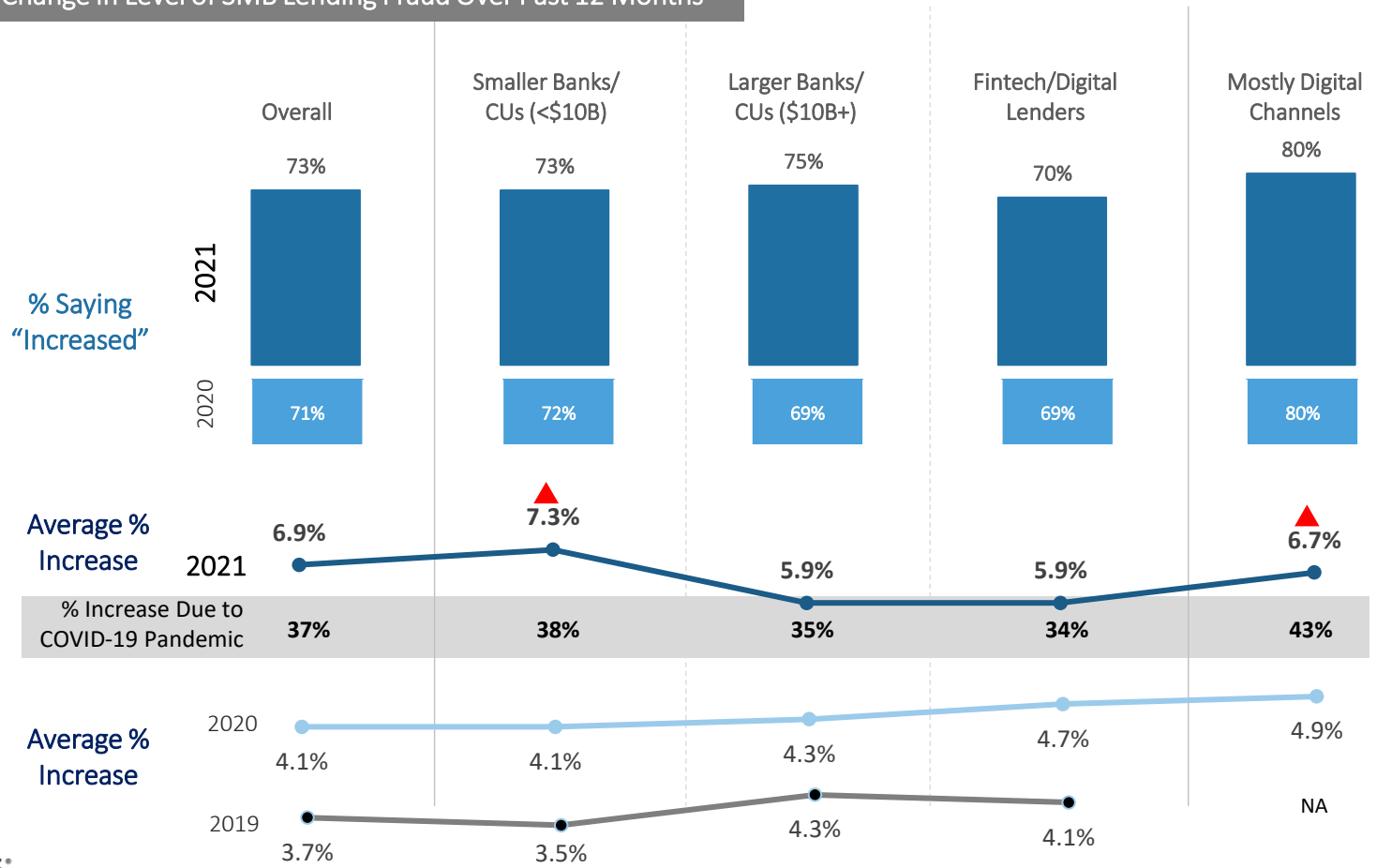
SMB lending fraud has increased at a higher rate since 2019, with the COVID-19 pandemic accounting for over one-third of this.

Smaller banks, credit unions, and firms with a sizeable volume of digital transactions have experienced the largest year-over-year (YOY) fraud increase. That said, fraud volumes have increased for larger firms as well as later findings will show that larger firms are getting hit by SMB fraud.

Those processing a sizeable volume of loans through digital channels indicate an even larger cost increase due to COVID-19.

Survey Q5: Over the past 12 months, has SMB lending fraud targeted at your company increased or decreased and by how much?

Change in Level of SMB Lending Fraud Over Past 12 Months



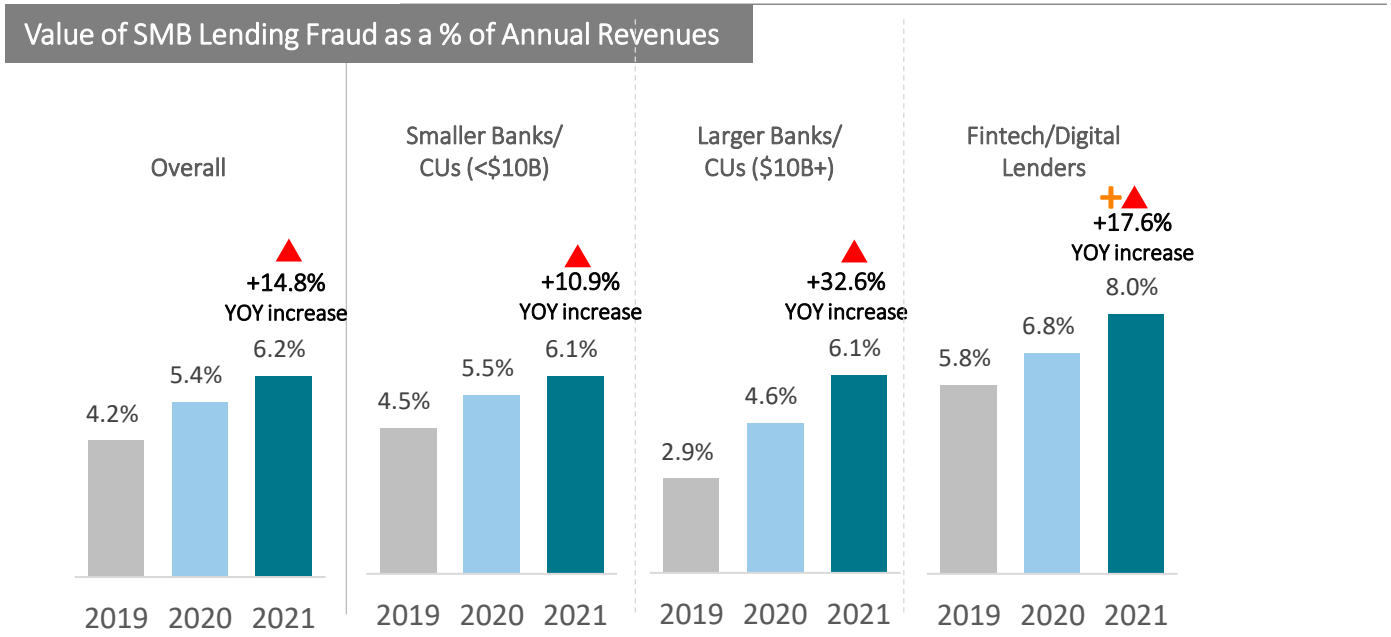
= significantly or directionally different from 2020, within segment

And, SMB lending fraud losses are accounting for a significantly higher percent of financial firms' annual revenues year-over-year (YOY) (6.2% more overall), with larger banks and Fintech's seeing a sharper YOY change.

SMB lending fraud as a percent of revenues continues to be highest for Fintech's, with a sizeable 17.6% increase over last year.

However, larger banks have seen the largest YOY increase (32.6%), catching up to smaller banks.

Survey Q8: What is the approximate value of your company's total fraud losses over the past 12 months, as a % of annual revenues?



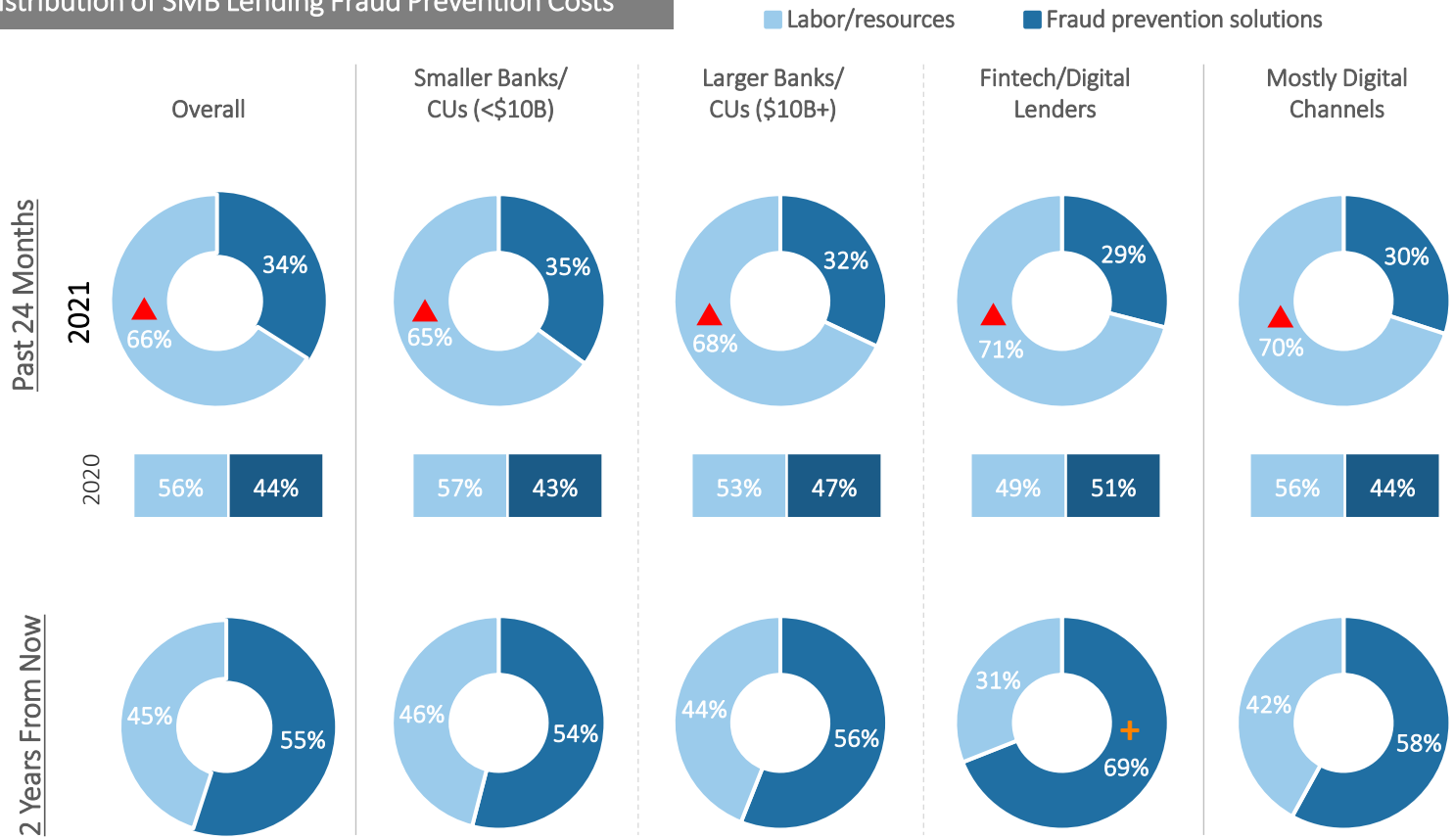
+ = significantly or directionally different from other segments, 2021

▼▲ = significantly or directionally different from 2020, within segment

Past 24-month spending heavily towards labor, though that could change depending on the direction of the COVID-19 pandemic.

In fact, labor-focused spending increased significantly, with much of that likely occurring during the early pandemic period in order to deal with deluge of volume related to PPP loans. Financial institutions currently anticipate returning to a more balanced or slightly leaning solutions distribution of fraud prevention spend over the next two years. However, that could change depending on the market and COVID-19.

Distribution of SMB Lending Fraud Prevention Costs



Survey Q25a: What has been the percentage distribution of SMB lending fraud prevention costs across the following areas over the past 12 mths?*
Q25b: And what do you expect the distribution of SMB lending fraud prevention costs across the following areas will be 2 years from now?

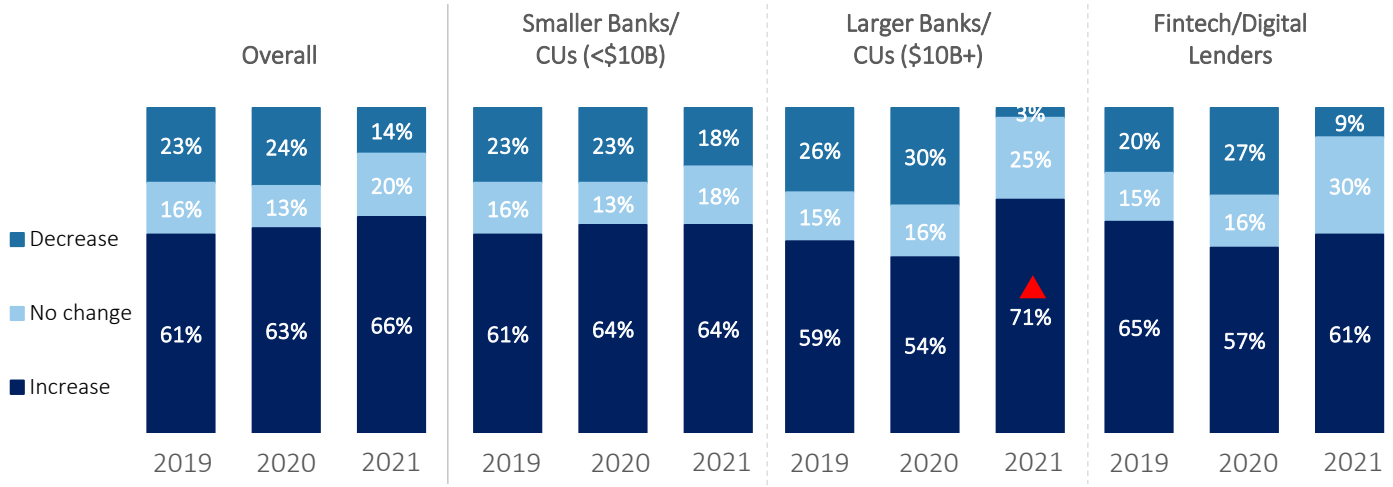
+ = significantly or directionally different from other segments, 2021

▼▲ = significantly or directionally different from 2020, within segment

Many continue to expect increasing fraud levels with SMB lending, with significantly more of the larger banks/credit unions concerned about this than recent years.

The average expected increase cited across segments is approximately 5%, which is above the 2019-2020 levels, though under the recent past 12-month period (5.9% - 7.3%).

Expected Change in SMB Lending Fraud Levels in the next 12 months



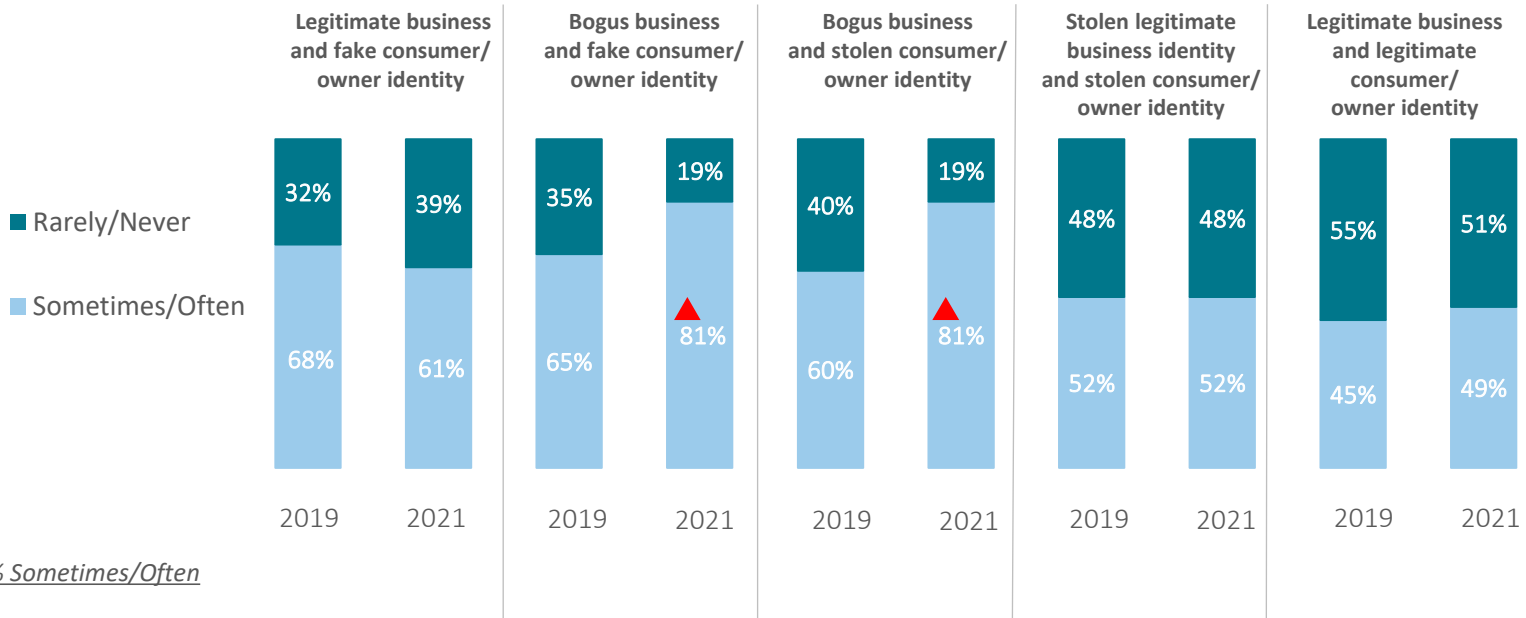
Survey Q6: For 2020, do you expect SMB lending fraud targeted at your company to increase or decrease and by how much?

▲▼ = significantly or directionally different from 2020, within segment

SMB lending fraud related to bogus business credentials and fake or stolen consumer / owner identities is occurring more often than pre-COVID-19.

Larger banks / credit unions have also experienced more frequent SMB lending fraud involving the use of legitimate consumer and business identity information since before COVID-19. All of this has a relationship to PPP/CARES Act fraud. Fraudsters used stolen identity / Social Security data and Employer Identification numbers (EIN)s during disbursement of these loans.[1] There is risk that fraudsters will continue to use this stolen data.

Frequency With Which Fraud Types Are Experienced



*Survey Q17: How often does your company experience the following types of SMB lending fraud?**

% Sometimes/Often

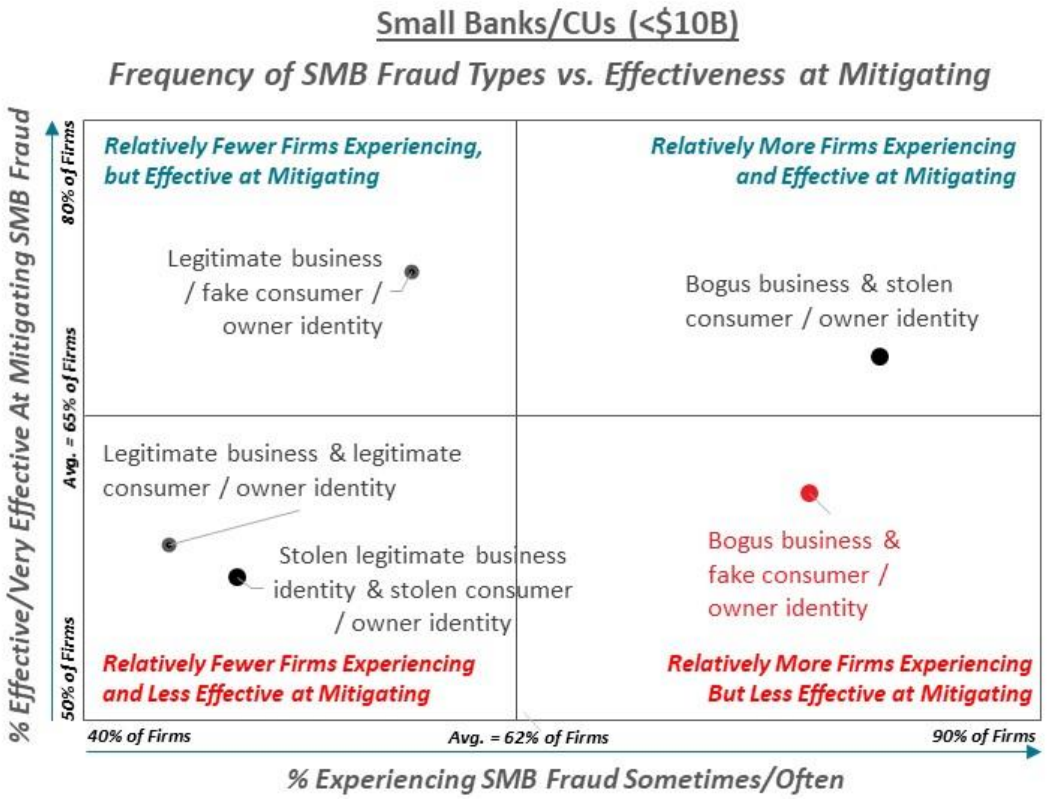
	2019	2021	2019	2021	2019	2021	2019	2021	2019	2021
Small Banks/CUs (<$10B)	71%	57%	68%	80% ▲	60%	84% ▲	56%	47%	45%	43%
Large Banks/CUs ($10B+)	60%	70% ▲	55%	83% ▲	57%	71% ▲	43%	63% ▲	45%	60% ▲
Fintech/Digital Lenders	73%	61%	81%	96% ▲	65%	91% ▲	50%	48%	62%	48%

[1] https://www.idtheftcenter.org/sba-loan-identity-fraud-continues-to-grow-into-2021/

▼▲ = significantly or directionally different from 2020, within segment

With increased frequency of the bogus business fraud scams, small banks/credit unions indicate that they are less effective at mitigating risks when involving fake consumer or owner identities.

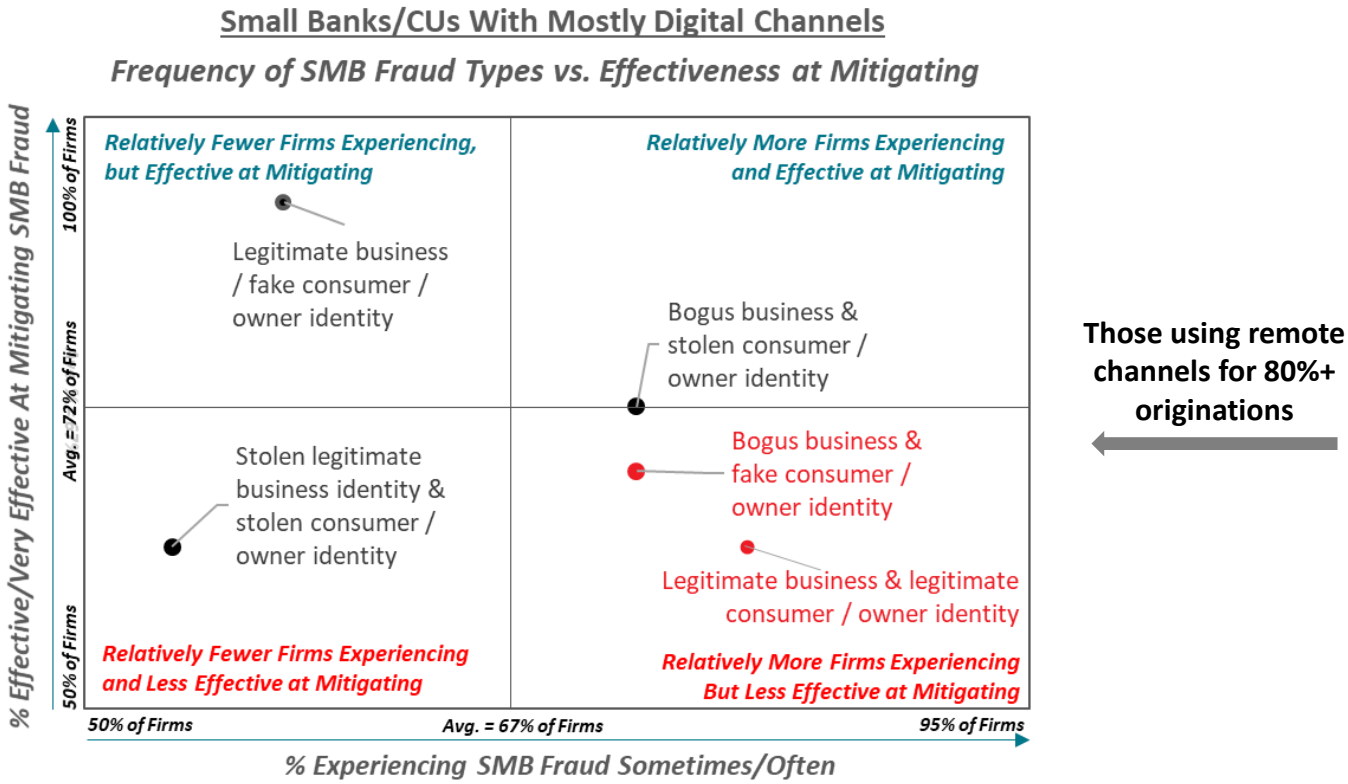
That suggests the use of synthetic identities which are particularly difficult to distinguish from legitimate ones.



Survey Q17: How often does your company experience the following types of SMB lending fraud? Q18: How effective is your company at mitigating the following permutations of SMB lending fraud?

The risk of fraud grows for smaller banks/credit unions that originate a significant majority of SMB loans via online/mobile channels.

In addition to challenges with mitigating SMB fraud involving bogus business and fake consumer/owner identities, many of these smaller digital banks are also less effective at mitigating fraud involving legitimate business and consumer/owner identities.

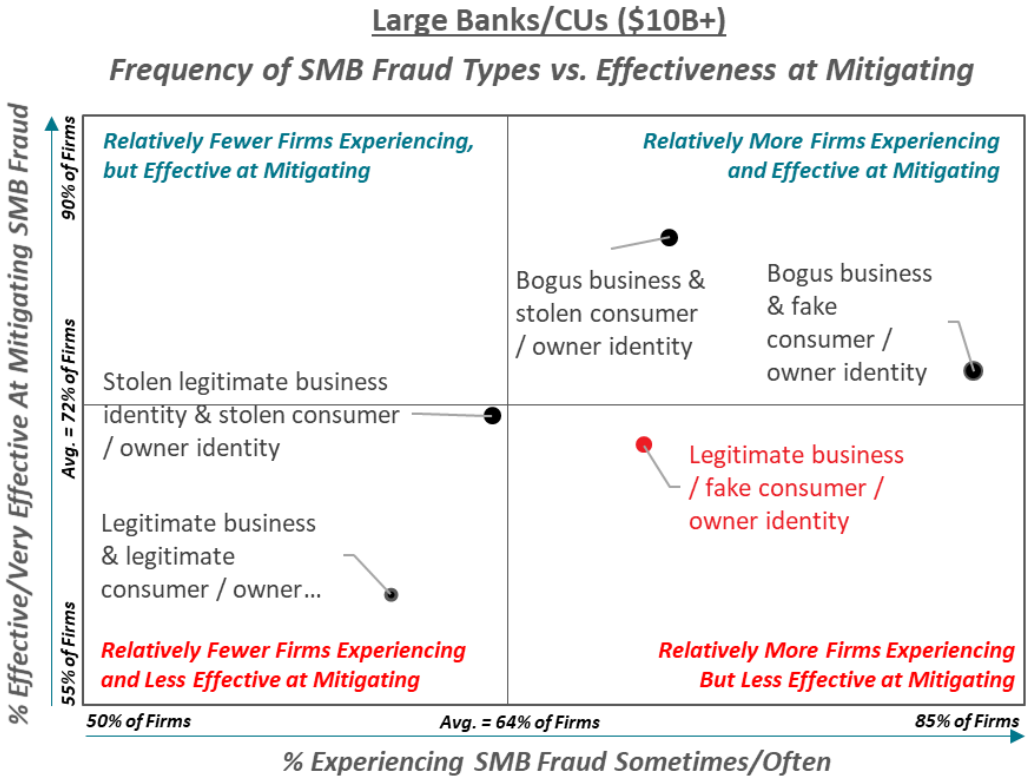


Those using remote channels for 80%+ originations

Survey Q17: How often does your company experience the following types of SMB lending fraud? Q18: How effective is your company at mitigating the following permutations of SMB lending fraud?

Large banks/credit unions say they are effective at catching bogus business fraud, though less effective when a legitimate business identity is coupled with fake consumer or owner identity data.

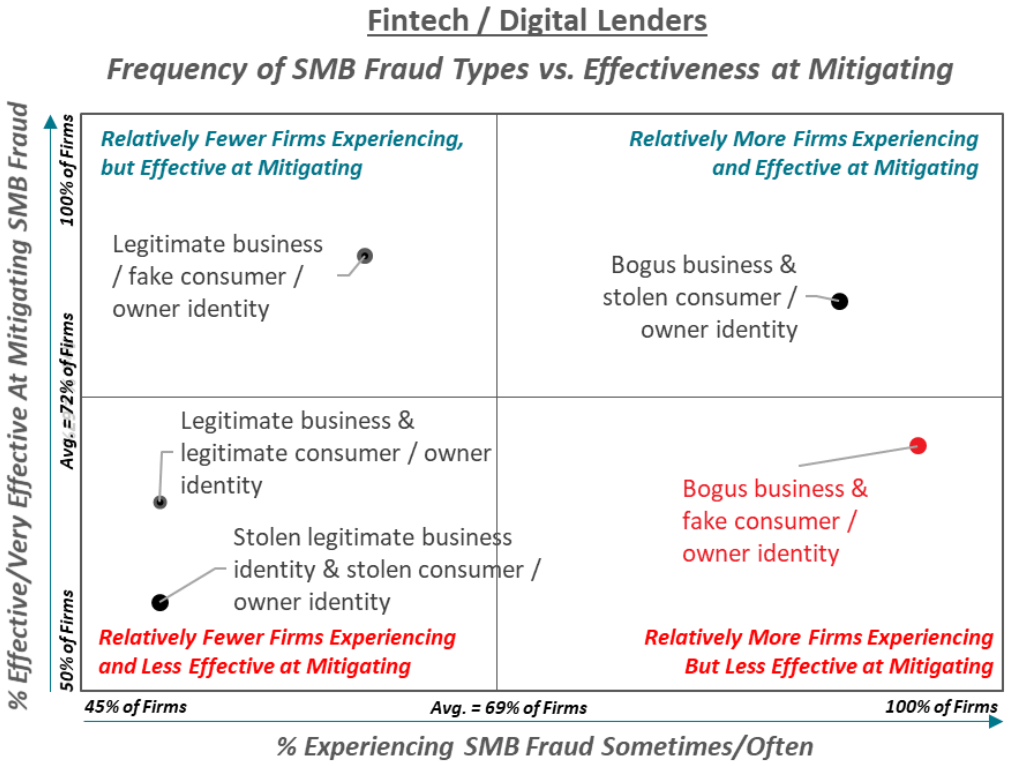
This further underscores the risk of synthetic identities where financial institutions can validate a legitimate business while being fooled by a very real looking and acting consumer identity.



Survey Q17: How often does your company experience the following types of SMB lending fraud? Q18: How effective is your company at mitigating the following permutations of SMB lending fraud?

Fintech's also indicate that they are less effective at mitigating risks when involving fake consumer or owner identities.

The remote online and mobile channels, through which Fintech's largely operate, makes identity verification very challenging, especially when involving synthetic identities.



Survey Q17: How often does your company experience the following types of SMB lending fraud? Q18: How effective is your company at mitigating the following permutations of SMB lending fraud?

Key Finding #2: COVID-19 has significantly contributed to increased SMB lending fraud and costs.

Lenders specifically indicate that COVID-19 negatively impacted them regarding increased fraud and made consumer fraud more complex than it has typically been.

Stolen legitimate business and consumer identities, and use of synthetic consumer identities that look and feel real, makes it incredibly difficult for lenders to distinguish legitimate from fraudulent loan requests if only using physical identity attributes to support this effort.

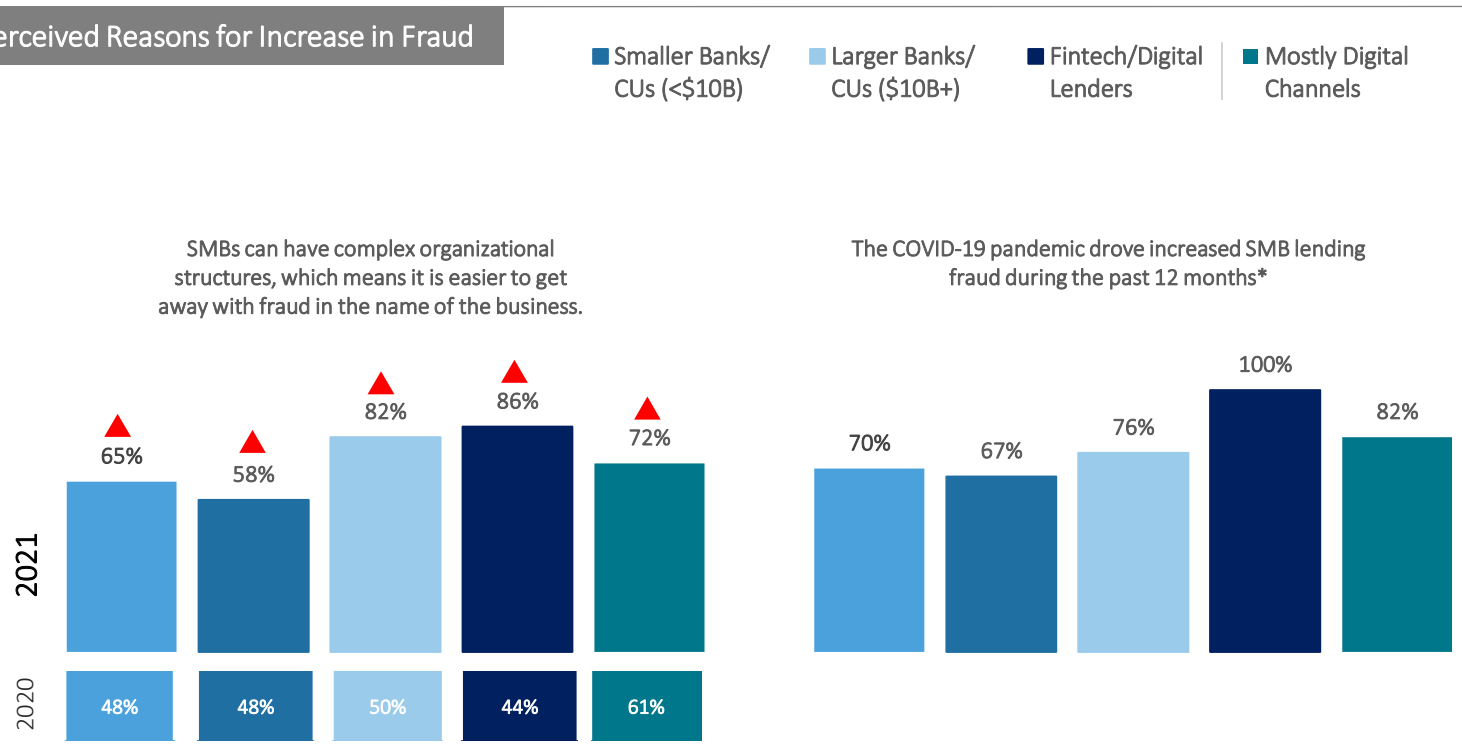
COVID-19 has forced many lenders to make changes to their fraud detection and mitigation approaches, particularly among Fintech's and larger banks. This is the link to higher labor costs. That said, Fintech's and larger banks have followed the best practice of integrating the digital / customer experience with their fraud prevention solutions. However, there is still limited use of digital identity solutions that will effectively detect and assess risks from both the remote channels and the transaction risk itself.

A significant majority of SMB lenders attribute increased fraud to the COVID-19 pandemic, along with significantly more firms than a year ago blaming complex organizational structures that become a barrier to fraud detection.

Compared to pre-COVID-19, significantly more larger banks/credit unions and Fintech's have indicated that it is easier for SMBs to get away with fraud due to their complex organization structure.

Perceived Reasons for Increase in Fraud

Survey Q7: Why do you think SMB lending fraud is increasing?



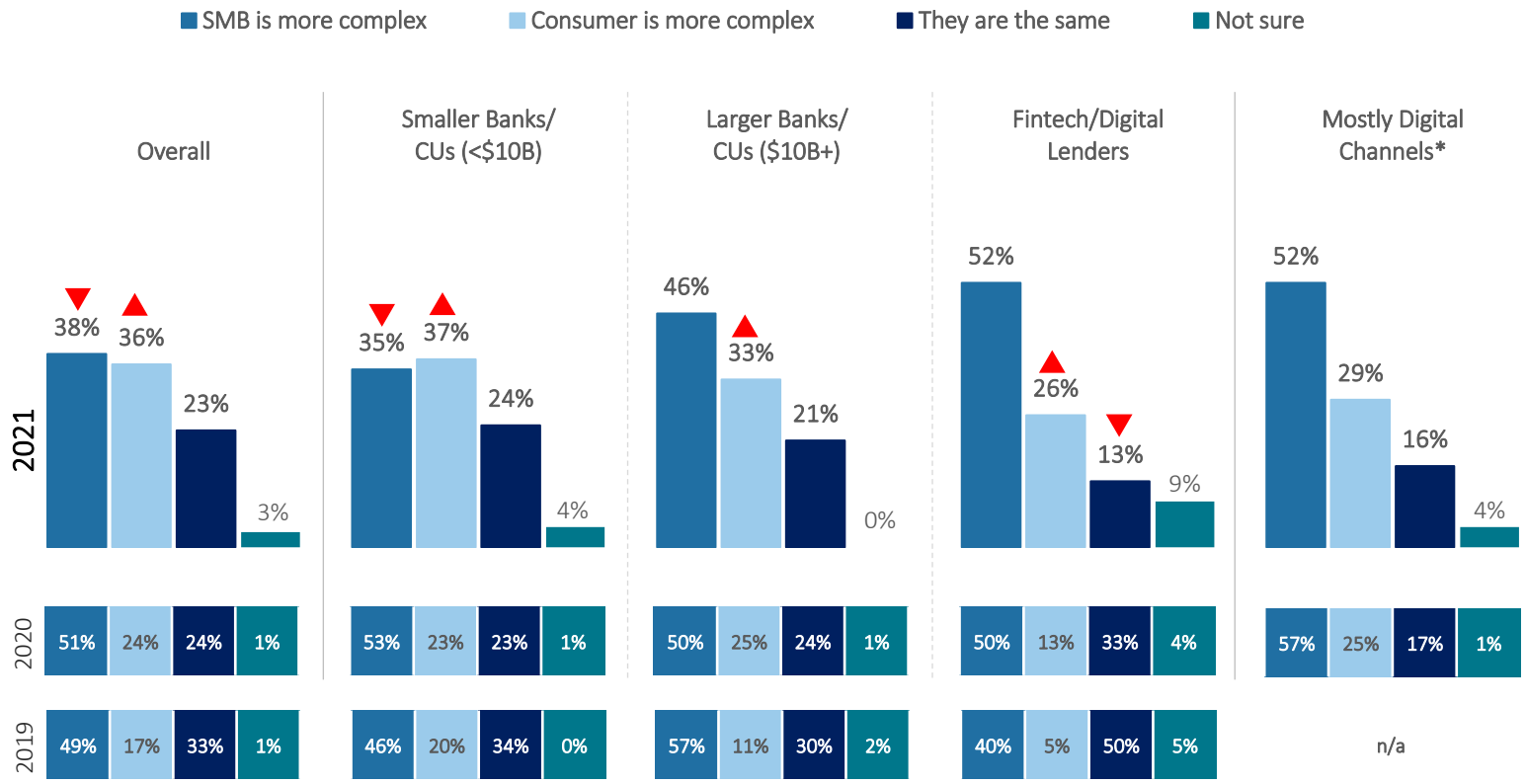
*First asked in 2021

▼▲ = significantly or directionally different from 2020, within segment

During the past year of the COVID-19 pandemic, consumer lending fraud has become seen as being more complex than in previous years.

PPP/CARES Act loans likely played a part in this as more fraud involving stolen or fake consumer identities has occurred with SMB lending. Fintechs have been particularly more likely to experience suspicious loans[2] though the speed with which these were introduced, and less restrictive requirements made this challenging across financial institutions.

Perceptions of SMB Lending Fraud Complexity



Survey Q16: How does a fraud involving an SMB targeting your company compare to a fraud that involves only a consumer targeting your company?

[2] https://www.bankingdive.com/news/ppp-fintechs-suspicious-loans-texas-study/605124/

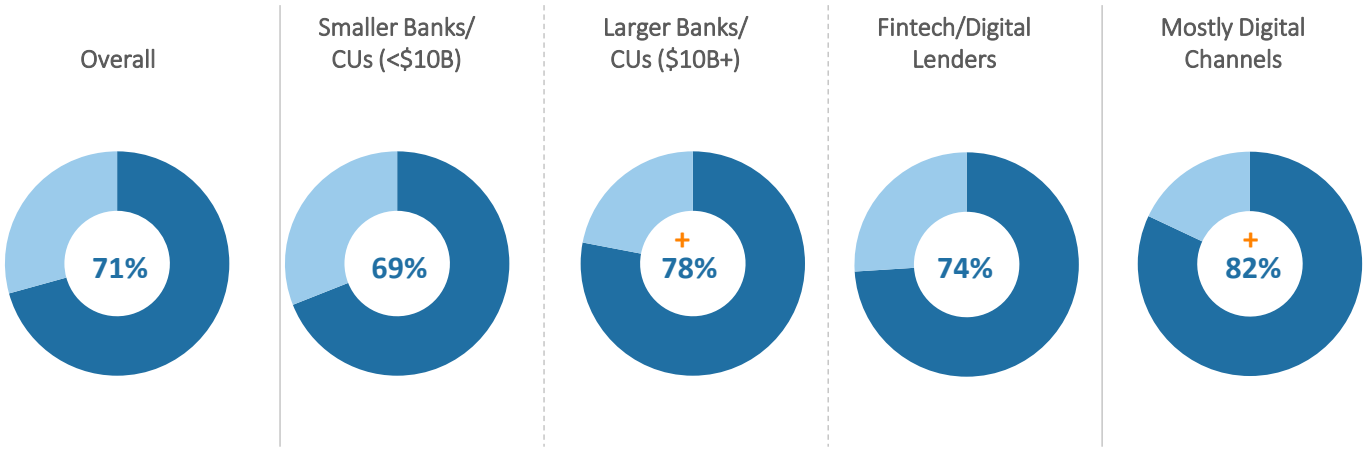
*Includes fintech/digital lenders, as well as banks/credit unions that are processing 80%+ of applications through online/mobile channels

▼▲ = significantly or directionally different from 2020, within segment

The significant majority of financial institutions needed to change their approach to detecting and mitigating SMB lending fraud because of the pandemic, particularly larger banks and Fintech's.

Larger banks/credit unions with sizeable digital channel lending transactions were particularly likely to make changes.

% Firms Indicating that Pandemic Required a Change in Approach to Fraud Detection



Survey Question: Q20d: Did the pandemic require you to change your approach to detecting SMB lending fraud through online / mobile channels? Q20e: In what ways?

LexisNexis® RISK SOLUTIONS

+ = significantly or directionally different from other segments, 2021

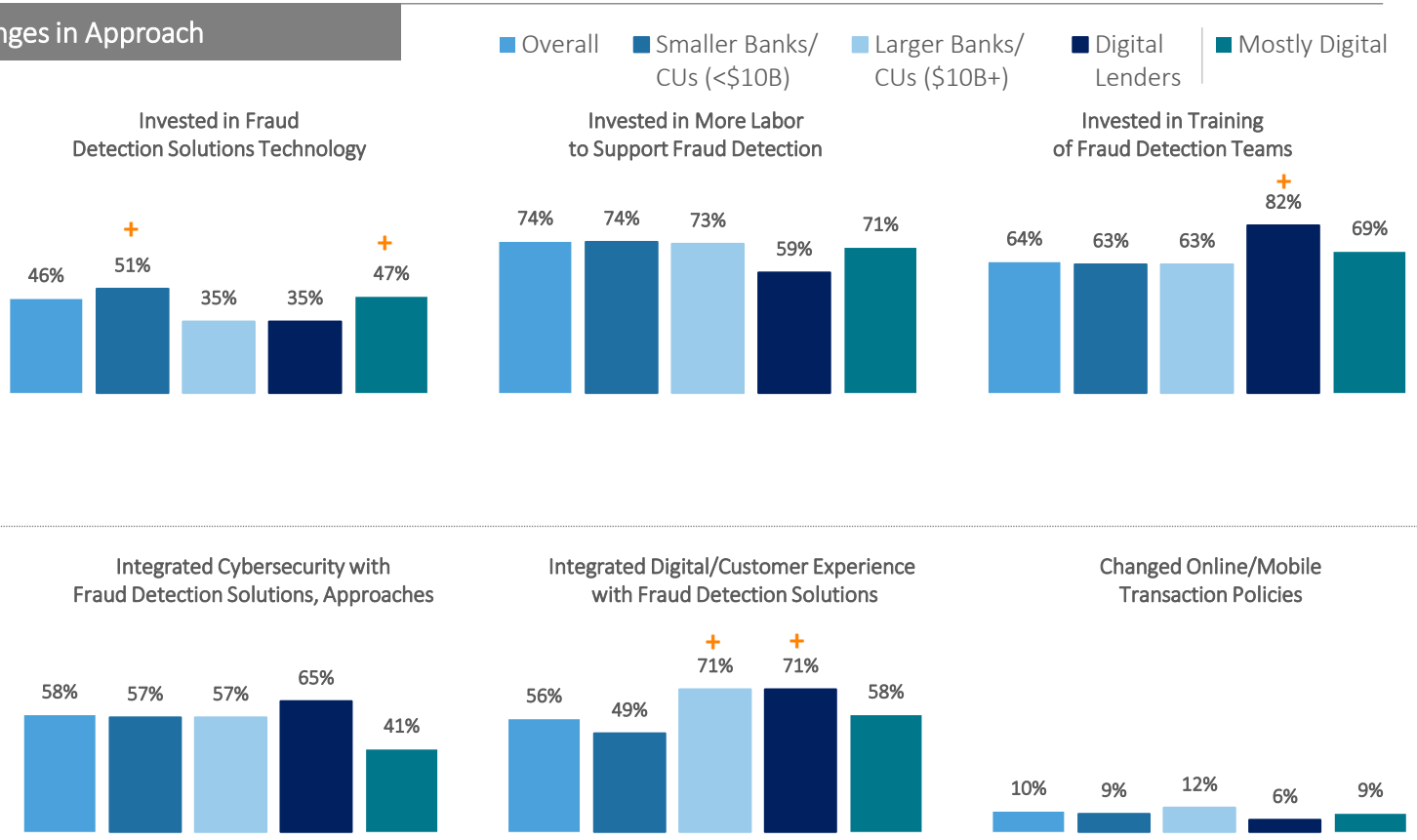
▼▲ = significantly or directionally different from 2020, within segment

The distribution of fraud prevention investments towards labor is clearly shown to be driven by the COVID-19 pandemic, much more than compared to investment in fraud detection solutions.

Fintech's and larger banks have also been more likely to follow the best practice of integrating the digital/customer experience with fraud detection solutions. That said, a number of these firms have not leveraged the power of solutions that effectively assess digital behaviors and attributes to detect fraud through the online and mobile channels, instead relying on assessing the physical identity attributes that can be stolen or synthetically created.

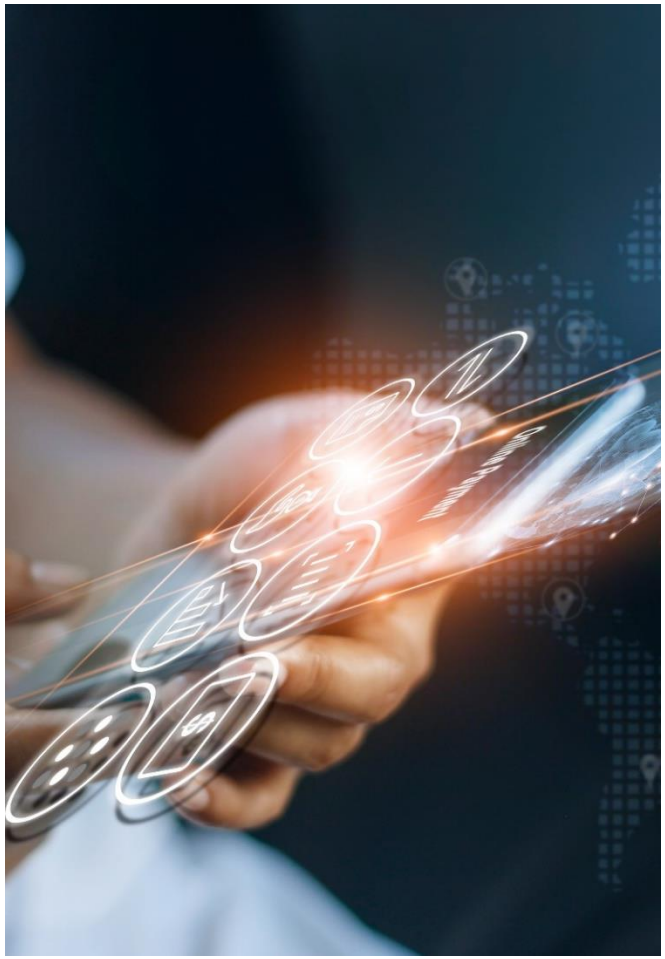
Changes in Approach

Survey Q20e: In which ways did you change your approach to detecting and mitigating SMB lending fraud based on the pandemic driving more transactions through the online and mobile channels?



+ = significantly or directionally different from other segments, 2021

Key Finding #3: Use of the mobile channel is also driving increased SMB lending fraud, some of which is also influenced by COVID-19.



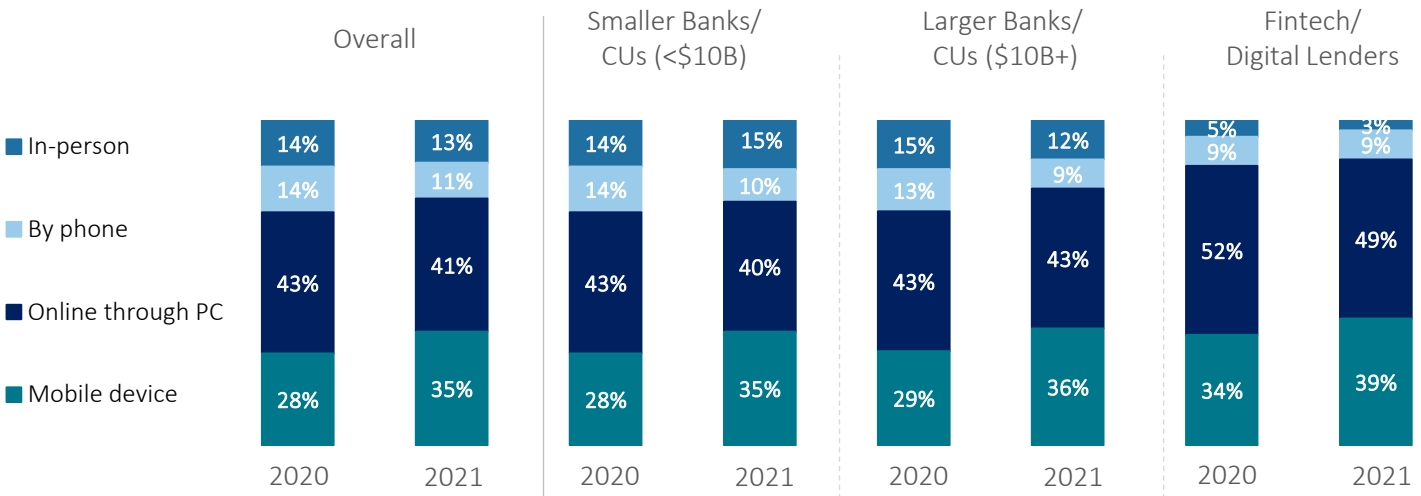
The online (Internet browser) and mobile channels continue to represent the largest share of lending origination transactions.

There has been a directional increase from 2020 with the volume of transactions through the mobile channel.

At the same time, fraud losses due to the mobile channel have increased, particularly among Fintech's and larger banks.

Remote channels continue to be the primary source of SMB loan origination, with a directional increase in the use of the mobile channel for these transactions.

% of SMB Loan Applications Submitted/Loans Originated By Channel



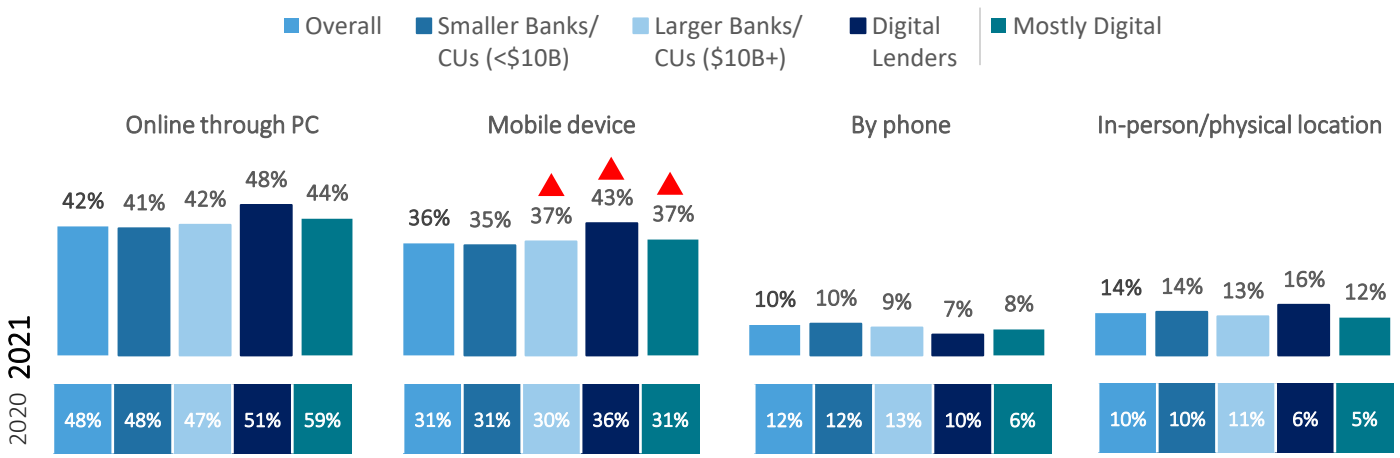
Survey Question: Q3. please indicate the percentage of small and midsize business (SMB) loans that were originated, or applications that were submitted, through each of the following channels used by your company (over the past 12 months).*

The significant majority of SMB lending fraud losses continue to occur through remote channels, with the mobile channel accounting for slightly more compared to 2020.

Banks and lenders are reporting more threats from malicious botnet attacks compared to before COVID-19 (from an average 3% of bank transactions in 2019 to 24% in 2021; 2% for lenders in 2019 to 24% in 2021).[3]

Further, half of credit lenders and nearly two-thirds of banks indicate a 10% or more increase in the degree of fraud targeting the mobile channel during the past year. At the same time, identity verification is a key mobile channel challenge for U.S. banks and lenders.[4]

Distribution of Fraud Losses



Survey Q8b: Indicate the distribution of total SMB lending fraud costs generated through each of the following channels currently used by your company (as a % of total annual fraud losses).

[3] 2021 LexisNexis® Risk Solutions True Cost of Fraud™ Study, Financial Services & Lending, US & Canada Edition
[4] Ibid

▼▲ = significantly or directionally different from 2020, within segment

Key Finding #4: SMB lenders expect to increase their investment in fraud mitigation prevention, with a focus on additional labor resources which will drive up costs.

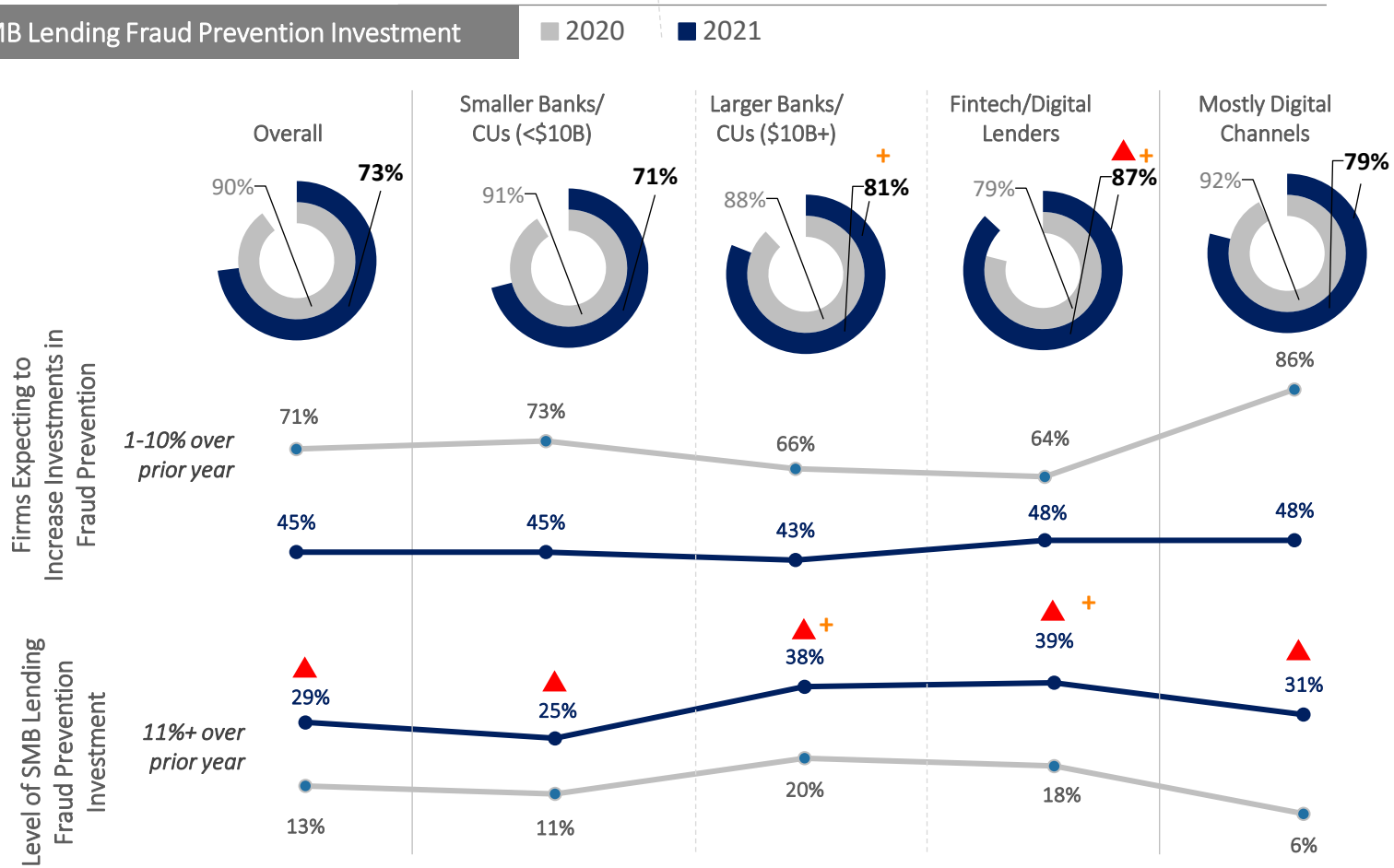
While Fintech's are more likely to use fraud mitigation solutions than others, there is still limited use of a multi-layered solutions approach across lending segments that can address fraud risks from different channels and digital behaviors.

There is also limited use of solutions that assess digital identity attributes in a behind-the-scenes manner that minimizes customer friction while increasing the effectiveness of detecting fraud in the online and mobile channels.

As SMB fraud continues to rise, lenders expect to increase their investment in fraud prevention resources, particularly Fintech's and larger banks.

A significant number of financial services firms expect a significant level of increased investment in fraud prevention, again with Fintech's and larger banks expecting to do so at a higher level than others.

Survey Q14: In 2021, at what level will your company invest to prevent SMB lending fraud from targeting it?



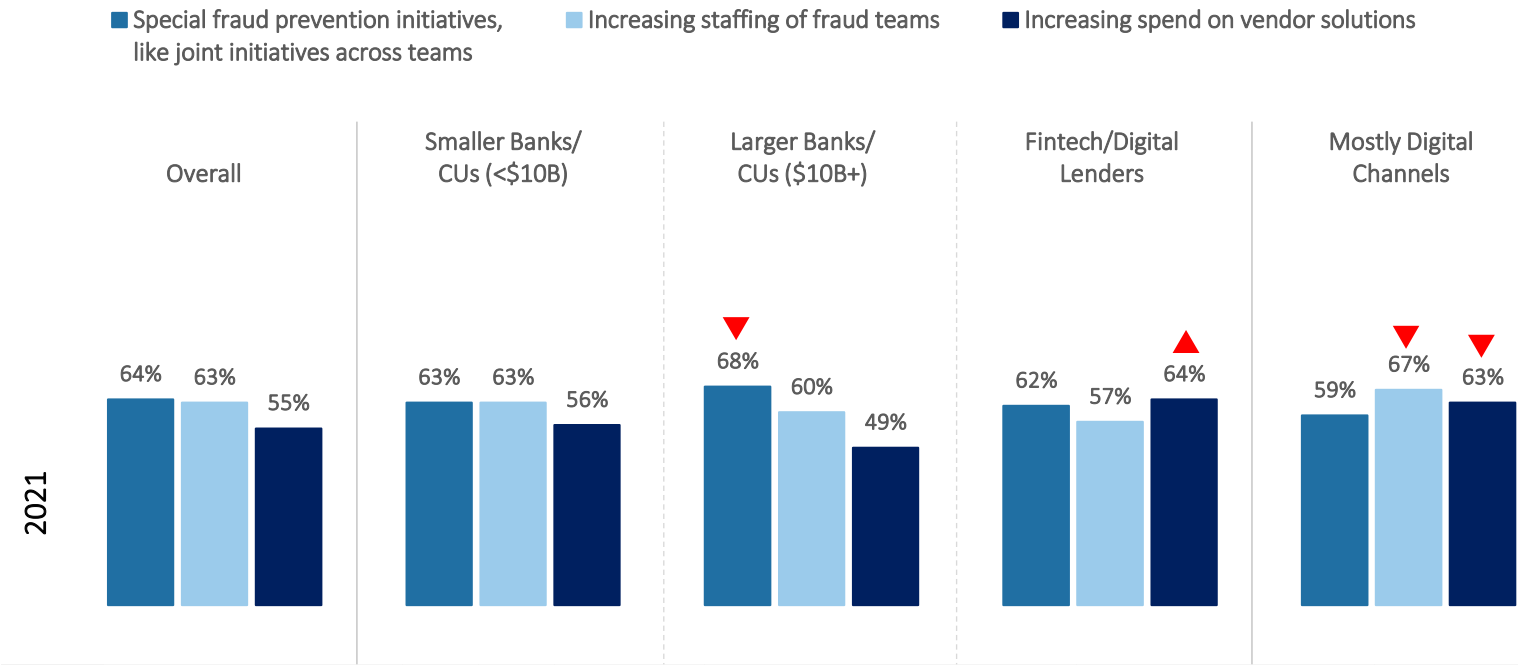
+ = significantly or directionally different from other segments, 2021

▼▲ = significantly or directionally different from 2020, within segment

For many, these expected investments include a focus on increased staffing of fraud teams which can drive up the actual cost of fraud prevention efforts.

While more Fintech's plan to invest in fraud mitigation/prevention solutions compared to last year, fewer non-Fintech's plan to adjust their strategies from 2020 even though they are battling higher volumes and more complex types of SMB lending fraud. Given that Fintech organizations are, by nature, more involved with technology, they can serve as a lighthouse to others regarding the benefits of fraud prevention solutions.

Activities Being Undertaken to Curb SMB Lending Fraud



	Overall			Smaller Banks/ CUs (<$10B)			Larger Banks/ CUs ($10B+)			Fintech/Digital Lenders			Mostly Digital Channels		
2020	70%	65%	54%	68%	66%	54%	77%	60%	54%	58%	58%	51%	52%	83%	74%
2019	79%	53%	38%	76%	58%	36%	87%	40%	45%	82%	45%	36%		n/a	

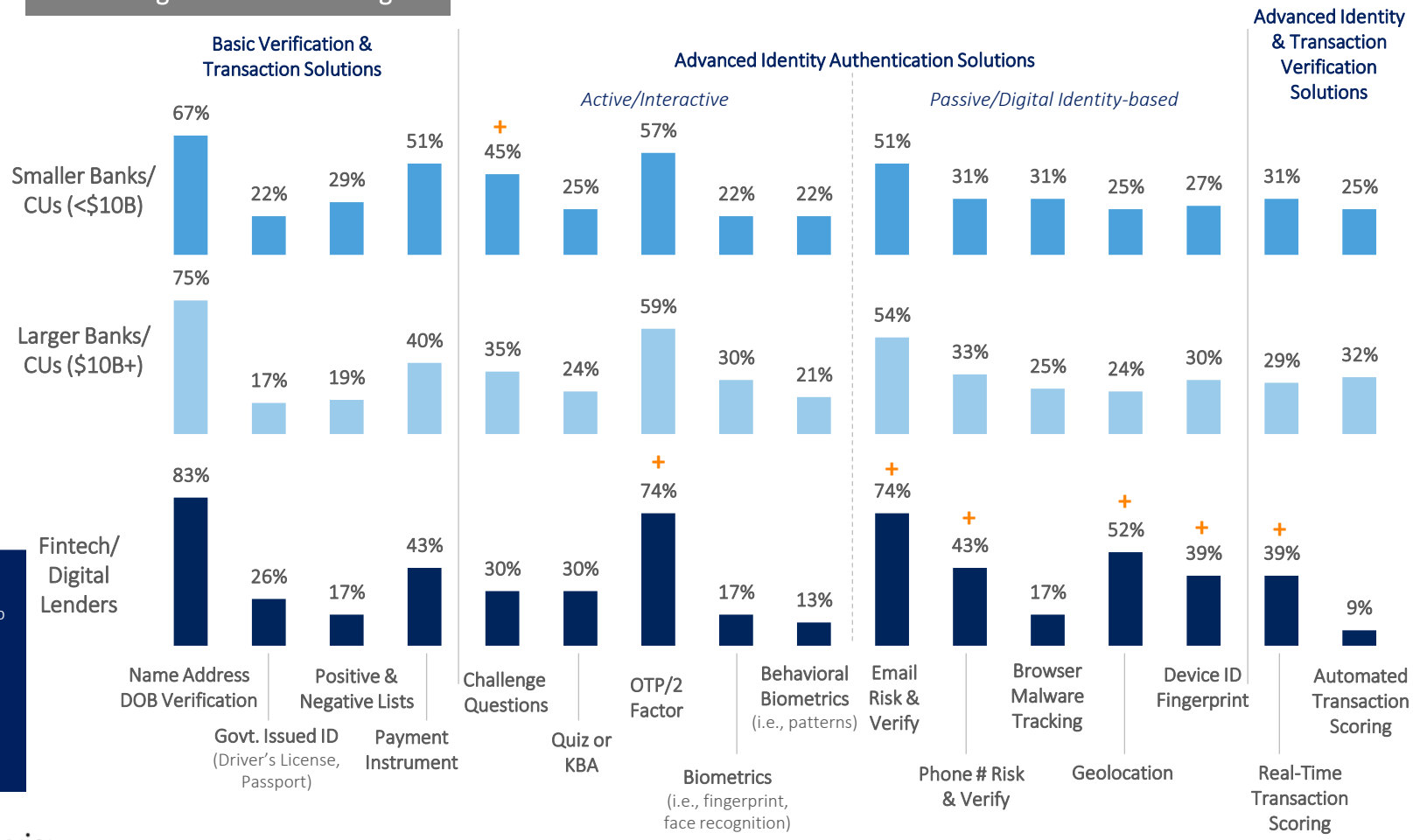
Survey Q15: What internal activities is your company taking to curb SMB lending fraud from targeting your company?

▼▲ = significantly or directionally different from 2020, within segment

Fintech's are more likely than others to use solutions that assess risk of digital identities and the transaction, though use is limited even among this segment.

Fraud mitigation solutions assess both individual and device risks (Email Risk Verification, Geolocation, Device ID, Biometrics and Behavioral Biometrics) and transaction risk (Near Real-Time Fraud Detection, Automated Transaction Scoring), which provide fast, seamless, and "behind the scenes" fraud detection that reduces customer delays while more effectively distinguishing synthetic identities and malicious bots.

Fraud Mitigation Solutions Usage



Survey Q20: Which of the following solutions does your company currently use to help combat/prevent SMB lending fraud?*

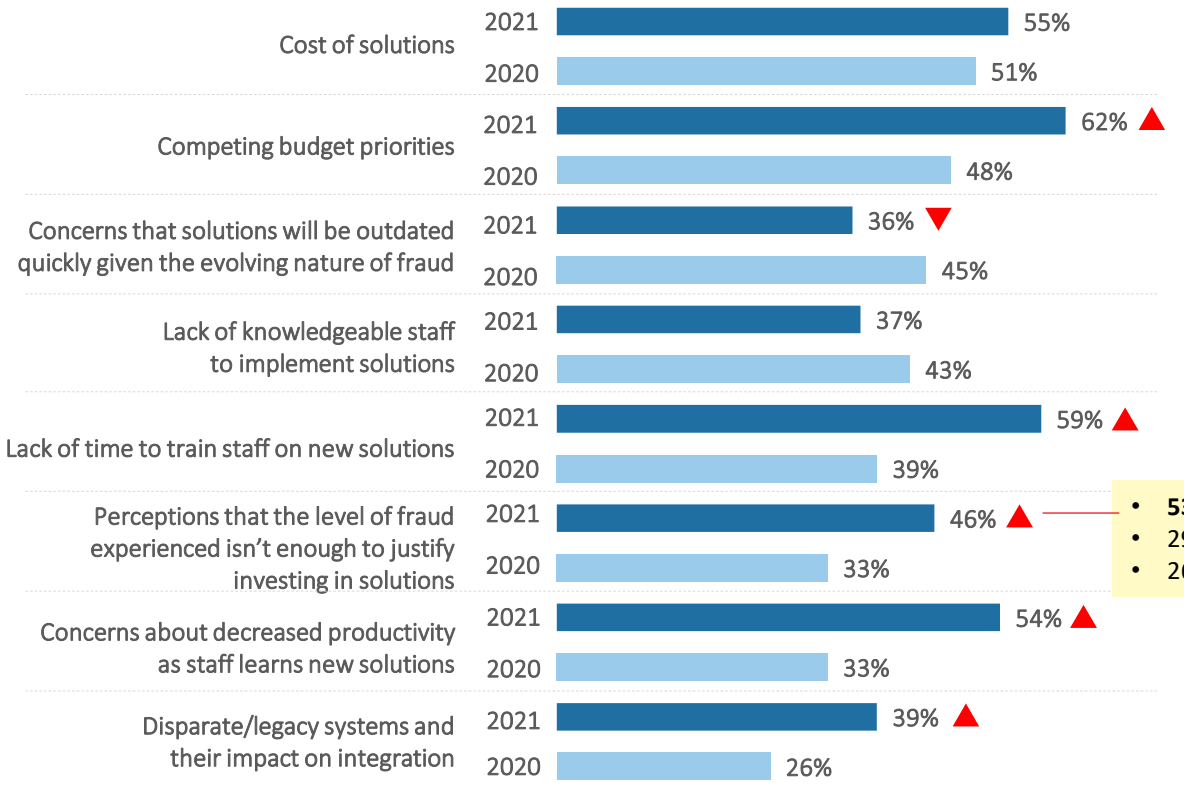
+ = significantly or directionally different from other segments, 2021

The rapid changes brought by the COVID-19 pandemic changed budget priorities towards labor and forced lenders to pivot quickly to address increased fraud volumes. This appears to lead to increased perceptions that technology investments would slow this process as it relates to training and systems integration.

Smaller banks/credit unions were more likely than others to say that the level of fraud isn't enough to justify investing in solutions.

Survey Q22: Which of the following, if any, have been barriers to investing in fraud prevention solutions for SMB lending fraud?

Barriers to Investing in Fraud Mitigation Solutions



- **53%** Small Banks/Credit Unions;
- 29% Larger Banks/CUs;
- 26% Fintech's

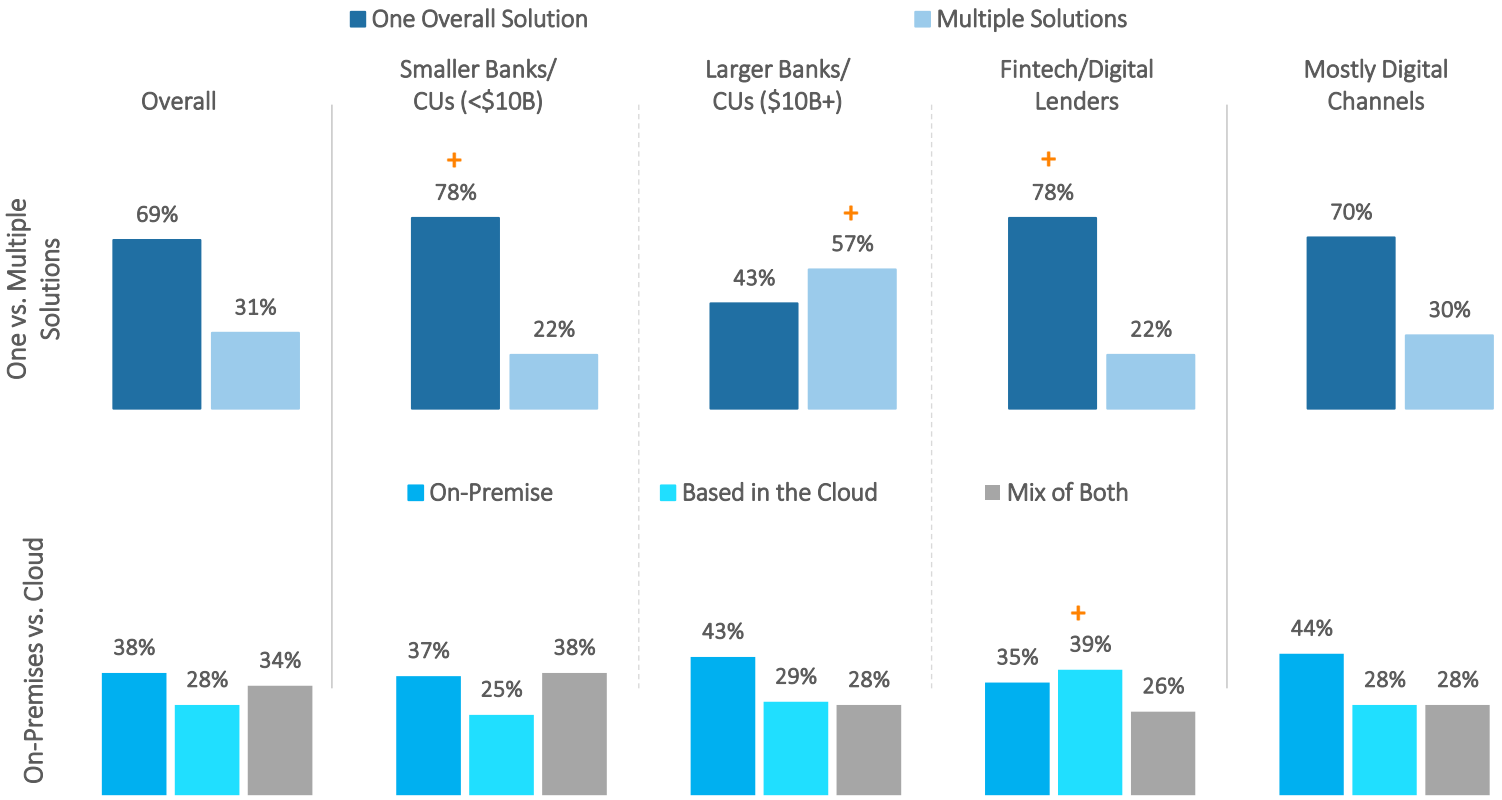
▼▲ = significantly or directionally different from 2020, within segment

A portion of larger banks are more likely to use multiple solutions for identity verification while smaller banks and Fintech's are more likely to be using one.

While just under half of larger banks did indicate using just one overall solution, there are many that are likely needing to integrate different solutions with legacy systems, or multiple systems inherited through mergers and acquisitions.

Across financial institutions, there is often a mix of on-premises and cloud-based locations for these solutions.

Scope and Location of Identity Verification Solutions



Survey Q20b: Are you using one overall solution or multiple solutions? Q20c: Is/are your solutions based on-premises or from the Cloud?

+ = significantly or directionally different from other segments, 2021

Key Finding #5: Study findings show that lenders which use a multi-layered solutions approach to assess fraud risk by various transaction channels, by physical and digital identity attributes and by transaction have experienced a lower year-over-year increase in SMB lending fraud.

This also includes less impact from COVID-19 on lending fraud.

Further, these lenders rate their solutions as being very effective, thereby justifying the solutions investment.

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.

Compared to traditional in-person transaction environments, remote channel applications require a more dynamic approach to fraud detection and prevention.

FRAUD ISSUES

Digital services

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

Account-related fraud

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

Synthetic identities

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

Botnet attacks

mass human or automated attacks often to passwords and 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 match up or if there appears to be an irregularity.

Solution examples: near 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 user provides two different authentication factors to verify themselves.

Solution examples: authentication by challenge or quiz; authentication using OTP/ 2 factor

AUTHENTICATING THE DIGITAL PERSON

Digital identity/behavioral biometrics: analyzes human-device interactions and behavioral patterns such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognizing normal user and fraudster behavior.

Solution examples: authentication by biometrics; email/phone risk assessment; browser/malware tracking; device ID / fingerprinting

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

Solution examples: device ID/ fingerprint; geolocation

Best practice approaches involve a layering of different solutions to address unique risks from different channels, payment methods and products. And they go farther by integrating capabilities and operations with their fraud prevention efforts.

Integration

Tools and Capabilities with Fraud Prevention Approach

- Cybersecurity Alerts
- Social Media Intelligence
- AI/ML Models
- Crowdsourcing
- Cybersecurity Operations
- Digital / Customer Experience Operations

Fraud Detection and Prevention Solution Layering

A multi-layered solution approach is essential to fighting fraud while mitigating customer friction.

Strategy and Focus

Minimizing Friction While Maximizing Fraud Protection

- Tracking successful and prevented fraud by both transaction channel and payment method
- Use of digital / passive authentication solutions to lessen customer effort (let solutions do the work behind the scenes)
- Assessing both the individual and transactional risk

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

Effectiveness of Fraud Mitigation Solutions

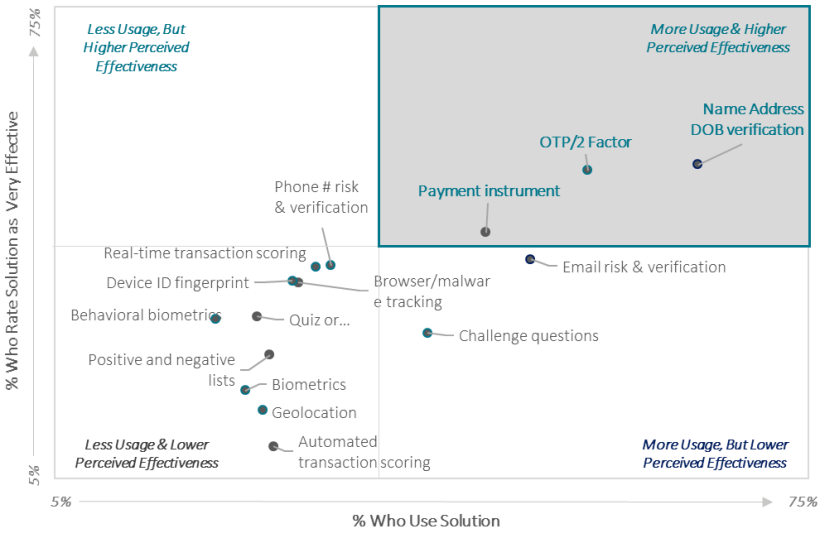
Those using a multi-layered solutions approach, involving solutions that assess both physical and digital identity plus transaction risk are significantly more likely to get very effective results compared to those that do not layer.

This includes use of behavioral biometrics provides fraud detection/prevention teams with insights about the behavioral patterns, such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognizing normal user and fraudster behavior.

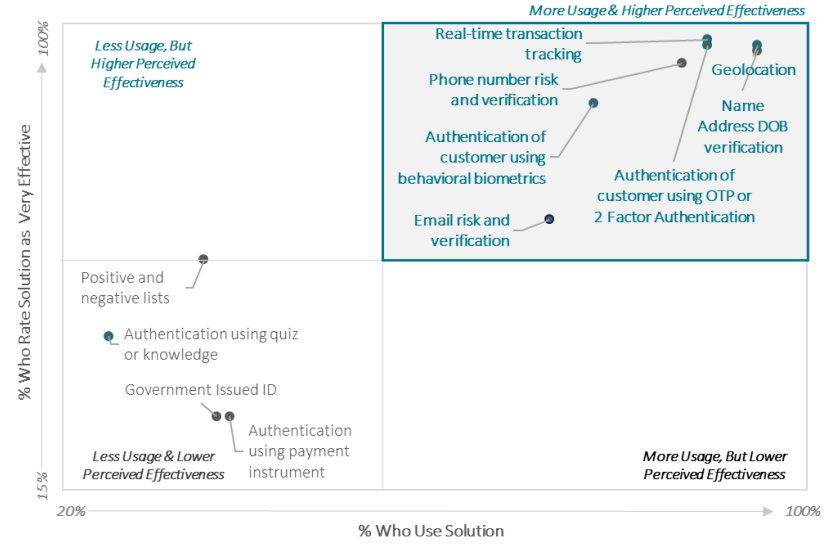
Digital identity assessment solutions also reduce customer friction by conducting risk analysis quickly and transparently, minimizing customer effort.

Survey Q20: Which of the following solutions does your company currently use to help combat/prevent SMB lending fraud?* Q21: How effective are the solutions that your company currently uses at combatting/preventing SMB lending fraud?

All Respondents



Those Using a Multi-Layered Solutions Approach*



*For this illustration, multi-layering includes the following: Authentication using Name/Address/DOB, Authentication using OTP/2 Factor, Email Risk Verification, Phone Risk Verification, Geolocation, Behavioral Biometrics and Real-time Transaction Tracking

Study findings show, as an impact of COVID-19, that SMB lenders who layered more advanced identity authentication plus advanced transaction/identity verification solutions experienced a lower rate of fraud overall.

Layering of Fraud Mitigation Solutions

	Percentage Increase of SMB Lending Fraud	7.9%	5.1%
	Percentage Increase of SMB Lending Fraud Due to COVID-19	**44%**	**29%**
	Layers of Protection	Limited	Multi-layered with Digital Identity
Common Core Solutions	Authenticate Using Payment Instrument, Name/Address/DOB Verification, Positive & Negative Lists, Government-issued ID	Many	✓
Advanced ID Authentication Solutions	Challenge Questions/Quiz, OTP/2-Factor, Biometrics, Behavioral Biometrics, e-Mail Risk & Verification, Phone # Risk & Verification, Browser/Malware Tracking, Geolocation, Device ID	Some	✓
Advanced ID and Transaction Verification Solutions	Automated Transaction Scoring, Real-Time Transaction Scoring	Minimal	✓
	Average # Advanced Solutions Used	4	7

Recommendations

Recommendation #1

Lenders, large and small, that conduct significant remote channel transactions should prioritize a multi-layered risk solution approach.

The digital channel environment is upon us and continues to grow. Customers and prospects expect this option, particularly during times that make in-person transactions more challenging. At the same time, fraudsters are professionals who continue to evolve; that means fraud will continue to increase. Left unaddressed, lenders that conduct transactions remotely will not only continue to see increased fraud costs, but also increased risk for customer friction and churn.

A multi-layered solution approach is critical for both identity and transaction-related fraud detection.

Identity verification and authentication is important for "letting your customers in" with the least amount of friction.

Transaction verification is important for keeping fraudsters out.

Recommendation #2

When seeking a layered solution approach, it is essential that lending firms with digital channel business models implement solutions for unique channel issues and fraud. There is no one-size-fits-all solution.

There are differences between the online and mobile channels in terms of device identification and transaction options (i.e., mobile apps).

Using the same solution to address both may not be as effective, particularly given the transient nature of mobile transactions.

And, where one tries to force a one-size-fits-all approach, particularly by using traditional onsite with remote channel transactions, there is likelihood of increasing false positives which leads to customer friction and lost current/future business.

Recommendation #3

Lenders should seek external providers with deep data and analytics resources to most effectively address identity-based fraud challenges.

Identity fraud can be complicated, with various layers of masks and connections in the background. Investing in a layered solution approach will be much more effective if from a solutions partner that provides unique linking capabilities that identify and match hidden relationships, shed light on suspicious activities or transactions and identify collusion. These patterns are not easily uncovered by several risk solutions on the market today.

Recommendation #4

Lenders need to remain vigilant by holistically tracking fraud by channel type – including by which has been successful and prevented.

If fraudsters perceive SMB lending as victimless, then that will empower them to continue testing weak points of entry and detection with lending firms.

Fraud occurs in multiple ways, particularly for multi-channel lenders (given overlap between use of online and mobile channels). The remote channel, of course, is important to monitor in comparison to physical POS locations since the anonymity of online and mobile make these channels higher risk. Additionally, there are different security issues and approaches between online and mobile channels.

The rise of synthetic identities makes it easier for fraud where solutions are not being employed to detect anomalies with digital identities and transactional behaviors.

About LexisNexis Risk Solutions
LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com. Our solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

This document is for informational purposes only and does not guarantee the functionality or features of any LexisNexis Risk Solutions products identified. LexisNexis Risk Solutions does not warrant that this document is complete or error free.