US SMB Lending Fraud, Research Results

April 2020

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 February – March 2020. A total of 135 completions were obtained, broken out as follows:

Total	<$10B Asset Banks/Credit Unions	$10B+ Asset Banks/Credit Unions	Fintech/Digital Lenders	Payment Processors*
135	53	51	20	11

- 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:

Synthetic Identity	Creation of a new identity/business entity using a combination of real and fabricated information, or sometimes entirely fictitious information, to commit fraud
3rd Party Identity Fraud	Identity theft of true owner/authorized business representative to commit fraud
3rd Party Account takeover	The use of a combination of a victim's PII to access an associated financial account in an effort to fraudulently secure a loan
1st Party or Friendly Fraud	Business owner/authorized user or individual associated with business owner (i.e. family member, friend, etc.) commits loan fraud

LexisNexis RISK SOLUTIONS

Key Findings

1. “Traditional” banks and credit unions are anything but traditional, having moved a large portion of their SMB loan application processes into remote channels. This exposes them to even more risk.

2. SMB lending fraud levels have risen over the past 24 months, especially for lenders that operate more digitally.

3. The value of SMB lending fraud has increased since last year, with higher levels for lenders that operate more digitally.

4. SMB lending fraud for 2020 is expected to increase at nearly the same rate as for the previous 24 months, but combatting it is a key corporate priority for most.

5. Lending firms may not be optimizing solutions and approaches to fight newer and more complex types of fraud, particularly those that operate more digitally.

6. Study findings show that SMB lenders that use a layered solutions approach involving identity authentication and verification, including digital identity/behavior and biometric tools, experience a lower proportion of fraud.

LexisNexis RISK SOLUTIONS

Key Finding #1: Channels & Fraud Perceptions

1 "Traditional" banks and credit unions are anything but traditional, having moved a large portion of their SMB loan application processes into remote channels. This exposes them to even more risk.

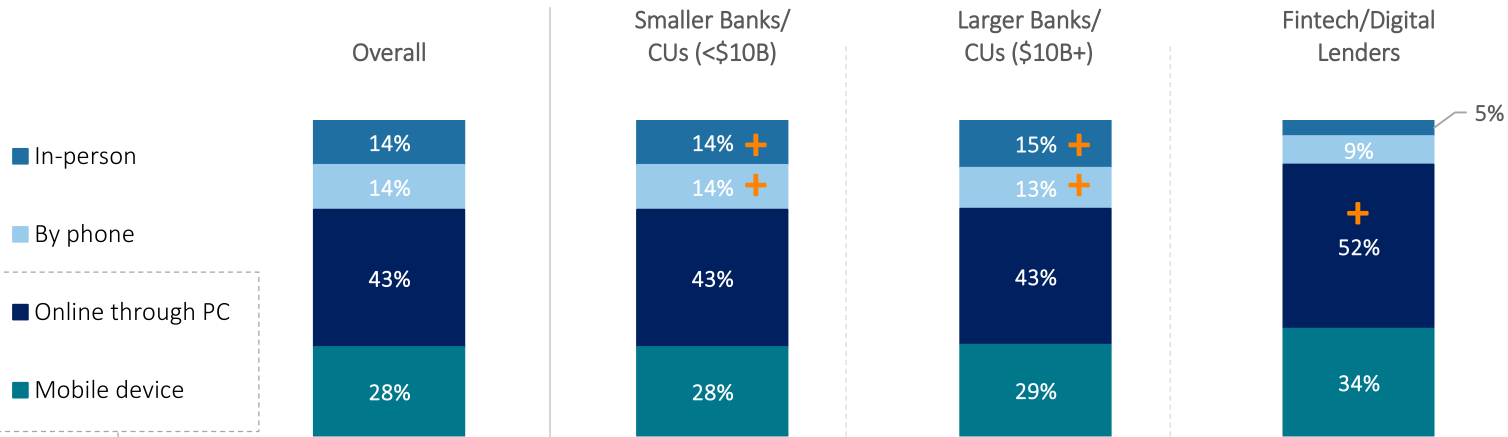
- 4 in 10 banking/credit union respondents report that they accept 80% or more of their SMB loan applications through online and mobile channels.
- This is in spite of the complex nature of SMB fraud and perceptions that the mobile channel presents a significant risk of fraud.

LexisNexis RISK SOLUTIONS

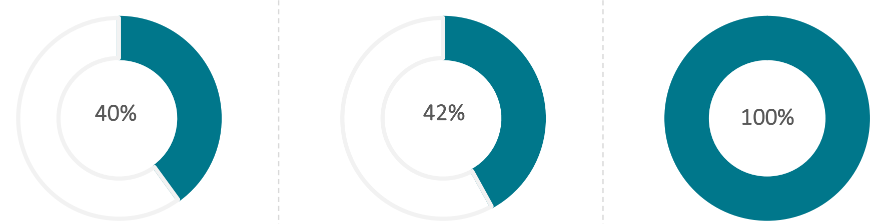
Banks and credit unions are becoming more digital, with 4 in 10 reportedly accepting 80% or more of their SMB loan applications through remote (online and mobile) channels.

- Though online submissions are more common across the board, a third or more of applications are accepted through the mobile channel.

% of SMB Loan Applications Submitted/Loans Originated By Channel



% of Organizations With Majority (80%+) of Applications Submitted/Originated Through Digital Channels



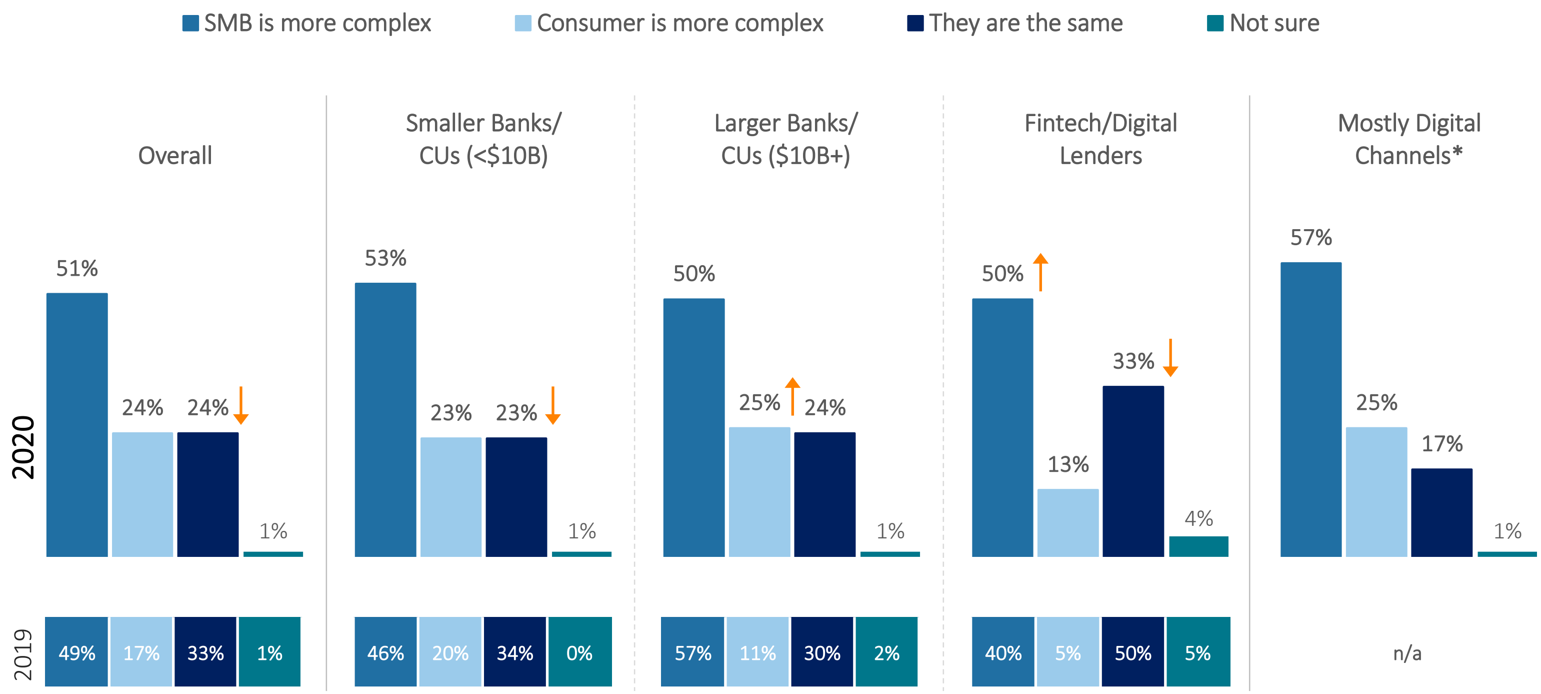
Survey Question: Q3. please indicate the percentage of small and midsize business (SMB) loans that were originated, or applications that were submitted, through each of the following channels used by your company (over the past 12 months).*

*First asked in 2020 + = significantly or directionally different from other segments, 2020

SMB lending fraud is largely still thought to be more complex than consumer lending fraud.

- Fintech/digital lenders, in particular, seem to feel the complexities of SMB lending fraud more this year than last.

Perceptions of SMB Lending Fraud Complexity



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

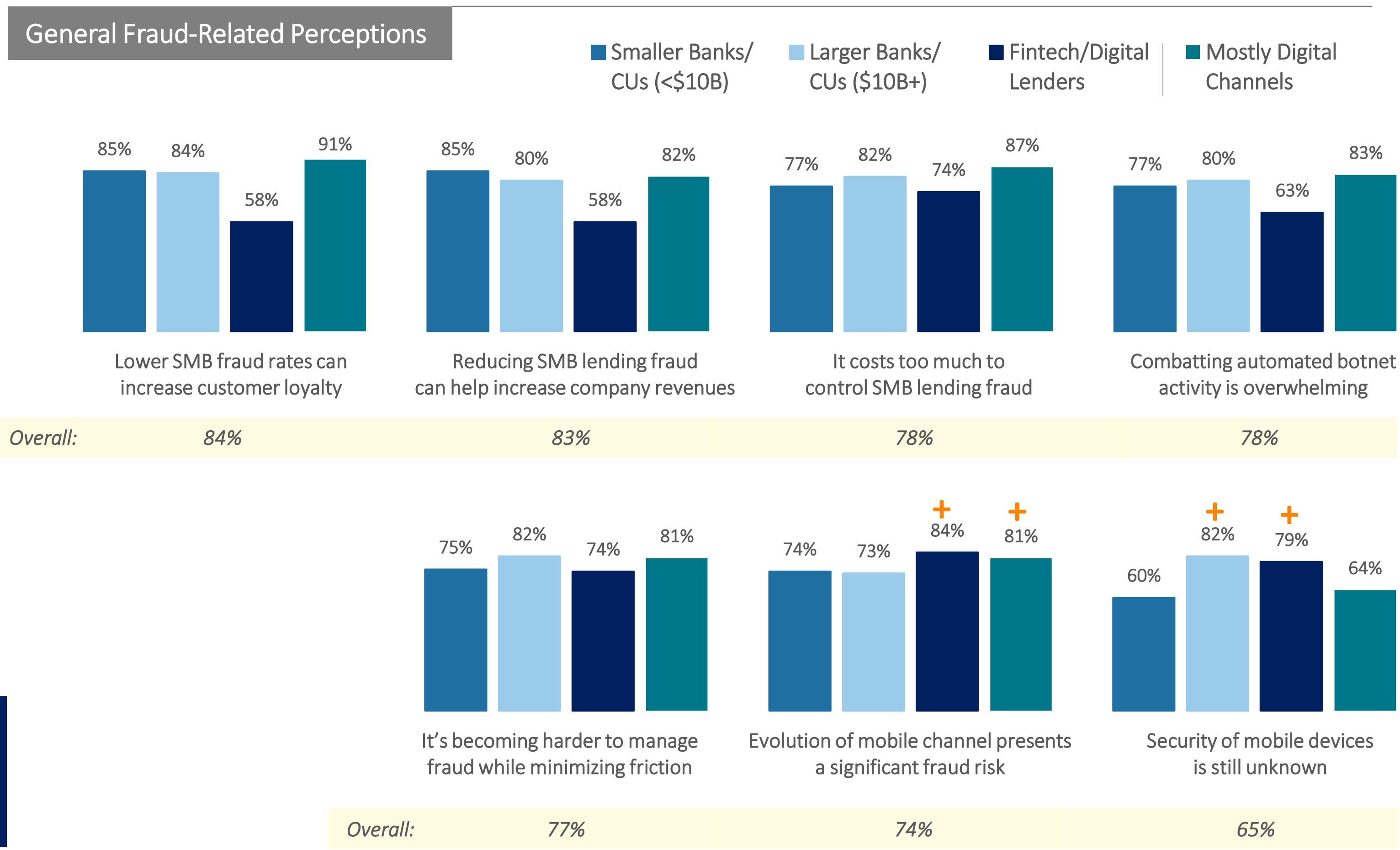
= significantly or directionally different from 2019, within segment

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

LexisNexis RISK SOLUTIONS

Use of mobile could be a contributing factor, with a majority of fintech/digital lenders and institutions that operate heavily through digital channels questioning the security of and risk related to this channel.

- More generally, SMB lending fraud is perceived to have various negative impacts, including difficulty in managing customer friction/retaining loyalty, the costs associated with controlling it, and overwhelming nature of associated botnet activity.



Survey Question: Q26. Please rate the extent to which you agree or disagree with the statements below.*

*First asked in 2020 + = significantly or directionally different from other segments, 2020

Key Finding #2: Fraud Levels, Past 24 Months, & Types of Fraud

2 SMB lending fraud levels have risen over the past 24 months, especially for lenders that operate more digitally.

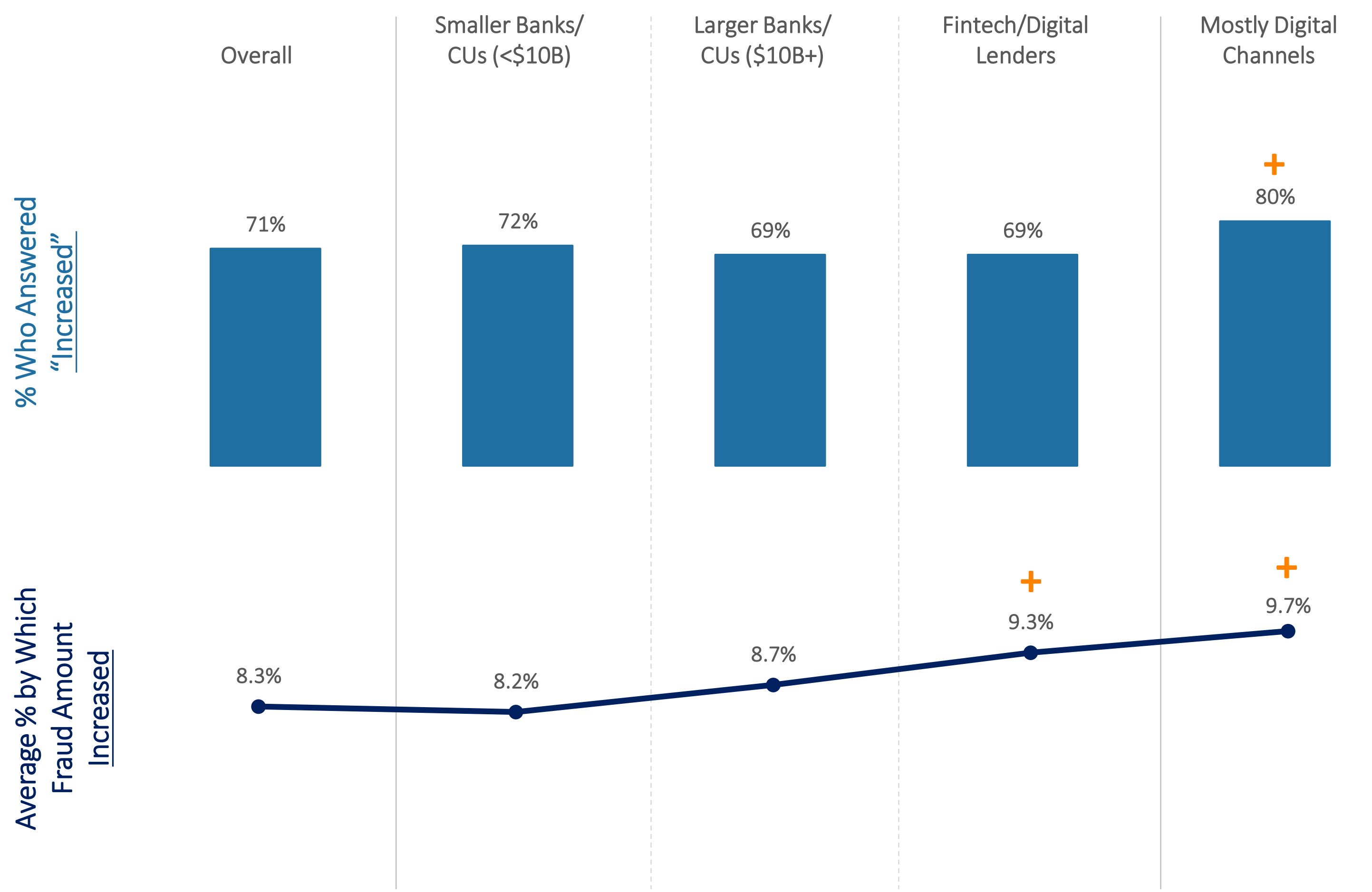
- Synthetic identity and 3rd party account frauds are issues for larger banks/credit unions and fintech/digital lenders.
- Larger institutions are more likely to report struggling with effectively mitigating these types of fraud.
- While fintech/digital lenders are attacked at a somewhat higher rate per month than others, smaller institutions and those operating heavily through digital channels have the most room for improvement in detecting fraud-related botnet attacks.

LexisNexis® RISK SOLUTIONS

A majority of lenders reported an increase in SMB lending fraud over the past 24 months, particularly those that operate heavily through digital channels.

- This group experienced the largest percent increase in fraud, at an average of 9.7%.

Change in Level of SMB Lending Fraud Over Past 24 Months



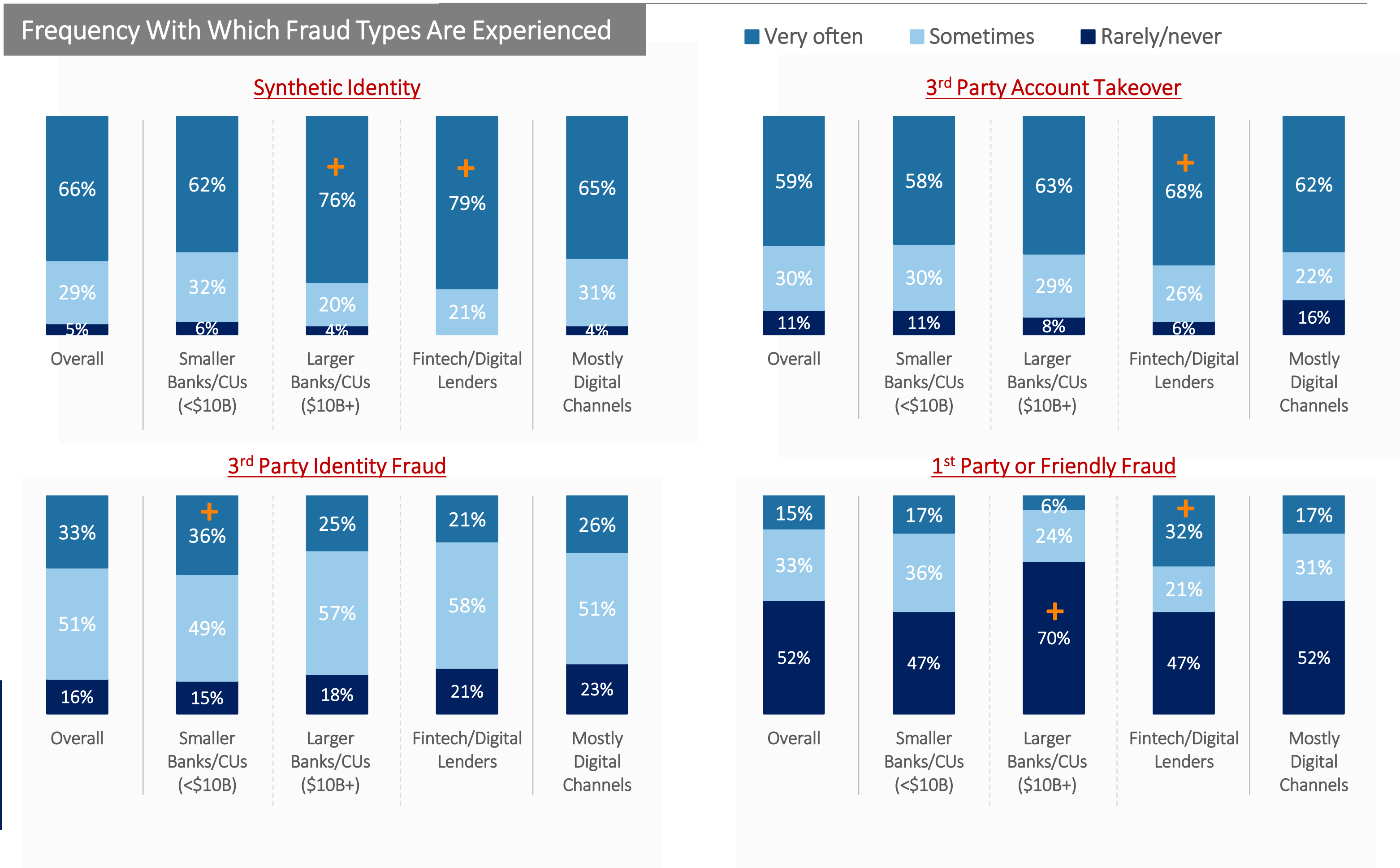
Survey Question: Q5. Over the past 24 months, has SMB lending fraud targeted at your company increased or decreased and by how much?

+ = significantly or directionally different from other segments, 2020

Synthetic identities and 3rd party account takeovers are contributing to a rise in fraud, with many lenders experiencing them regularly.

- Larger institutions and fintech/digital lenders are encountering synthetic identity fraud more than others; fintech/digital lenders are also more likely to combat 1st party/friendly fraud – this could be related to the nature of the digital lending business model, making some feel more comfortable to commit fraud “from a distance”.
- Smaller institutions are somewhat more likely to experience 3rd party identity fraud.

Frequency With Which Fraud Types Are Experienced



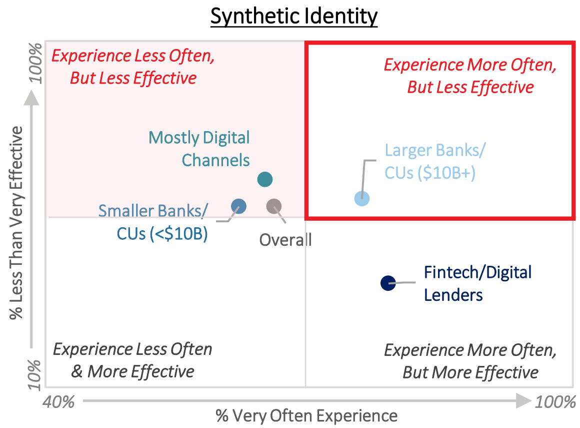
Survey Question: Q17. How often does your company experience the following types of SMB lending fraud?*

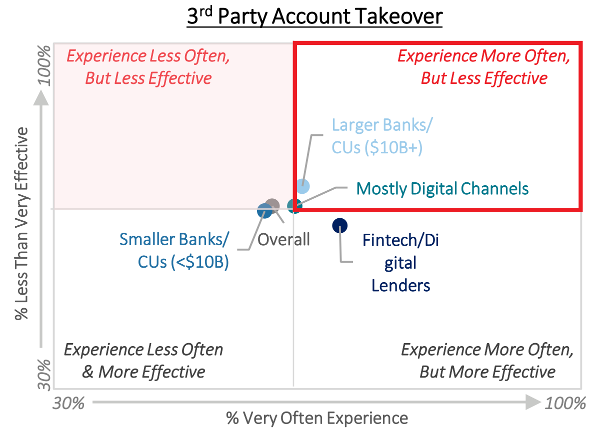
*First asked in 2020 + = significantly or directionally different from other segments, 2020

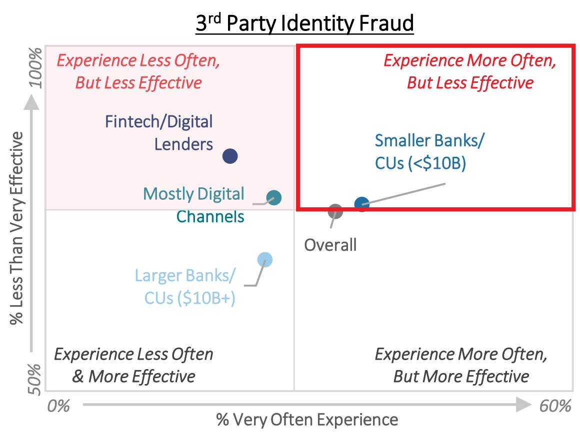
While both larger institutions and fintech/digital lenders experience synthetic identity fraud more often than others, larger banks/credit unions feel less equipped to mitigate it.

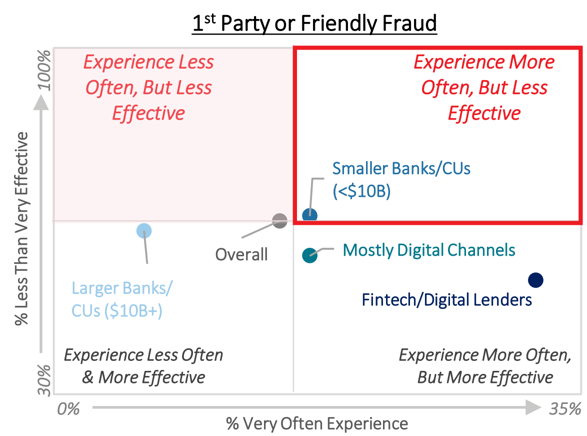
- They also report being less effective at mitigating 3rd party account takeover than others. This could be related to the use of remote channels, which requires using both physical and digital identifying information to be effective at combatting fraud.
- Smaller banks/credit unions, on the other hand, tend to be less effective at mitigating 3rd party and 1st party/friendly fraud.

Effectiveness at Mitigating Fraud Types









Survey Question: Q17. How often does your company experience the following types of SMB lending fraud?* Q18. And how effective is your company at mitigating the following types of SMB lending fraud?*

*First asked in 2020

LexisNexis RISK SOLUTIONS

Synthetic identities are a serious threat. Their very nature makes it extremely difficult to detect before damage is incurred.

Multiple real persons into a single fake identity, with a valid shipping address, Social Security Number (SSN), date of birth, name, etc. – none of which matches any one person. This type may be used for shorter-term fraud gains, such as bigger ticket items.

One real person by using some of his/her information combined with fake data. In this case, the fraudster is likely to be nurturing this identity, using it to establish a good credit history before ultimately "going bad".

No known persons in which the personally identifiable information doesn't belong to any consumer. It is entirely fabricated based on a new SSN, using the same range as the Social Security Administration for randomly-issued numbers. This may also be nurtured for longer-term gain and is useful when posing as an underbanked consumer with a less established purchasing footprint (e.g., younger Millennials).

Risks and Challenges

Extremely Hard to Distinguish from Legitimate Customers

Focus on nurturing the identity to mimic a good customer; establishes good credit, pays on- time, etc. before "breaking bad."

Difficult to detect with traditional identity verification / authentication solutions

These are professional fraudsters; they often know the types of information required to gain approval and pass certain checkpoints. Use of real identity data helps them do this.

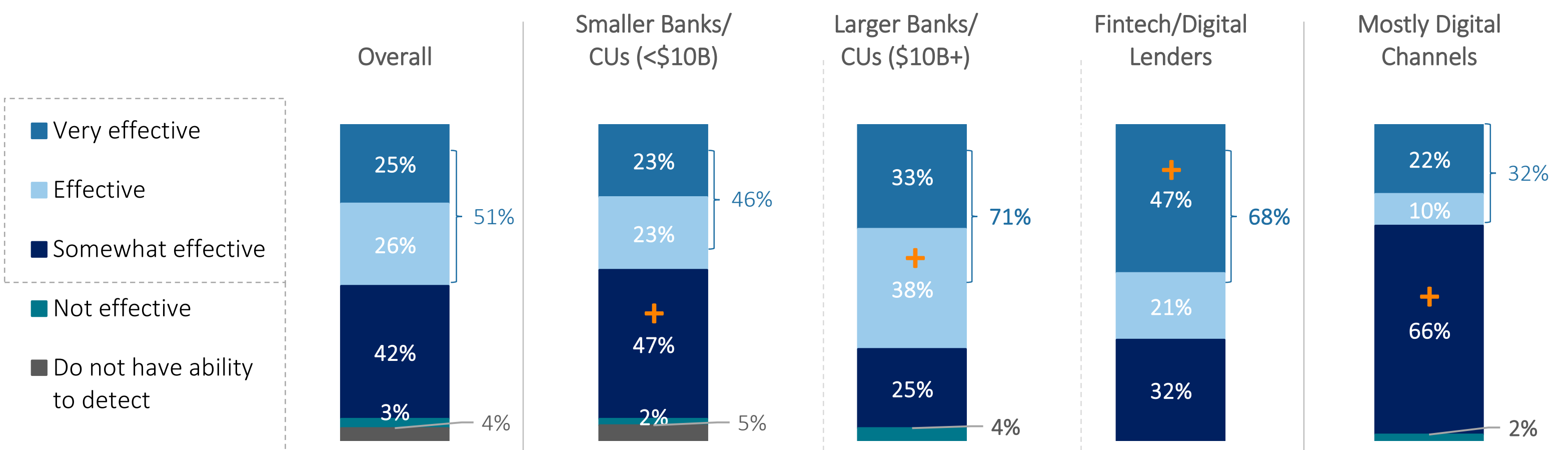
Real customers don't help; behaviors make it difficult to spot anomalies with current ID solutions

Consumers access accounts from different locations anywhere and anytime. They might share passwords and use different devices at different times. It is harder to make physical and digital connections that distinguish fraudulent from legitimate patterns.

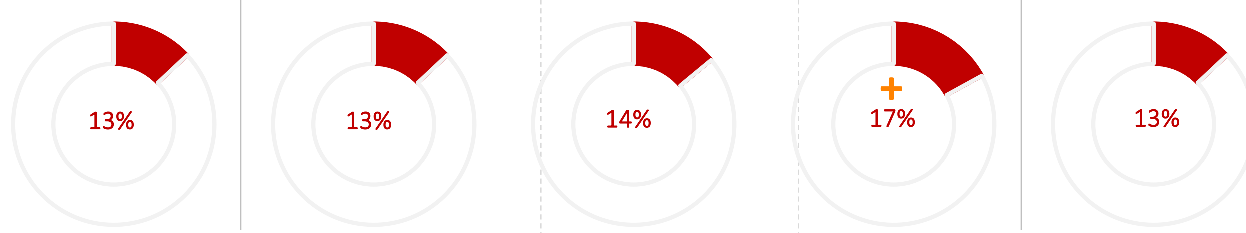
And, smaller institutions and those that operate heavily through digital channels report being only somewhat effective at detecting botnet attacks.

- Regardless of effectiveness, fintech/digital lenders tend to be attacked at a somewhat higher rate per month than others.

Effectiveness at Detecting Fraud-Related Botnet Attacks



Average % of Botnet Attacks Per month



Survey Question: Q19a. How effective would you say your company is at detecting fraud-related botnet attacks?* Q19b. In a typical month, what percent of your applications/account creations /log-ins are determined to be malicious automated bot attacks?*

*First asked in 2020 + = significantly or directionally different from other segments, 2020

Key Finding #3: Current Fraud Levels

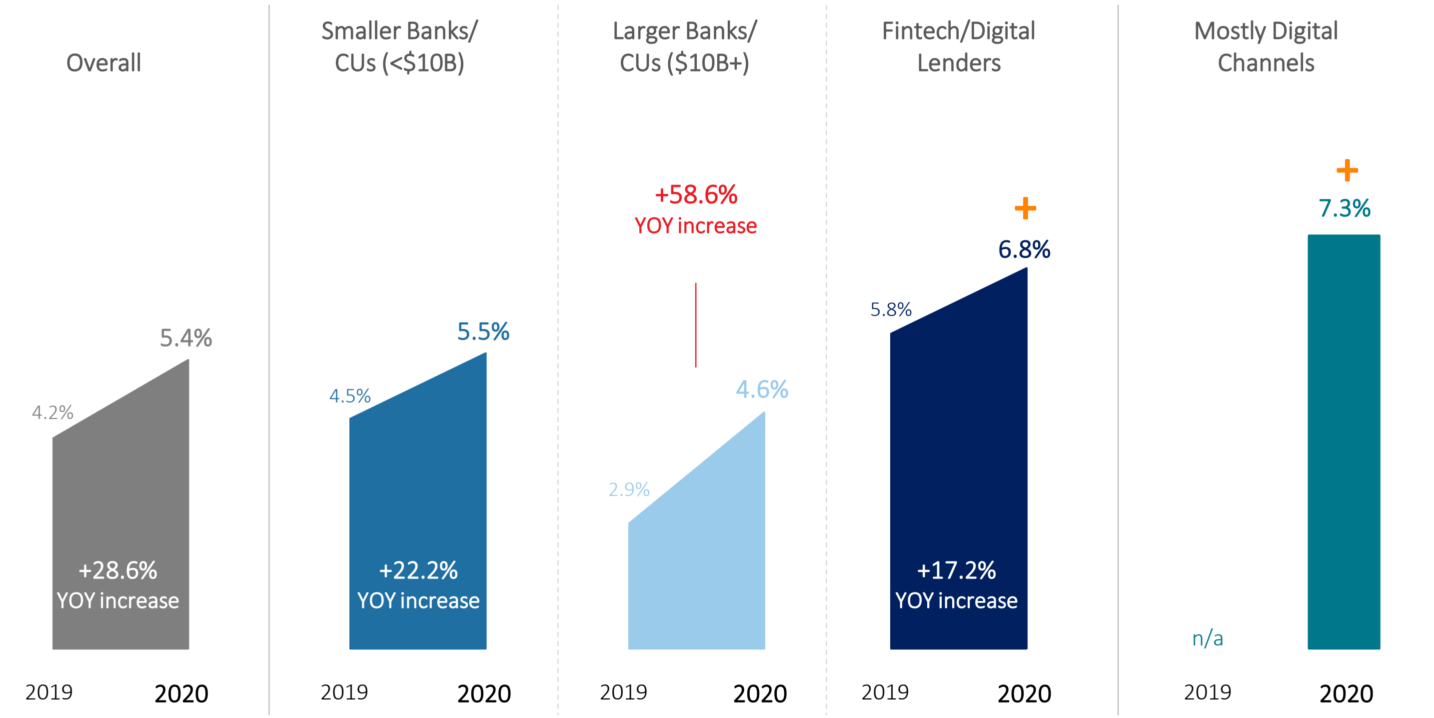
3 **The value of SMB lending fraud has increased since last year, with higher levels for lenders that operate more digitally.**

- Though fraud losses are highest for lenders that operate more digitally, larger institutions experienced the most growth – up 58.6% since last year.
- Most fraud losses occur through the online and mobile channels, and as the result of synthetic identity, account takeover, and 3 party identity fraud.

SMB lending fraud losses have increased overall from 4.2% to 5.4% of annual revenues over the past year and continue to be highest for lenders that operate more digitally.

- While SMB lending fraud as a percent of revenues is still lower for larger institutions comparatively, this segment experienced the most growth with a 58.6% increase since last year.

Value of SMB Lending Fraud as a % of Annual Revenues

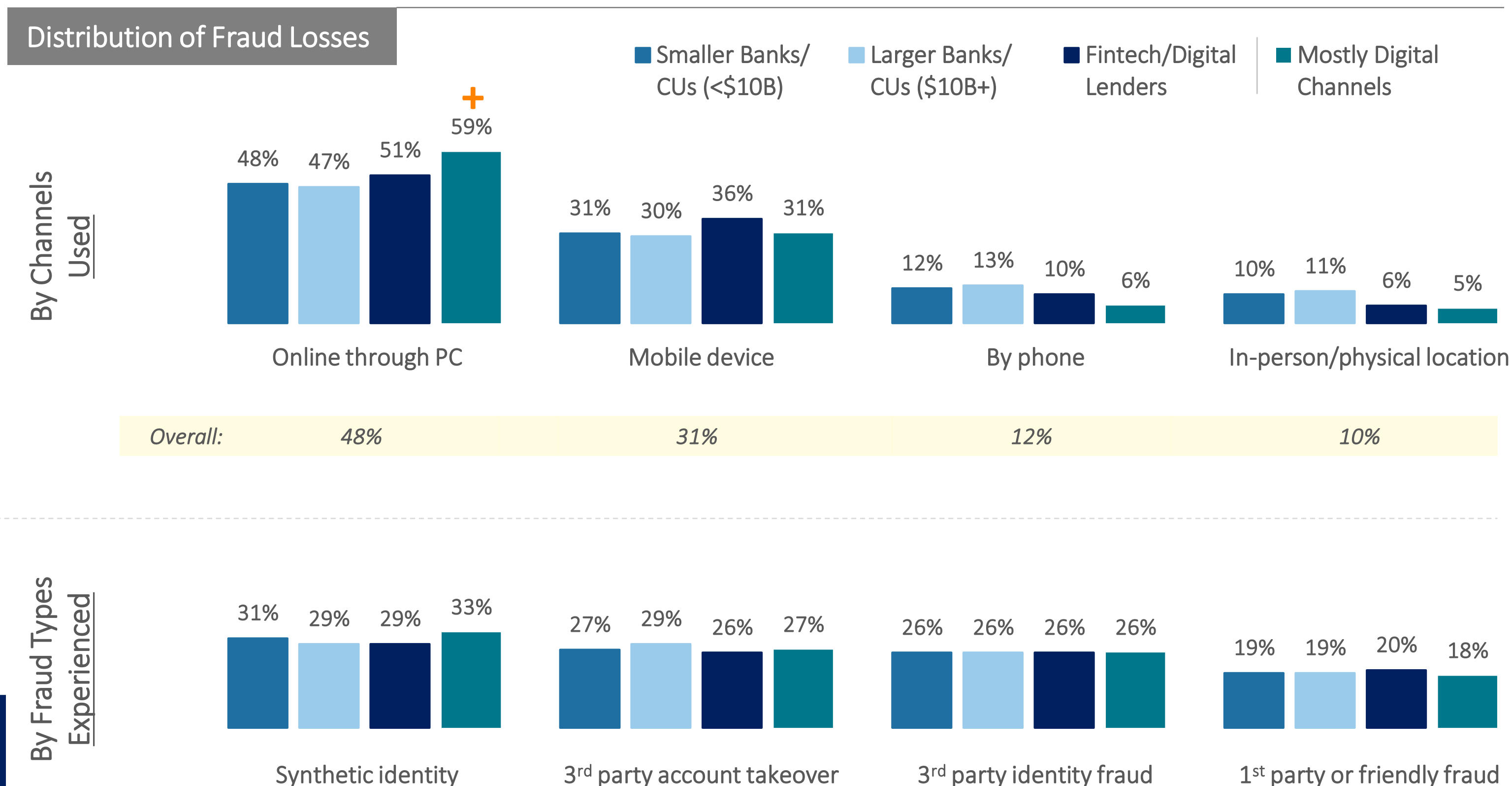


Survey Question: Q8. What is the approximate value of your company's total fraud losses over the past 12 months, as a % of annual revenues?

+ = significantly or directionally different from other segments, 2020

Given heavy usage of the online and mobile channels, it's not surprising that most SMB lending fraud losses occur through them and as the result of synthetic identity, account takeover, and 3rd party identity fraud.

- In fact, the North American financial services industry experienced a significant growth in new account creation attacks in the second half of 2019, due to sustained bot attacks.[1]
- And now, mobile attacks outpace desktop attacks by volume. While mobile browser activity is attacked at a higher rate, mobile app activity experienced a bigger growth in attack rate.[2]

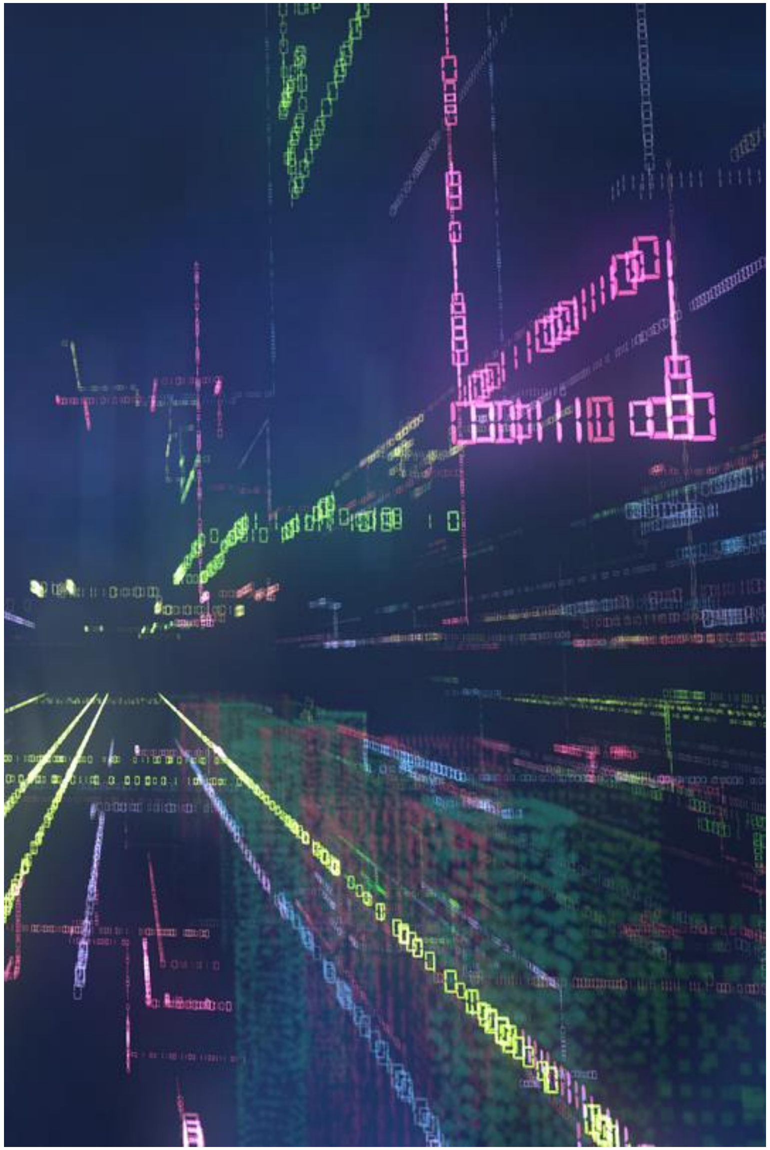


Survey Question: Q8b. Indicate the distribution of total SMB lending fraud costs generated through each of the following channels currently used by your company (as a % of total annual fraud losses).* Indicate the distribution of total SMB lending fraud losses generated through each of the following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

[1] LexisNexis® Risk Solutions Cybercrime Report, July-December 2019
[2] Ibid.

*First asked in 2020 + = significantly or directionally different from other segments, 2020

Key Finding #4: Future Fraud & Initiatives



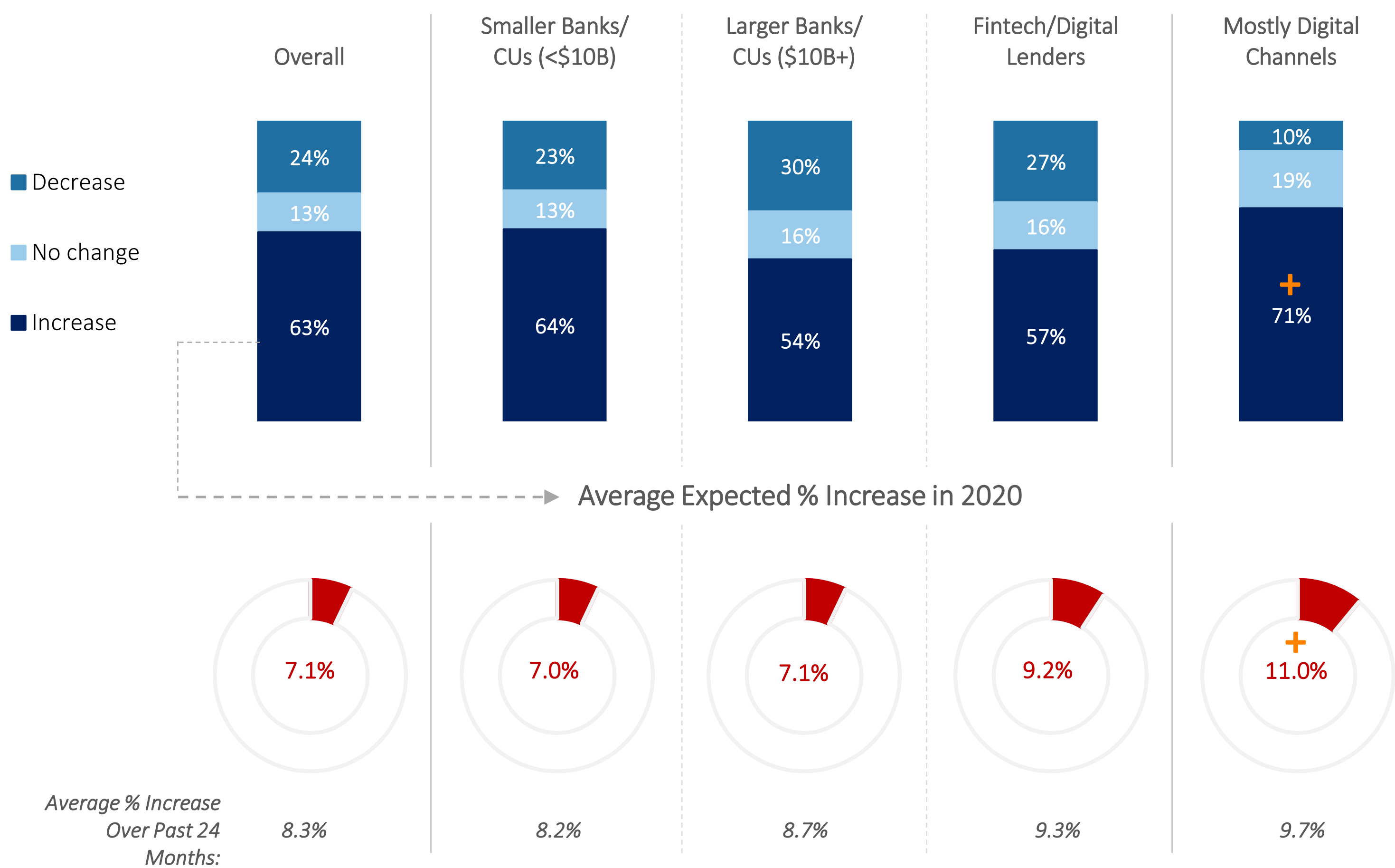
4 **SMB lending fraud for 2020 is expected to increase at nearly the same rate as for the previous 24 months, but combatting it is a key corporate priority for most.**

- Growth expectations are driven by lenders that operate heavily in the digital channels.
- Many lenders are increasing their levels of fraud prevention investment by 11%+ over last year, taking the form of increased staffing of fraud teams and higher spend on vendor solutions.

Many expect that SMB lending fraud levels will continue to grow, with expected increases for 2020 that are nearly as much as for the prior 24 month period.

- Growth expectations are highest for lenders that operate heavily through digital channels.

Expected Change in SMB Lending Fraud Levels in 2020



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

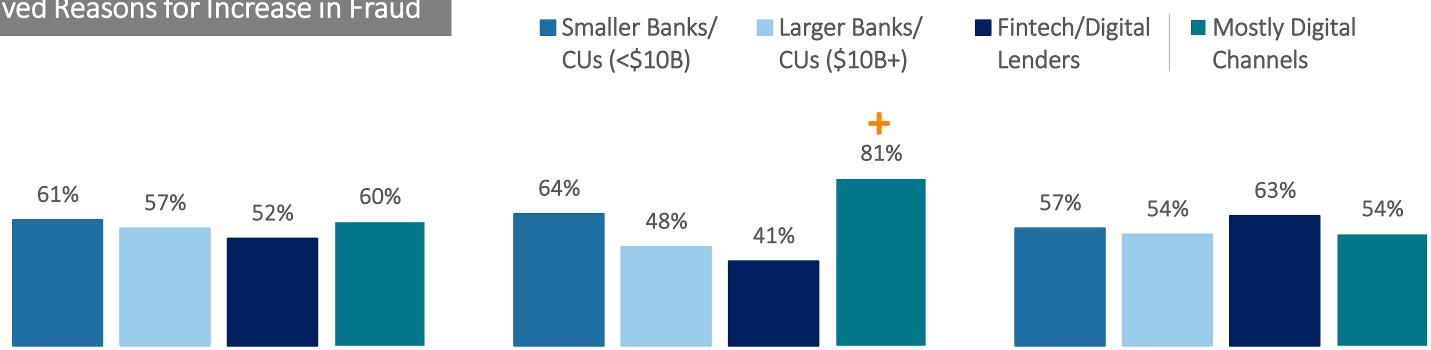
LexisNexis RISK SOLUTIONS

+ = significantly or directionally different from other segments, 2020

Overview
Key Findings
#1 Channels & Fraud Perceptions
#2 Fraud Levels, Past 24 Mos. & Types of Fraud
#3 Current Fraud Levels
#4 Future Fraud & Initiatives
#5 Solutions Use
#6 Strategic Approaches
Recommendations

Multiple factors are perceived to be contributing to increased SMB lending fraud, including complex business structures that make it easier to get away with fraud, less effort by lenders to curb SMB than consumer lending fraud, and a larger amount of money that can be stolen through SMB fraud.

Perceived Reasons for Increase in Fraud

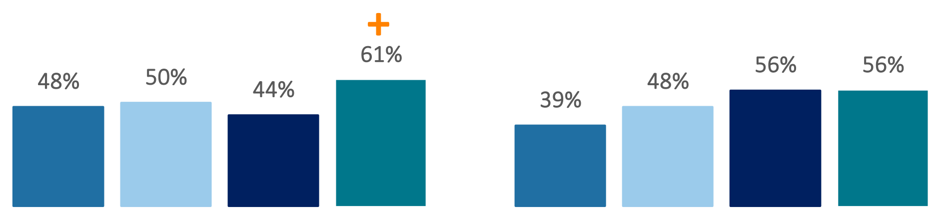


SMBs can have complex organizational structures, which means it is easier to get away with fraud in the name of the business.

Lenders place less effort on curbing SMB lending fraud than consumer lending fraud, so SMBs are an easy target for fraudsters.

The amount that a fraudster can steal by committing SMB lending fraud is typically larger than the amount a fraudster can steal by committing consumer-lending fraud.

Overall: *61%* *61%* *56%*



Fraudsters view SMBs as "victimless," which means it is less likely that law enforcement will pursue action against the fraudsters.

Consumer lending fraud has become more challenging, as lenders improve their fraud-prevention efforts, so fraudsters are following a path of least resistance to SMB lending fraud.

Overall: *48%* *41%*

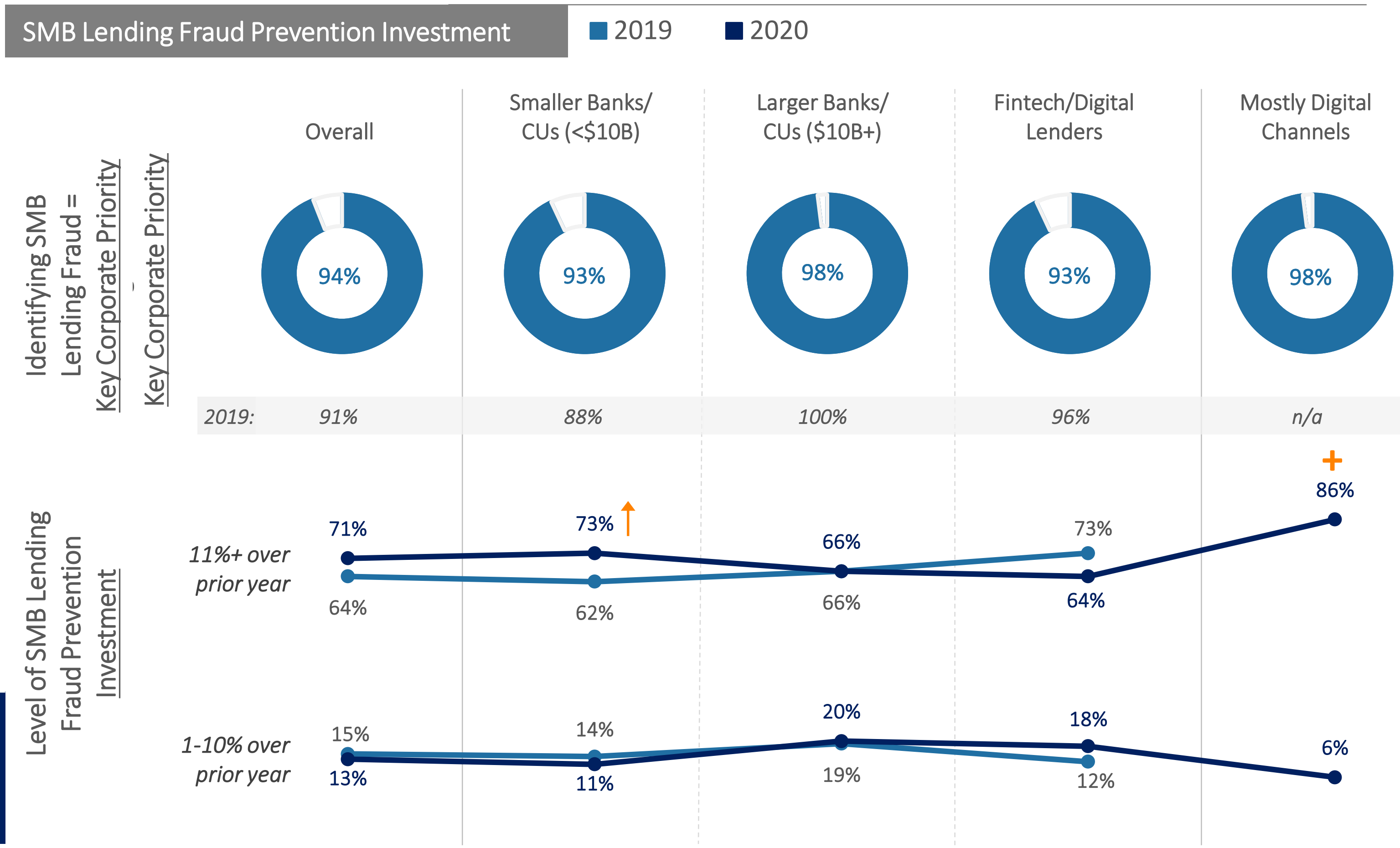
Survey Question: Q7. Why do you think SMB lending fraud is increasing?

+ = significantly or directionally different from other segments, 2020

Survey Question: Q9. Is identifying SMB lending fraud that is targeting your company a key 2020 corporate priority for your company? Q14. In 2020, at what level will your company invest to prevent SMB lending fraud from targeting it?

However, identifying SMB lending fraud is reported to be a key 2020 corporate priority for most, with many expected to increase their levels of fraud prevention investment by 11+% over last year.

- Lenders that are operating heavily through digital channels, and who expect the highest growth in fraud, expect to increase investment more than others.

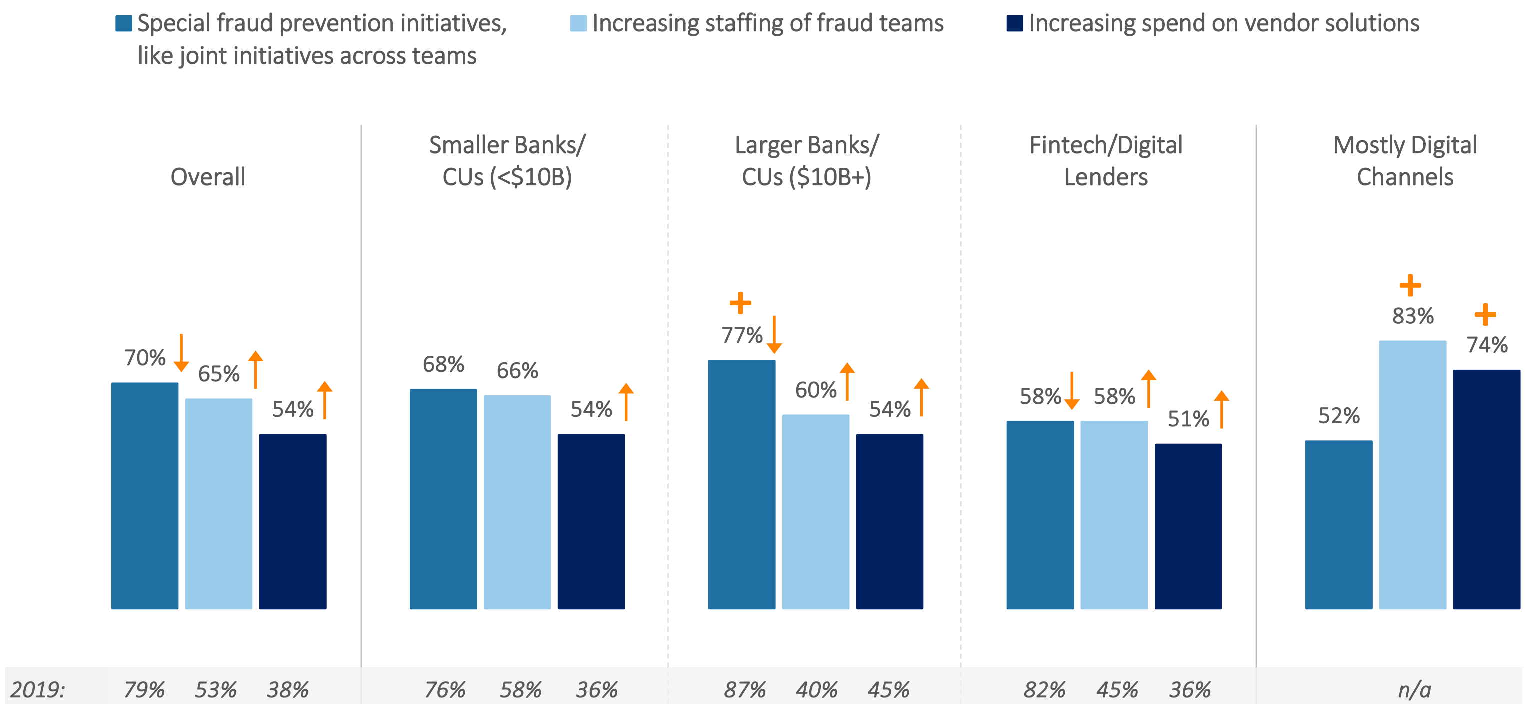


= significantly or directionally different from 2019, within segment

= significantly or directionally different from other segments, 2020

These investments include increased staffing of fraud teams and increased spend on vendor solutions, particularly among those banks/credit unions that are operating heavily through digital channels.

Activities Being Undertaken to Curb SMB Lending Fraud



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

↓↑ = significantly or directionally different from 2019, within segment
+ = significantly or directionally different from other segments, 2020

Key Finding #5: Solutions Use

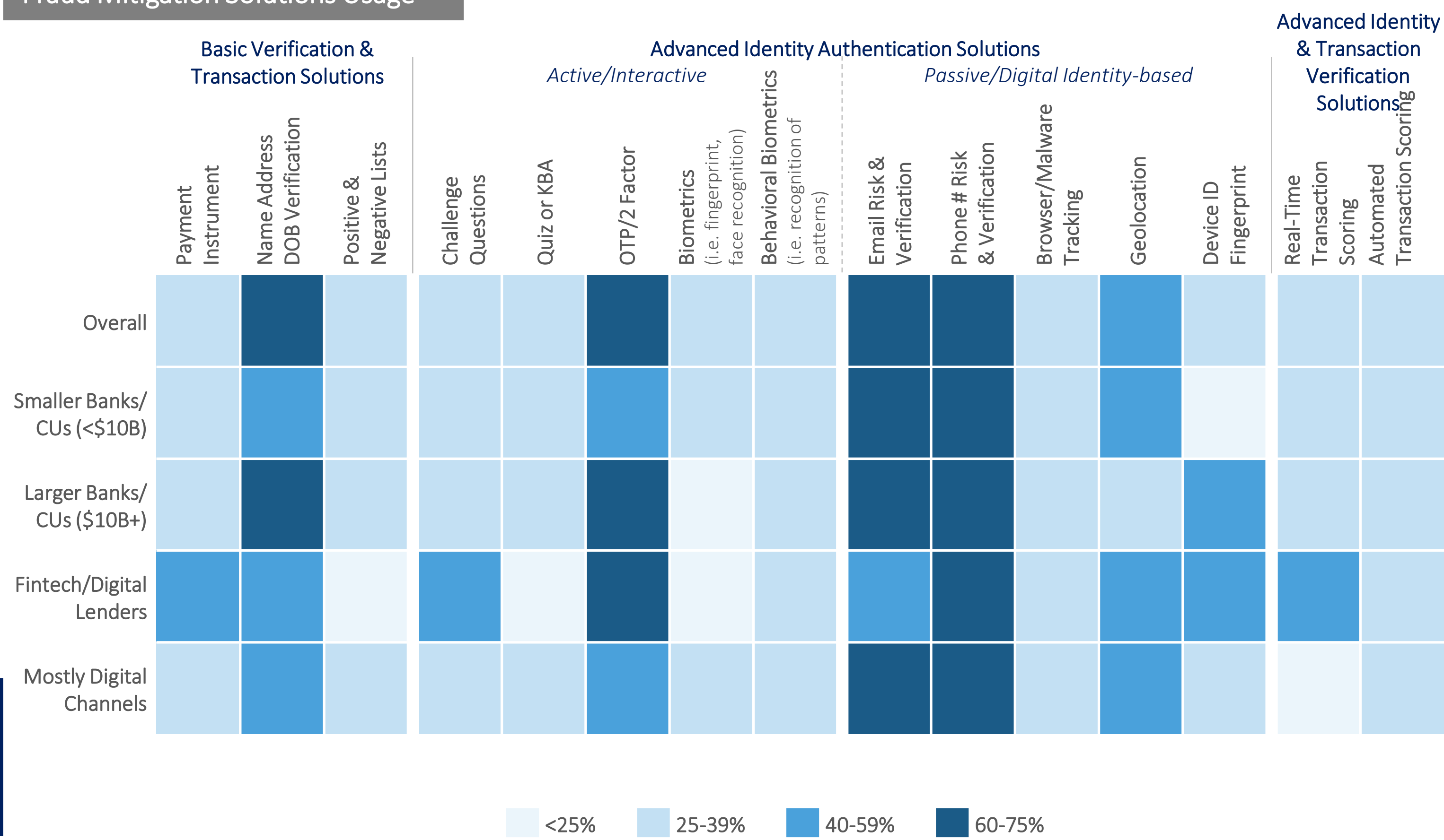
5 Lending firms may not be optimizing solutions and approaches to fight newer and more complex types of fraud, particularly those that operate more digitally.

- Many lenders report the usage of OTP/2 factor and e-mail and phone authentication, but the use of other identity solutions designed to address unique digital identity threats is currently more limited.
- More fraud prevention dollars are currently spent on labor/resources, but this is expected to shift more toward fraud prevention solutions 2 years from now.
- Though many are reportedly increasing spend on vendor solutions, only some are planning to implement the more advanced physical and digital identity authentication solutions that are currently more limited in use.

While many SMB lenders report using OTP/2 factor and e-mail and phone authentication, the use of other identity solutions designed to address unique digital identity threats, such as synthetic identities and botnets, is currently more limited.

- This is the case even for lenders that are most vulnerable to digital threats.

Fraud Mitigation Solutions Usage

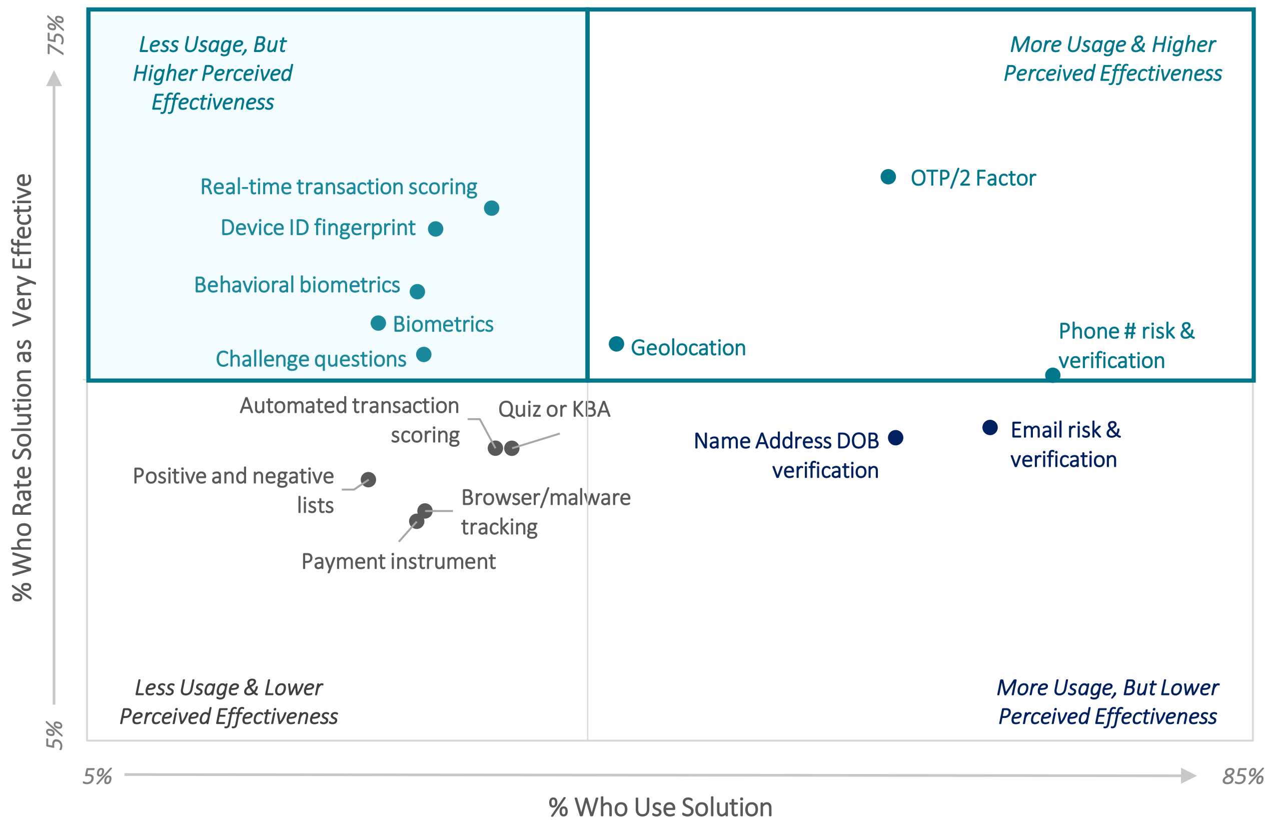


Survey Question: Q20. Which of the following solutions does your company currently use to help combat/prevent SMB lending fraud?*

*First asked in 2020

While OTP/2 factor, phone verification, and geolocation are more widely used, real-time transaction scoring, device ID fingerprint, biometrics, behavioral biometrics, and challenge questions are reported to be just as effective at combatting SMB lending fraud.

Effectiveness of Fraud Mitigation Solutions

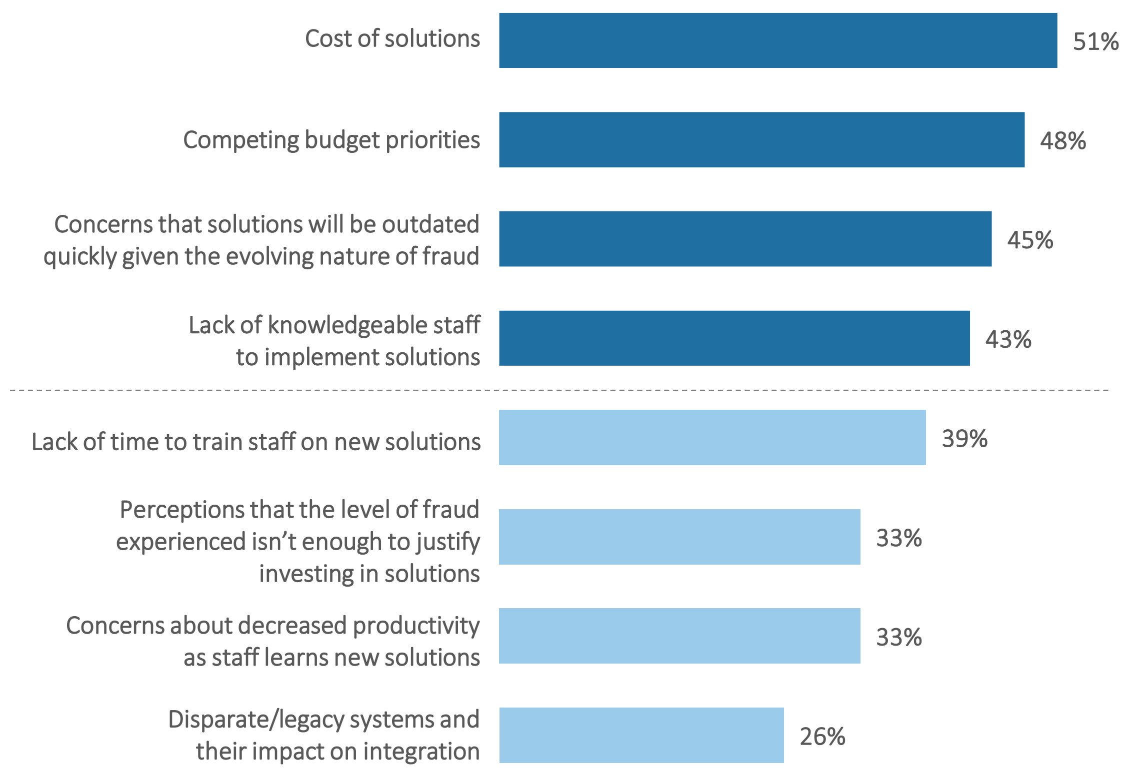


Survey Question: Q20. Which of the following solutions does your company currently use to help combat/prevent SMB lending fraud?* Q21. How effective are the solutions that your company currently uses at combatting/preventing SMB lending fraud?

*First asked in 2020

Where SMB lenders haven't been able to make investments in fraud solutions, it tends to be related to solutions cost, competing priorities, concerns that the solutions will not keep up with the evolution of fraud types/methods, and a lack of knowledgeable staff.

Barriers to Investing in Fraud Mitigation Solutions



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

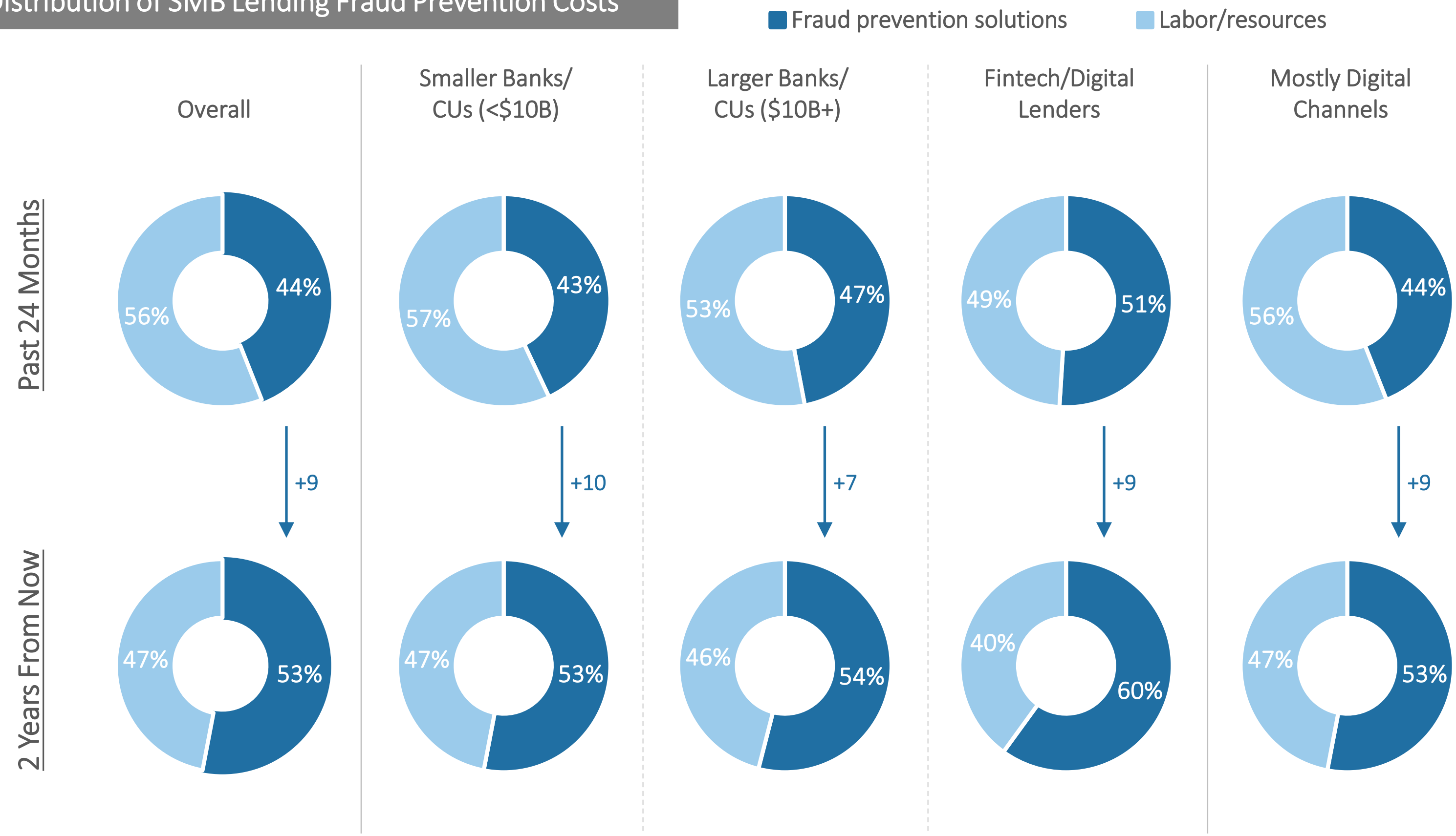
LexisNexis RISK SOLUTIONS

*First asked in 2020

SMB lenders are currently spending more of their fraud prevention dollars on labor/resources, but this is expected to shift slightly more toward fraud prevention solutions 2 years from now.

- That said, a sizeable portion of fraud prevention costs are still expected to include human/manual resources; this will contribute to increasing fraud prevention costs as salaries and benefits rise over time - particularly if more skilled labor is required as fraud methods increase in complexity.

Distribution of SMB Lending Fraud Prevention Costs



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

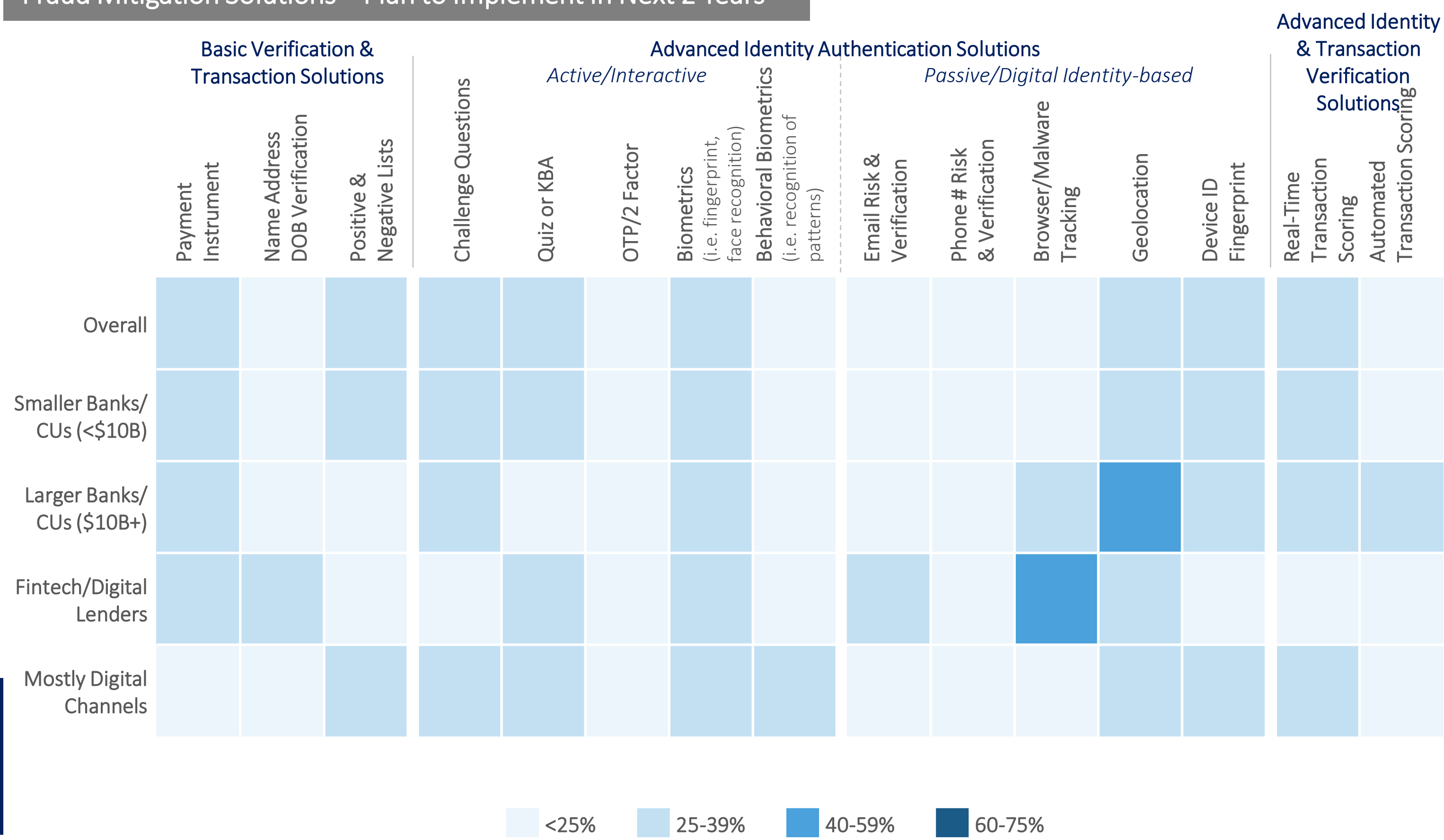
LexisNexis® RISK SOLUTIONS

*First asked in 2020

Though many expect to increase spend on vendor solutions, only some are planning to implement more advanced physical and digital identity authentication solutions that are important for detecting and preventing fraud in remote channels.

- These include challenge questions, quiz/KBA, biometrics and behavioral biometrics, and browser/malware tracking.

Fraud Mitigation Solutions – Plan to Implement in Next 2 Years



Survey Question: Q23. Which of the following solutions does your company plan to implement in the next 2 years to help combat/prevent SMB lending fraud?*

*First asked in 2020

Key Finding #6: Strategic Approaches

6

Study findings show that SMB lenders that use a layered solutions approach involving identity authentication and verification, including digital identity/behavior and biometric tools, experience a lower proportion of fraud.

- The risks posed by remote channels, in particular mobile, are different from those in in-person environments. The ability to distinguish between a legitimate person or business and a fraudster is very difficult when a criminal is using a synthetic identity with real personally identifiable information.
- Different solutions need to be applied for different channels. These should assess fraud for using both physical and digital identifying information.

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 trans-action 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: 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

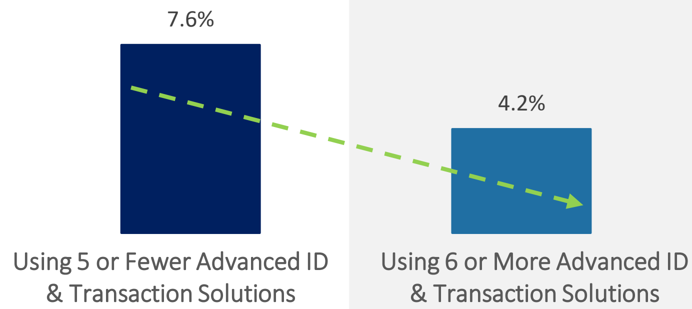
Device assessment: uniquely identify a remote computing device or user.
Solution examples: device ID/ fingerprint; geolocation

LexisNexis RISK SOLUTIONS

Study findings show that SMB lenders that layer more advanced identity authentication + advanced transaction/identity verification solutions have a lower proportion of fraud costs than others.

Layering of Fraud Mitigation Solutions

SMB Lending Fraud
as a % of Revenues



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 & Transaction Verification Solutions	Automated Transaction Scoring, Real-Time Transaction Scoring	Minimal	✓
	Average # Advanced Solutions Used	4	7

LexisNexis RISK SOLUTIONS

Data on the Impact of COVID-19

Shortly after the conclusion of our initial study, the impacts of Covid-19 began. We revisited a small sample of our March 2020 study respondents in June 2020 to assess how the developing economic and geopolitical consequences of the Covid-19 pandemic are challenging SMB lenders.

Main takeaways from conversations with our follow-up sample include:

- The types and frequency of SMB fraud have remained fairly consistent with pre-COVID levels. Respondents noted a slight increase in the frequency of stolen legitimate business identity and stolen consumer/owner identity fraud. This coincides with the application period for SMB Paycheck Protection loans, which suggests that fraudsters tried to take advantage of the program.
- Reported changes in SMB lending fraud losses compared to Pre-COVID levels are evenly mixed. 46% of follow-up respondents have seen decreases in fraud between 1-9%. 47% of our sample reported increases in fraud between 1-9%.
- Opinions are also nearly evenly divided on the expected time to return to 2/3 to 3/4 of typical Pre-COVID SMB Lending Levels. 44% feel it will take between 3-9 months while the remaining 56% of respondents felt it will take 9 months or longer.

*The initial study was completed before the COVID pandemic, so we followed up with a third of the original respondents to gather data on how COVID impacted lenders.

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 mutate; 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.

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 a number of 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 more high 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.

LexisNexis®

RISK SOLUTIONS