

2023 SMB Lending Fraud Study



LexisNexis®
RISK SOLUTIONS



Overview



Key Findings



#1 Fraud Trends



#2 Fraud Costs



#3 Channel Risks



#4 Solutions Use



#5 Smart Practices



Recommendations

Background

LexisNexis® Risk Solutions sought primary market research with lenders to understand small and midsize business (SMB) lending fraud. The intent was 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 to understand included:

- 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
- Any differences in the above by size or type of organization



Overview



Key Findings



#1 Fraud Trends



#2 Fraud Costs



#3 Channel Risks



#4 Solutions Use



#5 Smart Practices



Recommendations

Methodology

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

- Data was collected by phone during September and October 2022. A total of 147 completions were obtained, broken out as follows:

Total	<\$10B Asset Banks/Credit Unions	\$10B+ Asset Banks/Credit Unions	Fintech/Digital Lenders	Payment Processors*
147	55	57	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.



Overview



Key Findings



#1 Fraud Trends



#2 Fraud Costs



#3 Channel Risks



#4 Solutions Use



#5 Smart Practices



Recommendations

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



Overview



Key Findings



#1 Fraud Trends



#2 Fraud Costs



#3 Channel Risks



#4 Solutions Use



#5 Smart Practices



Recommendations

Key Findings

01

SMB lending fraud has increased significantly during the past 12 months, with many smaller banks/CUs and Fintechs expecting fraud levels to worsen over the next 12 months.

02

SMB lending fraud prevention costs are predominantly centered on labor, but lenders have been investing more in fraud prevention solutions over the past 12 months.

03

Remote channel transactions are driving fraud, though there is some uptick with in-person loan applications and fraud losses.

04

SMB lenders expect that they will continue to invest more in fraud prevention, with smaller banks/CUs, Fintechs and those with mostly digital channels being particularly likely to increase staffing on fraud teams.

05

Study findings show that lenders which use a multi-layered solutions approach that integrates with cybersecurity and the digital channel operations can be **more effective at detecting and mitigating fraud and its costs early**.

Key Finding #1: Fraud Trends



SMB lending fraud has increased significantly during the past 12 months, with many smaller banks/CUs and Fintechs expecting fraud levels to worsen over the next 12 months.

Most SMB lending fraud is being caught after the point of origination.

Although bogus business credentials and fake consumer/owner identities remain the overall most common type of SMB lending fraud, smaller banks/CUs and Fintechs in particular are also experiencing more legitimate business and fake identity fraud, which they find challenging to mitigate effectively.

A lack of effort on curbing SMB lending fraud, market economic uncertainties, the perception of SMB to be an easier target than consumers and online/mobile channel transactions are perceived drivers of increased fraud.

SMB lenders are concerned about balancing fraud detection with minimizing customer friction. They are also concerned about the negative impacts of fraud on costs and revenues.

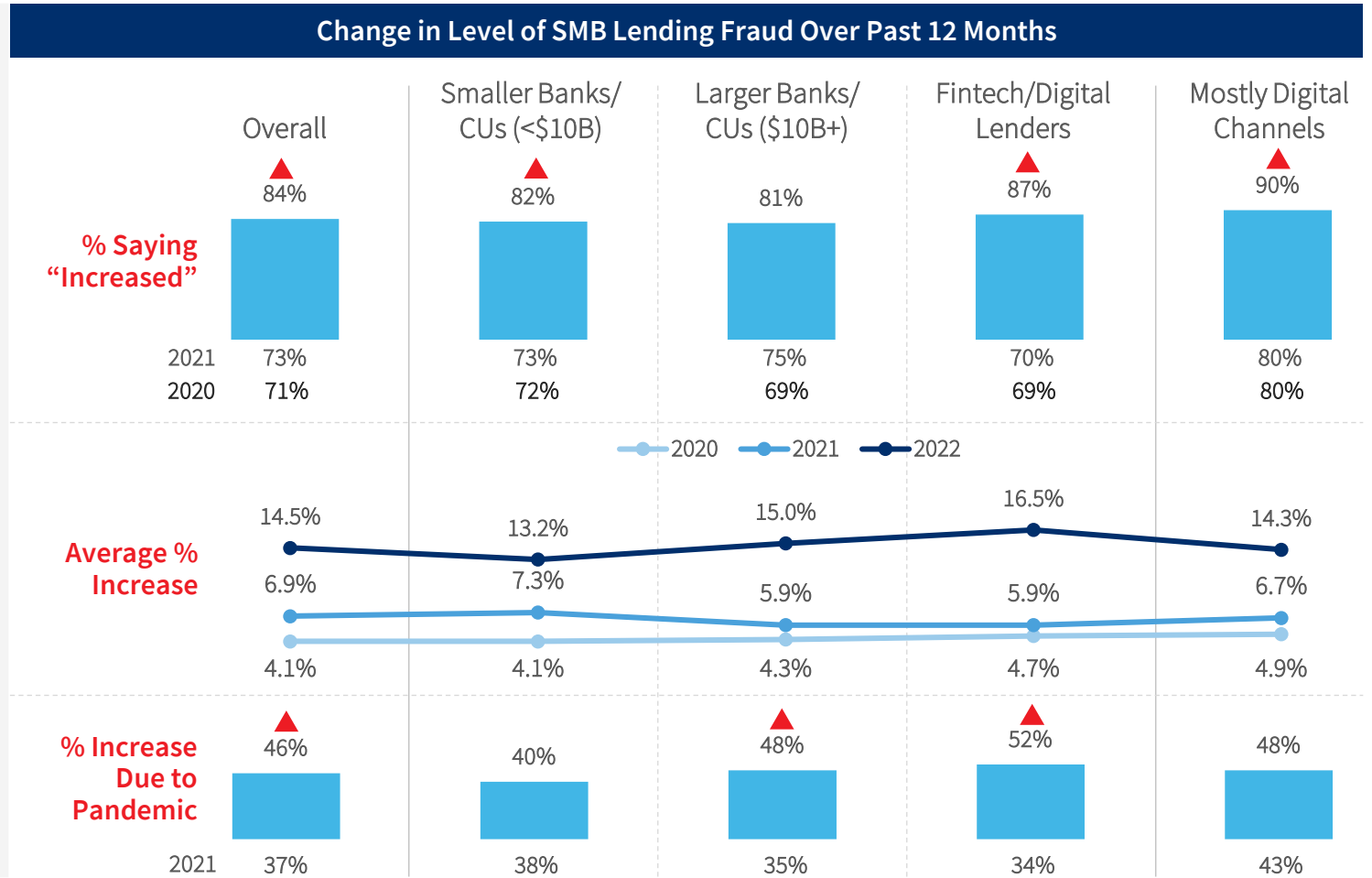
	Overview
	Key Findings
#1	Fraud Trends
#2	Fraud Costs
#3	Channel Risks
#4	Solutions Use
#5	Smart Practices
	Recommendations

Q5A. Over the past 12 months, has SMB lending fraud targeted at your company increased or decreased and by how much? Q5B. Of this [insert % increase], how much of that was due to the COVID-19 pandemic?

SMB lending fraud is increasing at a faster pace compared to the last two years, with the pandemic still accounting for increases. The year-on-year increases have more than doubled compared to 2021.

There has been a sizeable increase in Fintechs/digital lenders that have experienced more SMB lending fraud, with the average increase in fraud exceeding the other segments. Almost all lenders processing most of their loans via digital channels have also indicated an increase in SMB lending fraud.

▲ = significantly or directionally different from 2021, within segment



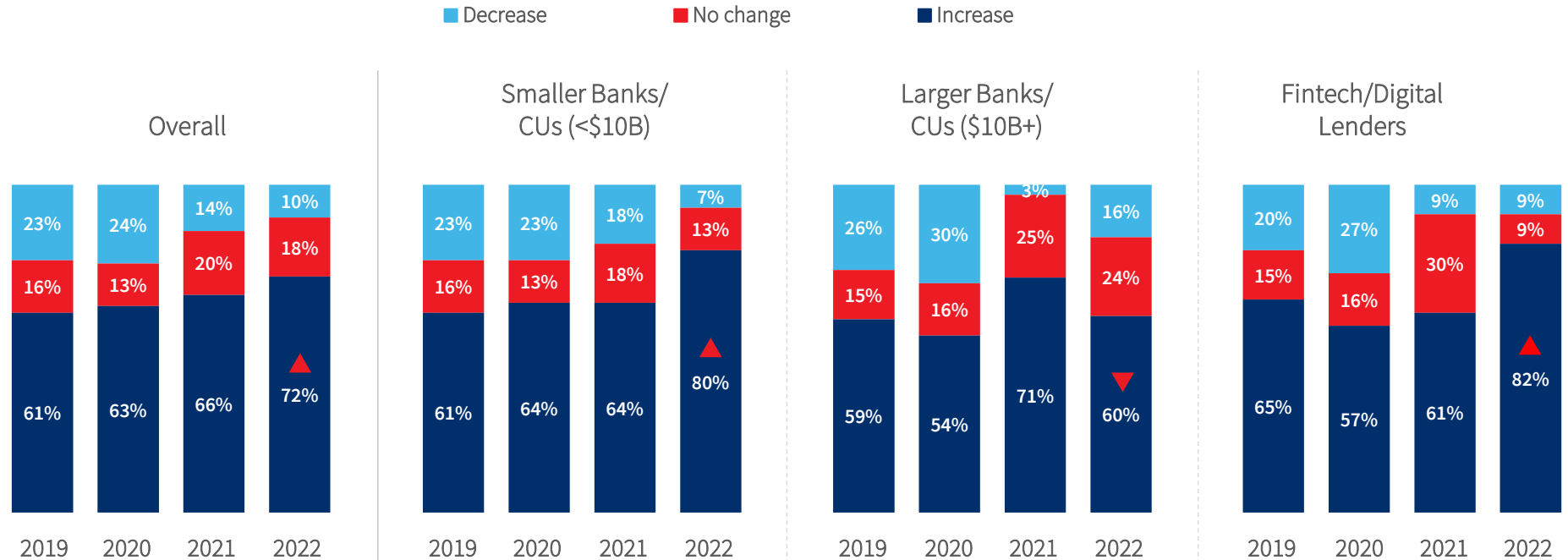
Q6. During the next 12 months, do you expect SMB lending fraud targeted at your company to increase or decrease and by how much?

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

Significantly more smaller banks/CUs and digital lenders expect SMB lending fraud levels to increase over the next 12 months.

The average expected increase cited across segments is approximately 10%, which is twice that of 2021 (5%). This increase is driven largely by smaller banks/CUs, which expect fraud to increase by 12%.

Expected Change in SMB Lending Fraud Levels in the Next 12 Months

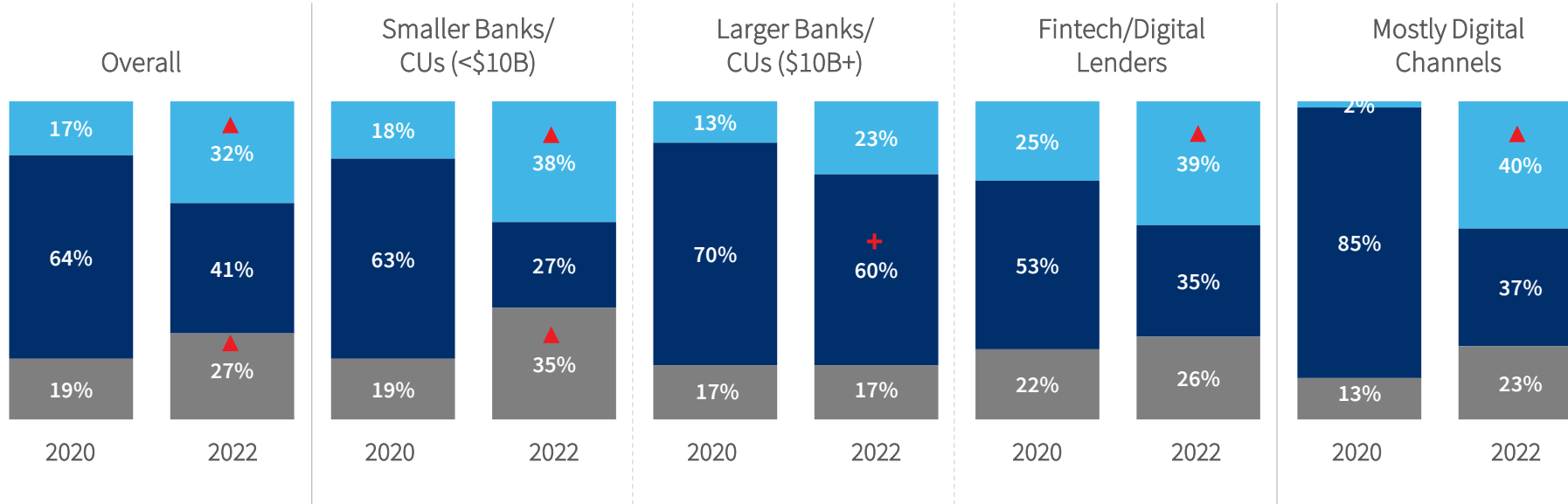


Compared to the early pandemic period, more lenders are catching fraud at the point of account origination though the majority continue to identify it at some point afterwards.

Large banks/CUs are more likely to catch fraud earlier, most often within the first month of the customer relationship.

Identification of SMB Lending Fraud

■ At the point of account origination ■ Within the first month of the customer relationship ■ After an account has charged off



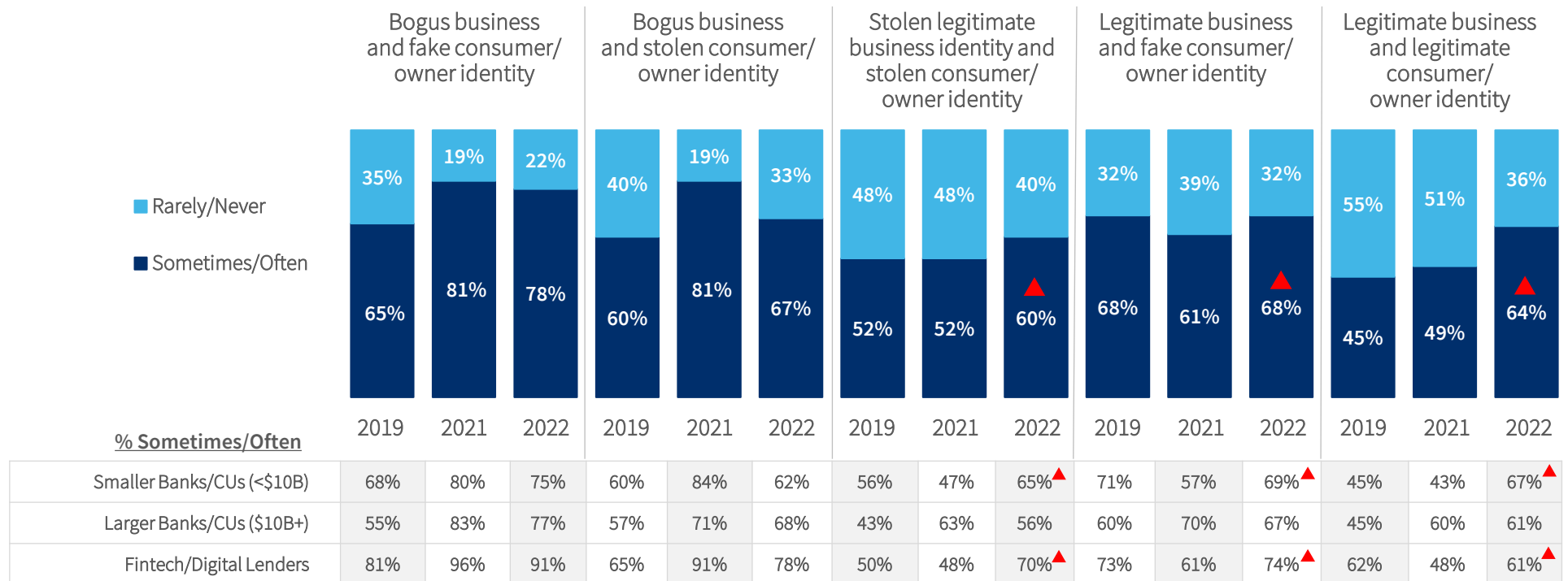
Q12. When do you typically identify an SMB lending fraud that is targeting your company?

▲ = significantly or directionally different from 2021, within segment
 + = significantly or directionally different from other segments, 2022

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

Although bogus business credentials and fake consumer/owner identities remain the most common type of SMB lending fraud, there has been an increase in the number of smaller banks/CUs and Fintechs also experiencing legitimate and stolen business credentials fraud.

Frequency With Which Fraud Types Are Experienced

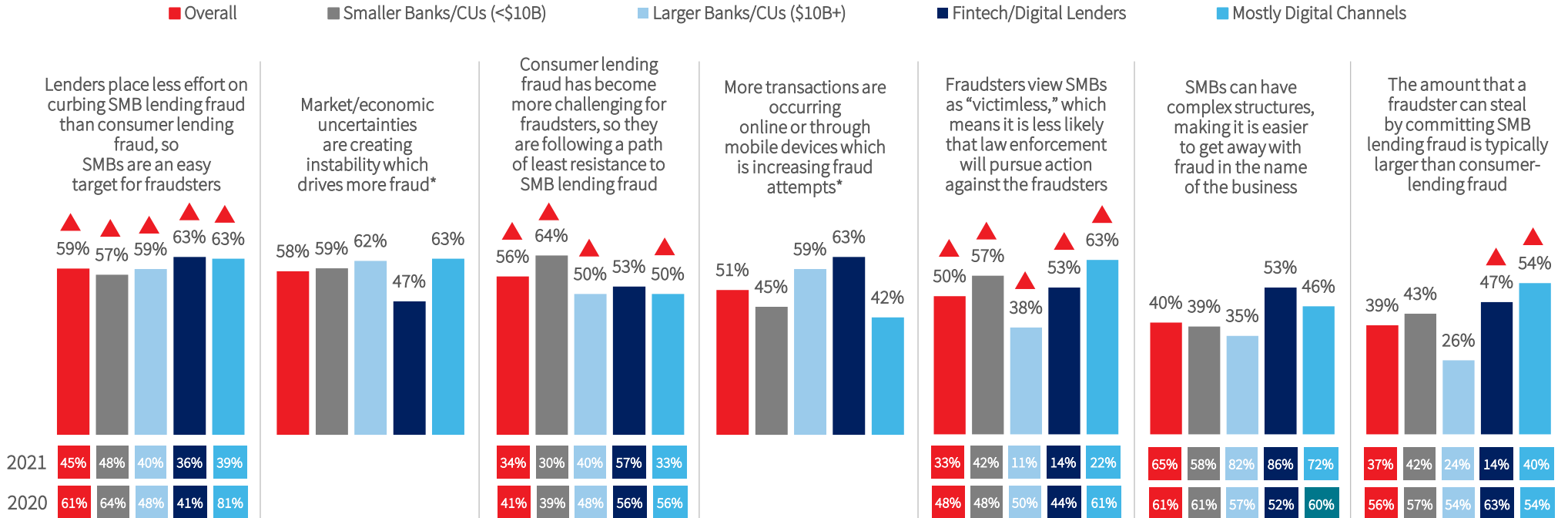


▲ = significantly or directionally different from 2020, within segment

A majority of lenders attribute increased fraud to multiple reasons, such as a lack of effort on curbing SMB lending fraud, market economic uncertainties and the perception of SMB being an easier target than consumers.

Online and mobile channel transactions are also perceived drivers of increased fraud.

Perceived Reasons for Increase in Fraud

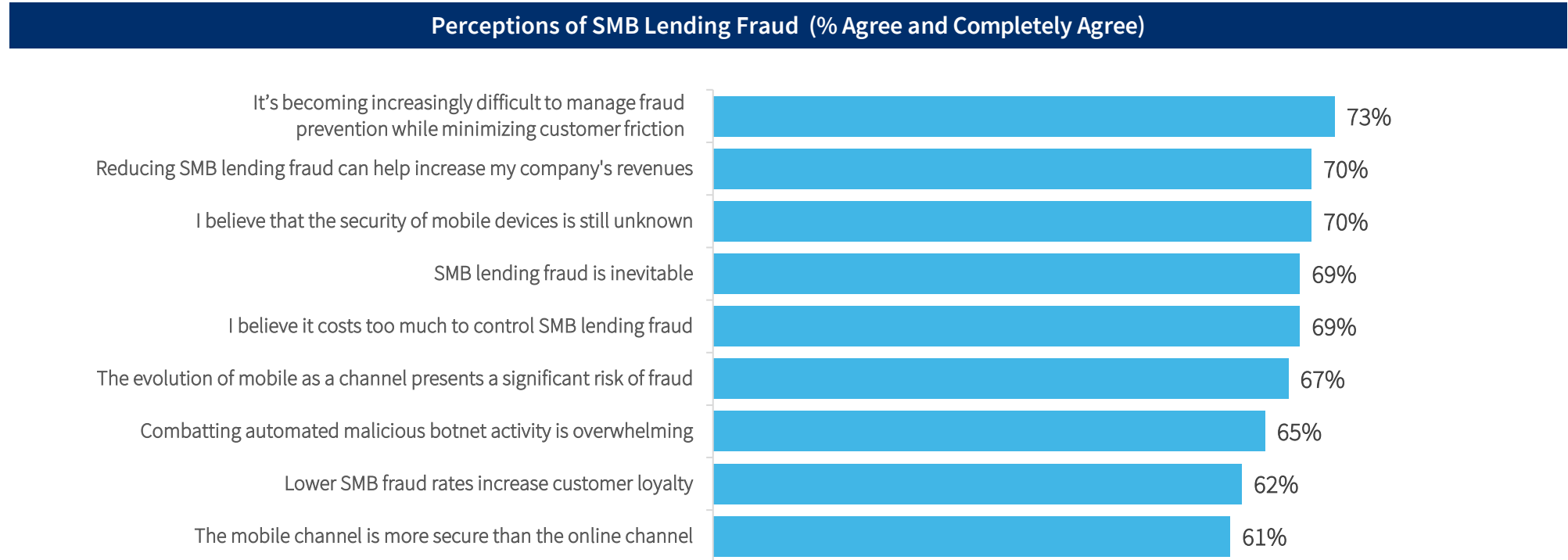


▲ = significantly or directionally different from 2021, within segment
 *First asked in 2022

Q26. Please rate the extent to which you agree or disagree with the statements below.

Many SMB lenders have multiple concerns about fraud, including being able to manage its prevention while minimizing customer friction and reducing the negative impact on costs and revenue.

While most lenders acknowledge that SMB lending fraud is inevitable, they also believe that reducing it can help increase their revenues and customer loyalty. The mobile channel particularly raises concerns about security and fraud risk.

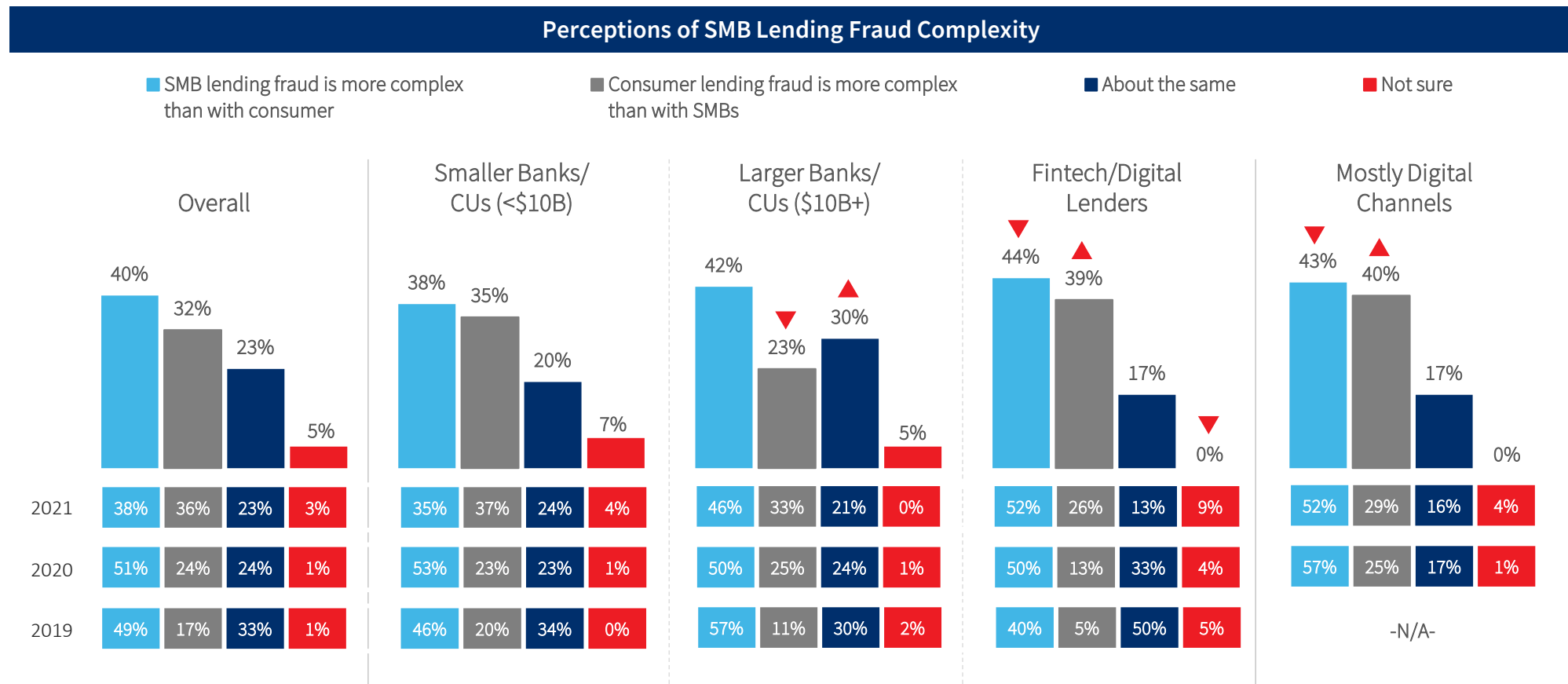


Q16. How does a fraud involving an SMB targeting your company compare to a fraud that involves only a consumer targeting your company?

▲ ▼ = significantly or directionally different from 2021, within segment

Overall, SMB lenders have mixed opinions on whether SMB lending fraud is more complex than consumer lending fraud in this post-pandemic environment.

There is an upward trend with lenders either seeing consumer lending fraud as more complex than with SMBs or that it is about the same between both types.











Key Finding #2: Fraud Costs



SMB lending fraud prevention costs are predominantly centered on labor, but lenders have been investing more in fraud prevention solutions over the past 12 months.

SMB lending fraud losses are likely to represent up to 15% of overall losses. About 19% of SMB lending fraud losses are attributed to post-pandemic changes to how transactions are occurring.

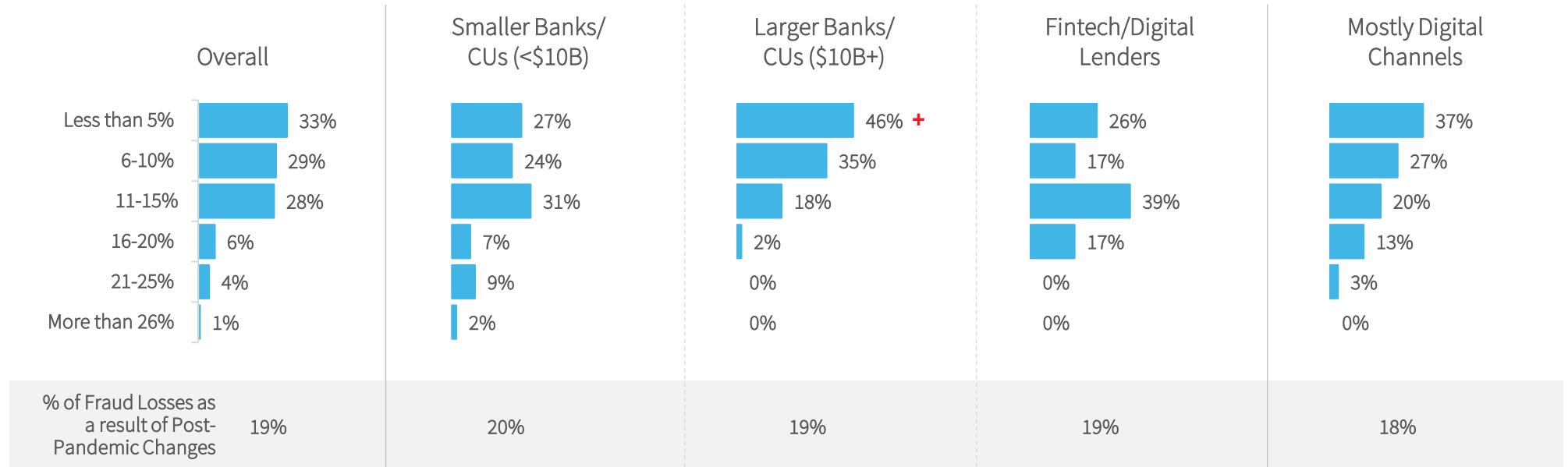
The average value of SMB lending fraud losses as a percent of annual revenues remains higher than before the pandemic (5.5% overall), with Fintechs continuing to experience the highest hit. This reflects a slight settling back to early pandemic figures after spiking as the pandemic progressed.

	Overview
	Key Findings
	#1 Fraud Trends
	#2 Fraud Costs
	#3 Channel Risks
	#4 Solutions Use
	#5 Smart Practices
	Recommendations

Overall, SMB lending fraud losses are likely to represent up to 15% of overall losses. About 19% of SMB lending fraud losses are attributed to post-pandemic changes to how transactions are occurring.

SMB lending fraud as a percent of overall losses is somewhat less among larger banks, with nearly half indicating only up to 5%.

% of Overall Losses Resulting From SMB Lending Fraud



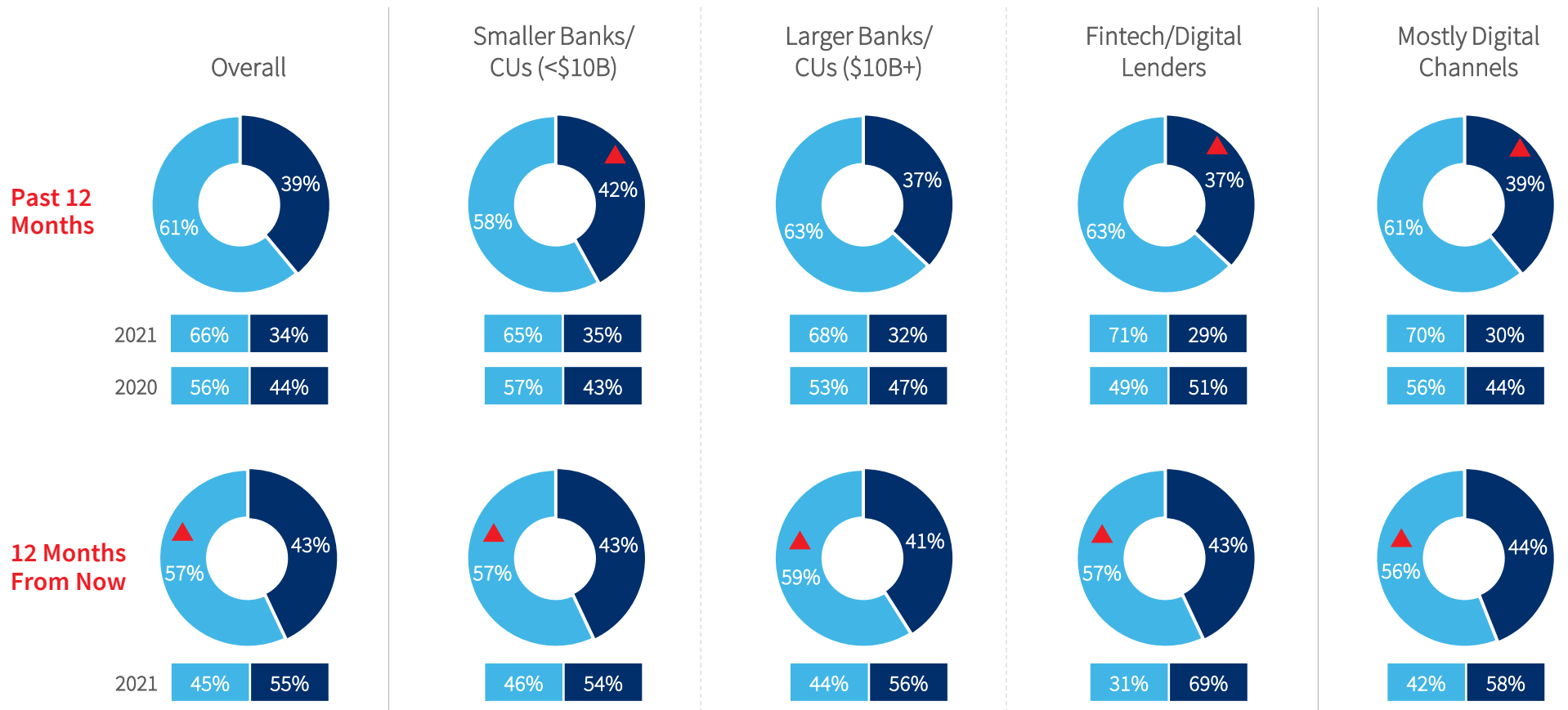
Q11A. What percent of the overall losses at your company do you suspect are because of SMB lending fraud that is targeting your company (please assume confirmed fraud and suspected fraud)? Q11B. Of the overall (insert % from Q11A) of losses directly related to SMB lending fraud, how much of this is because of new normal/post-pandemic changes to ways that transactions occur?

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 percentage distribution of SMB lending fraud prevention costs across the following areas will be during the next 12 months?

Most of the SMB lending fraud prevention costs continue to be centered on labor, with expectations for that continue over the next 12 months.

Distribution of SMB Lending Fraud Prevention Costs

■ Labor/resources ■ Fraud prevention solutions



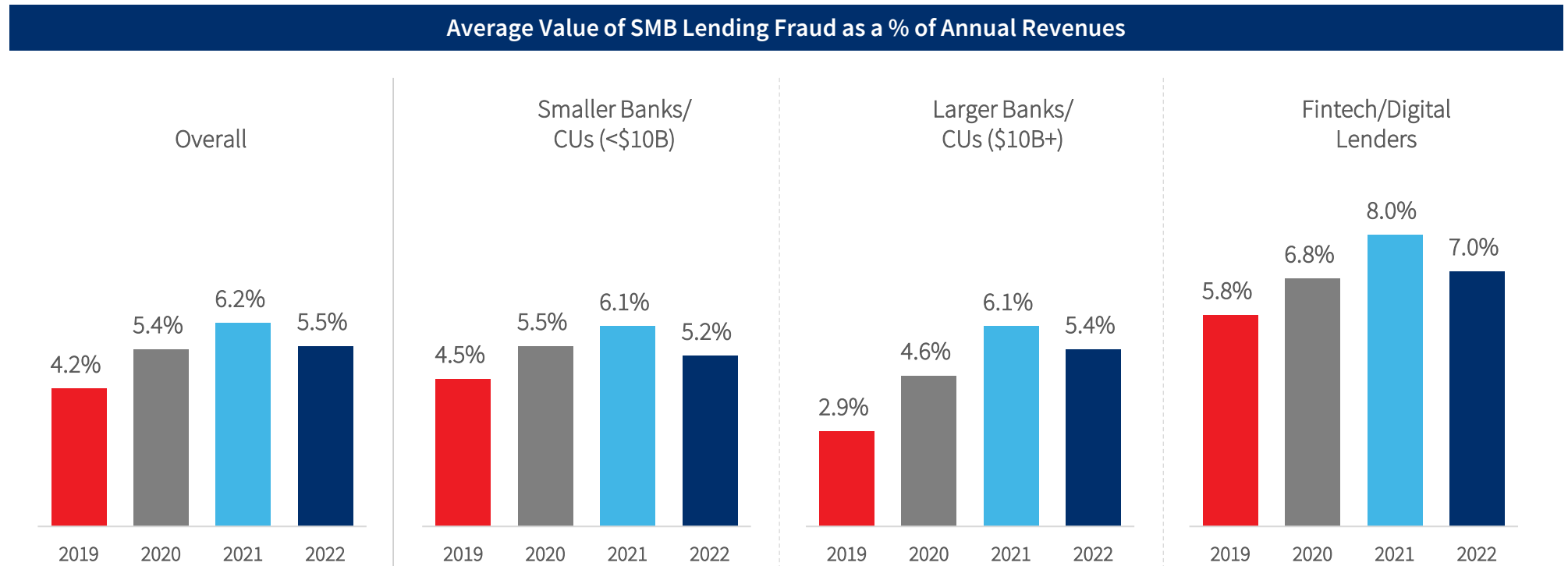
▲ = significantly or directionally different from 2021, within segment

CONFIDENTIAL

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

The average value of SMB lending fraud losses as a percent of annual revenues remains higher than before the pandemic (5.5% overall), with Fintechs continuing to experience the highest hit.

Findings show that the average value of fraud as a percent of annual revenues has settled back slightly towards the early pandemic period, after experiencing a spike as the pandemic progressed.



Key Finding #3: Channel Risks



Remote channel transactions are driving fraud, though there is some uptick with in-person loan applications and fraud losses.

Over half of the applications are submitted through remote channels (online/mobile), with a similar proportion of fraud losses attributed to these channels.

Banks/CUs are experiencing a limited uptick of in-person loan applications and fraud losses as most banks resume normal in-person operations.

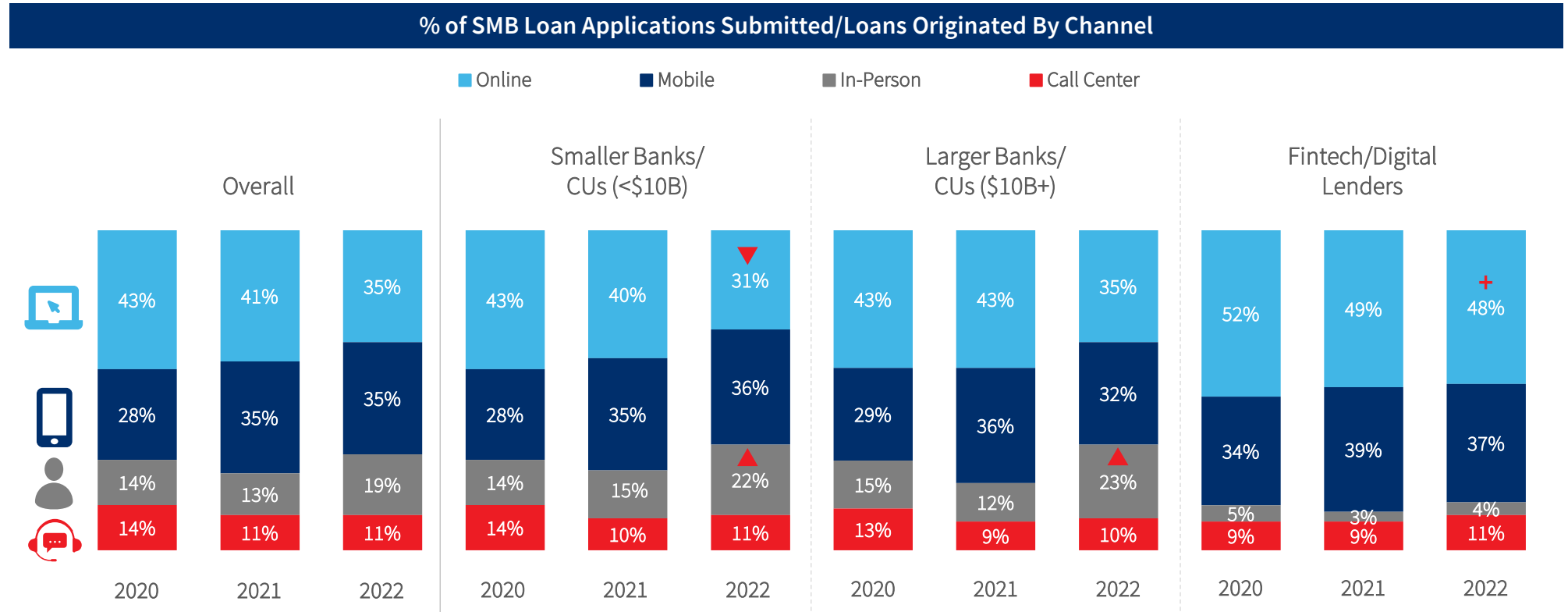
In the post-pandemic market, most lenders have changed their approach to detecting and mitigating SMB lending fraud with online and mobile transactions. This includes investments in training, increased staff and fraud detection solutions technology.

The above changes also include tightening protocols with online and mobile channels.

	Overview
	Key Findings
	#1 Fraud Trends
	#2 Fraud Costs
	#3 Channel Risks
	#4 Solutions Use
	#5 Smart Practices
	Recommendations

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).

Online and mobile channels continue to be the primary source of SMB loan origination, with a limited uptick of in-person applications among banks/CUs. This could be a result of post-pandemic resumption of in-person operations.

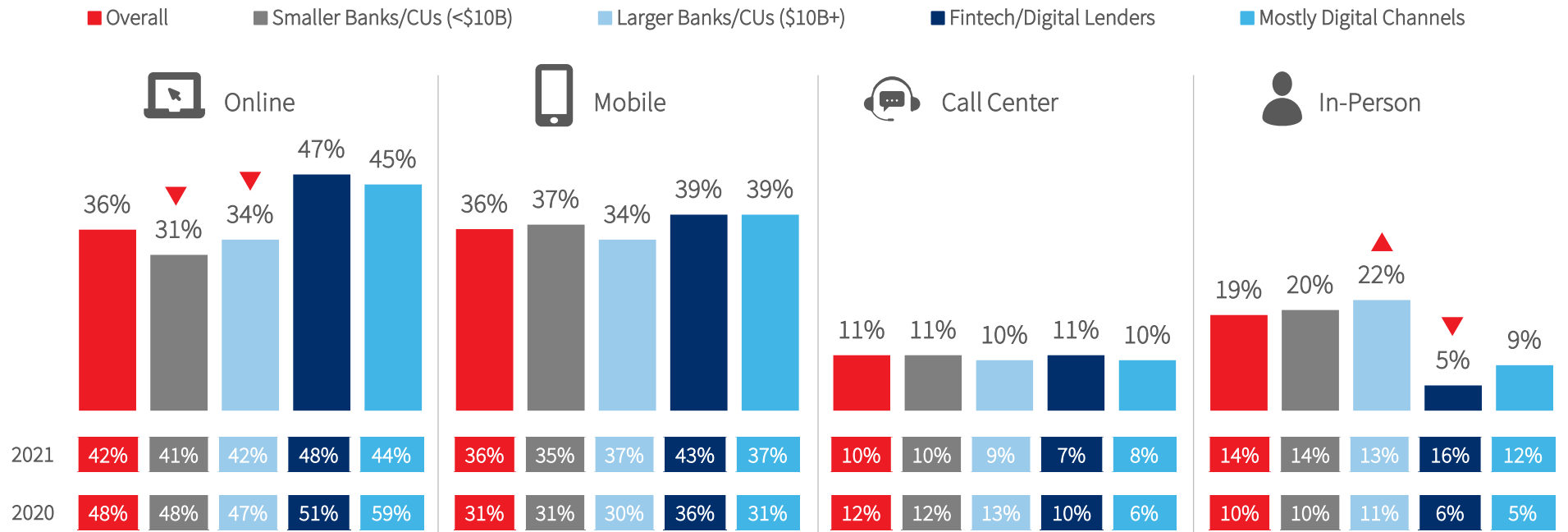


Q8b. Indicate the distribution of total SMB lending fraud costs generated through each of the following channels currently used by your company (as a % of total annual fraud losses).

▲ = significantly or directionally different from 2021, within segment

Relatedly, most SMB lending fraud losses continue to be generated via remote channels, though with a slight increase of in-person losses among banks/CUs.

Distribution of Fraud Losses





Overview



Key Findings



#1 Fraud Trends



#2 Fraud Costs



#3 **Channel Risks**



#4 Solutions Use



#5 Smart Practices

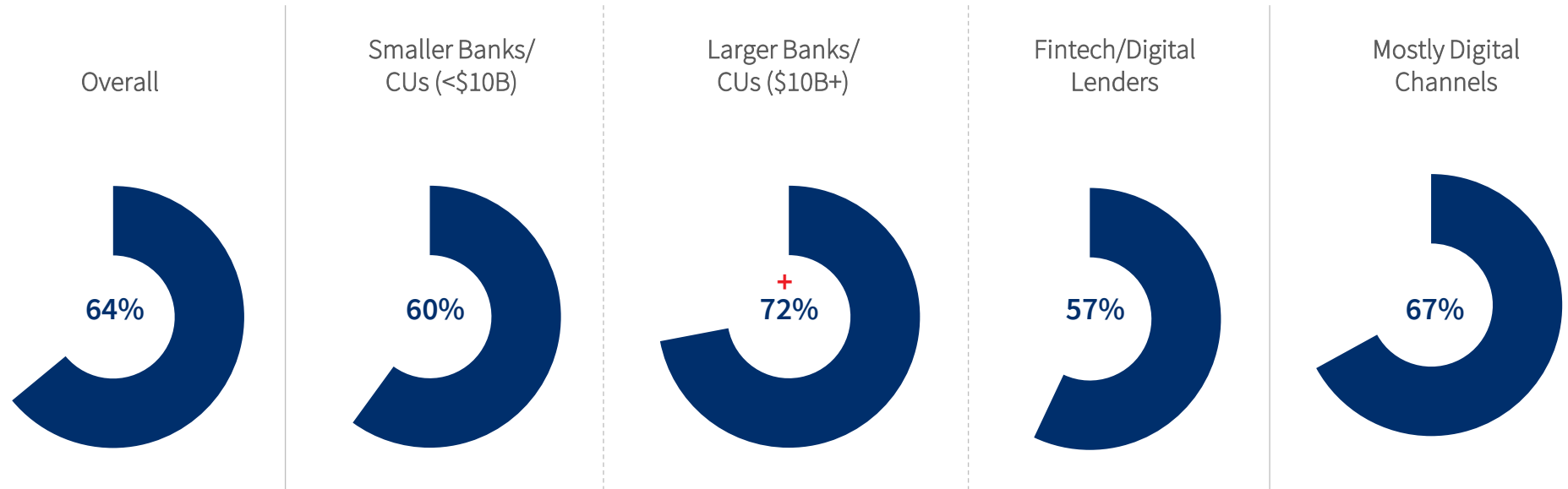


Recommendations

Q20d: Has the post-COVID/new normal made your organization to change its approach to detecting and mitigating SMB lending fraud as more transactions took place through online and mobile channels?

In the post-pandemic market, most lenders, particularly larger banks/CUs, have changed their approach to detecting and mitigating SMB lending fraud with online and mobile transactions.

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



+ = significantly or directionally different from other segments, 2022

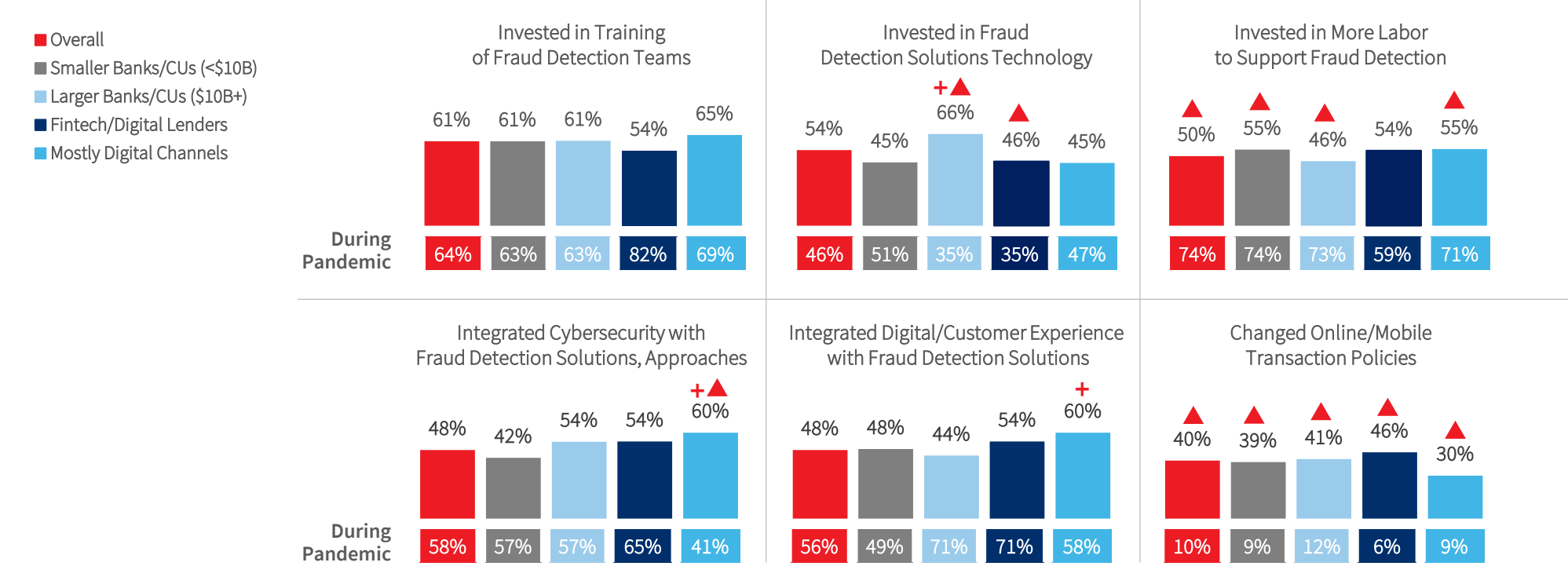
CONFIDENTIAL

Q20e: In what ways did your organization change its approach to detecting and mitigating SMB lending fraud based on the new normal/post-pandemic environment where more transactions are occurring through online and mobile channels?

Significantly more larger banks/Fintechs that have made changes to their approach have included technology in those changes. Over half have also integrated cybersecurity and the customer experience with fraud detection solutions.

The investment in training and labor occur across all segments. In addition, significantly more SMB lenders have changed their online/mobile transaction policies since the pandemic.

Changes in Approach in Post-Pandemic Environment



▼▲ = significantly or directionally different from 2021, within segment
 + = significantly or directionally different from other segments, 2022

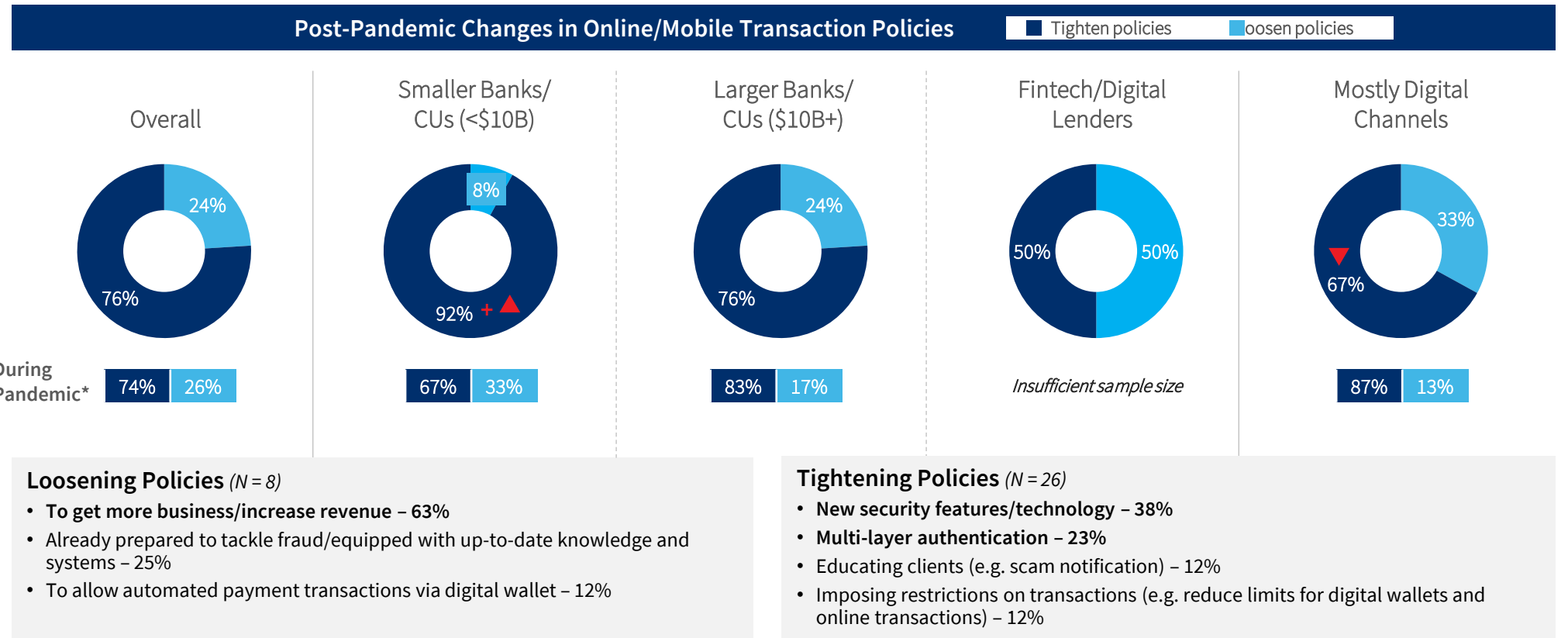
CONFIDENTIAL

Q20f: Which best describes the way that you changed online/mobile transaction policies during the new normal/post-pandemic environment?

*Findings are directional only as overall sample size is extremely small N = 11

As a result, most of the lenders that have made changes in online/mobile transaction policies have decided to tighten them by adding new security features/technology and multi-layer authentication. Some examples given include geolocation, biometrics and SSL protocols.

Lenders that decided to loosen policies have done so primarily to get more business and increase revenue.



Key Findings: Solutions Use



SMB lenders expect that they will continue to invest more in fraud prevention, with smaller banks/CUs, Fintechs and those with mostly digital channels being particularly likely to increase staffing on fraud teams.

Lenders indicate increasing staffing on fraud teams, launching special fraud prevention initiatives and spending more on vendor solutions to curb SMB lending fraud.

And while more SMB lenders indicate use of email and phone risk verification than previous years, the use of digital identity and advanced transaction verification solutions remains limited.

The more common barriers to investing in fraud mitigation solutions include the lack of time to train staff, competing budget priorities and cost of solutions.



Overview



Key Findings



#1 Fraud Trends



#2 Fraud Costs



#3 Channel Risks



#4 Solutions Use



#5 Smart Practices

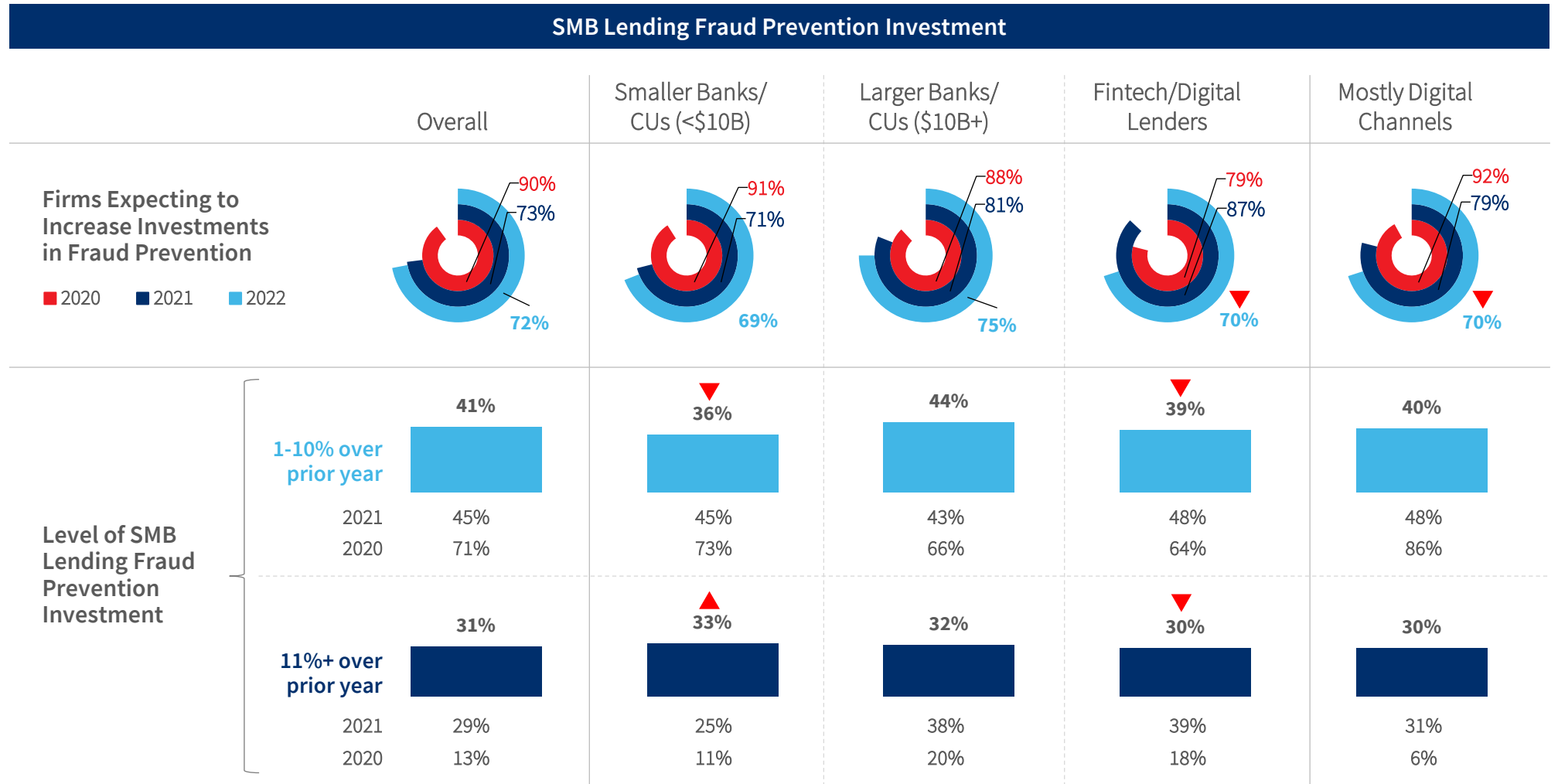


Recommendations

Q14. In 2023, at what level will your company invest to prevent SMB lending fraud from targeting it?

▼▲ = significantly or directionally different from 2021, within segment

A significant majority of SMB lenders expect to increase their investment in fraud prevention resources.

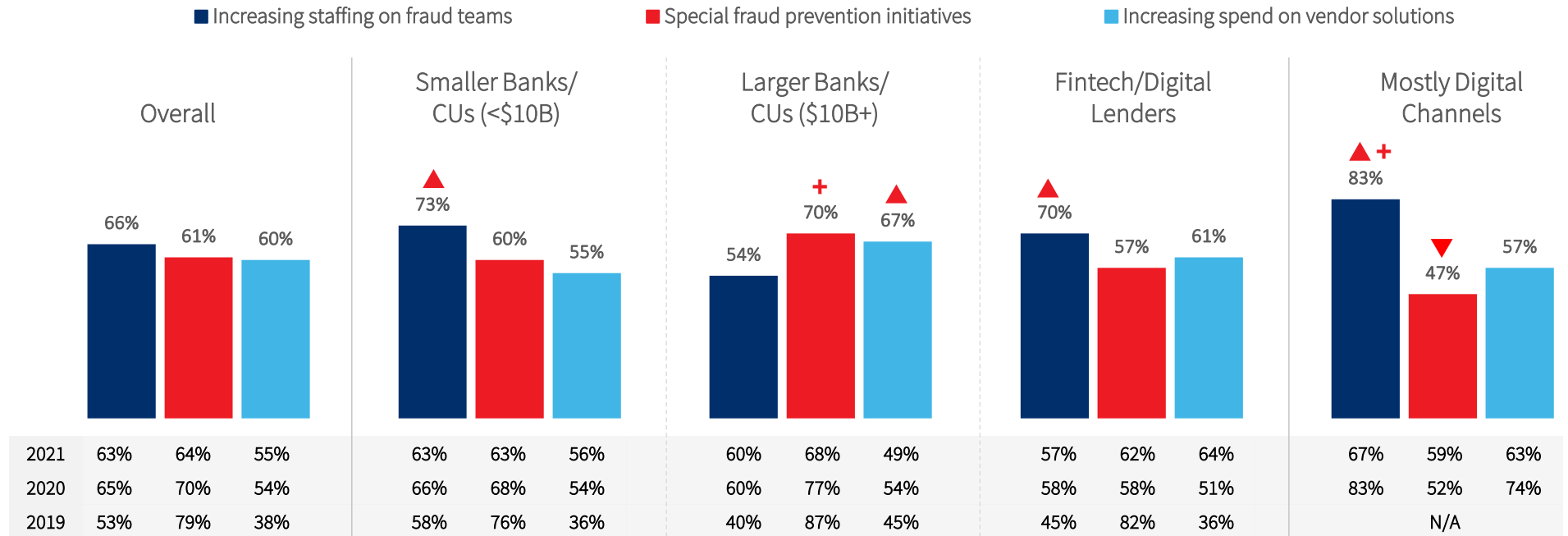


Q15. What internal activities is your company taking to curb SMB lending fraud from targeting your company?

Lenders are increasing staffing on fraud teams, launching special fraud prevention initiatives and spending more on vendor solutions to curb SMB lending fraud.

Smaller banks/CUs, Fintechs and those with mostly digital channels particularly prefer hiring more people on their fraud teams. Compared to 2021, larger banks/CUs are more likely to invest more in vendor solutions.

Activities Being Undertaken to Curb SMB Lending Fraud

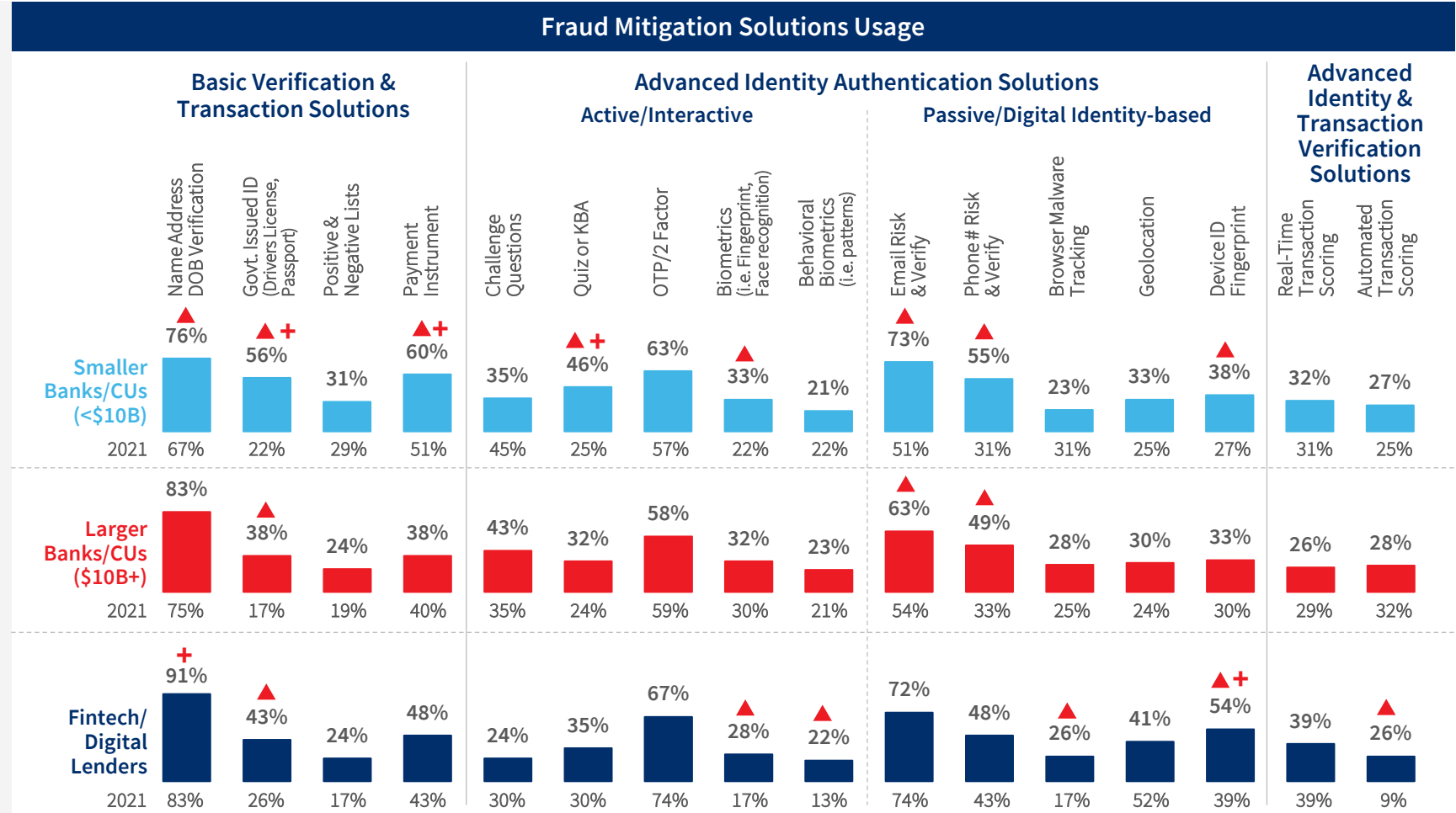


▲ = significantly or directionally different from 2021, within segment
 + = significantly or directionally different from other segments, 2022

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

In comparison to 2021, more SMB lenders indicate use of email and phone risk verification, as well as some uptick with device ID/fingerprint. However, the use of digital identity and advanced transaction verification solutions remain limited.

Digital identity verification solutions are designed to address unique threats from online and mobile channel transactions, such as distinguishing between legitimate and synthetic identities as well as identifying botnets. Further, few are using a multi-layered solutions approach that identifies fraud threats across different types of channels and transactions.



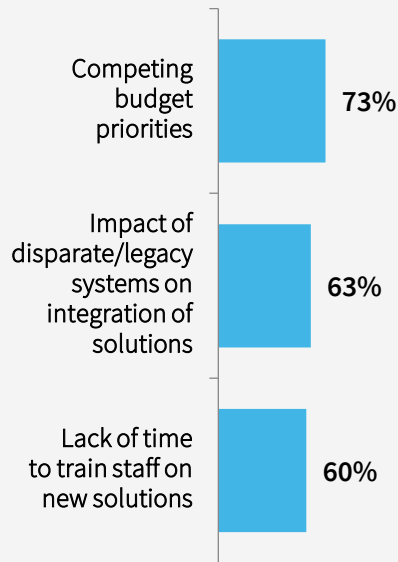
Q22. Which of the following, if any, have been barriers to investing in fraud prevention solutions for SMB lending fraud?

▲ = significantly or directionally different from 2021, within segment

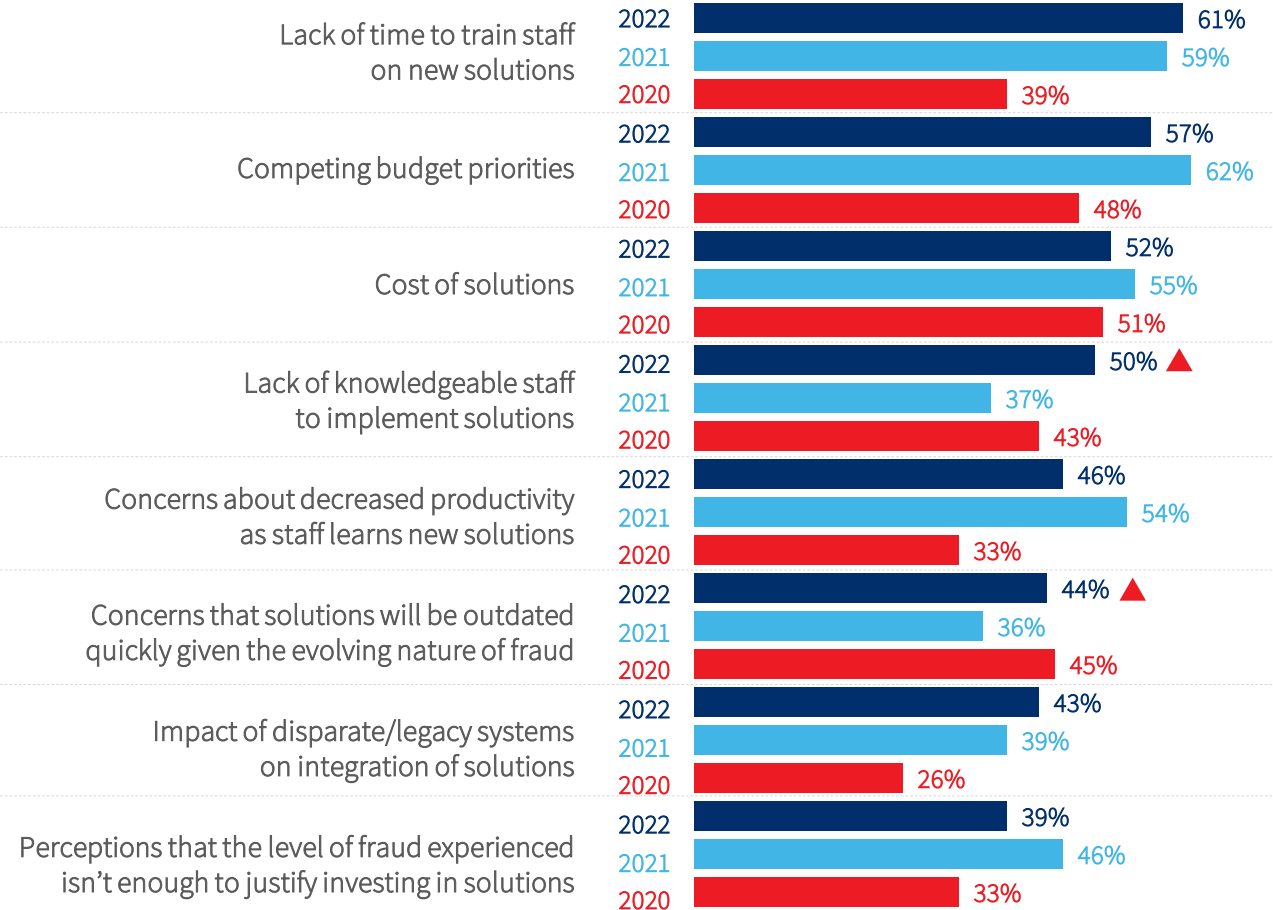
The more common challenges to investing in fraud mitigation solutions include the lack of time to train staff, competing budget priorities and cost of solutions.

Lenders with mostly digital channels are also particularly likely to experience barriers arising from the impact of disparate/legacy systems on integration of solutions.

Mostly Digital Channels



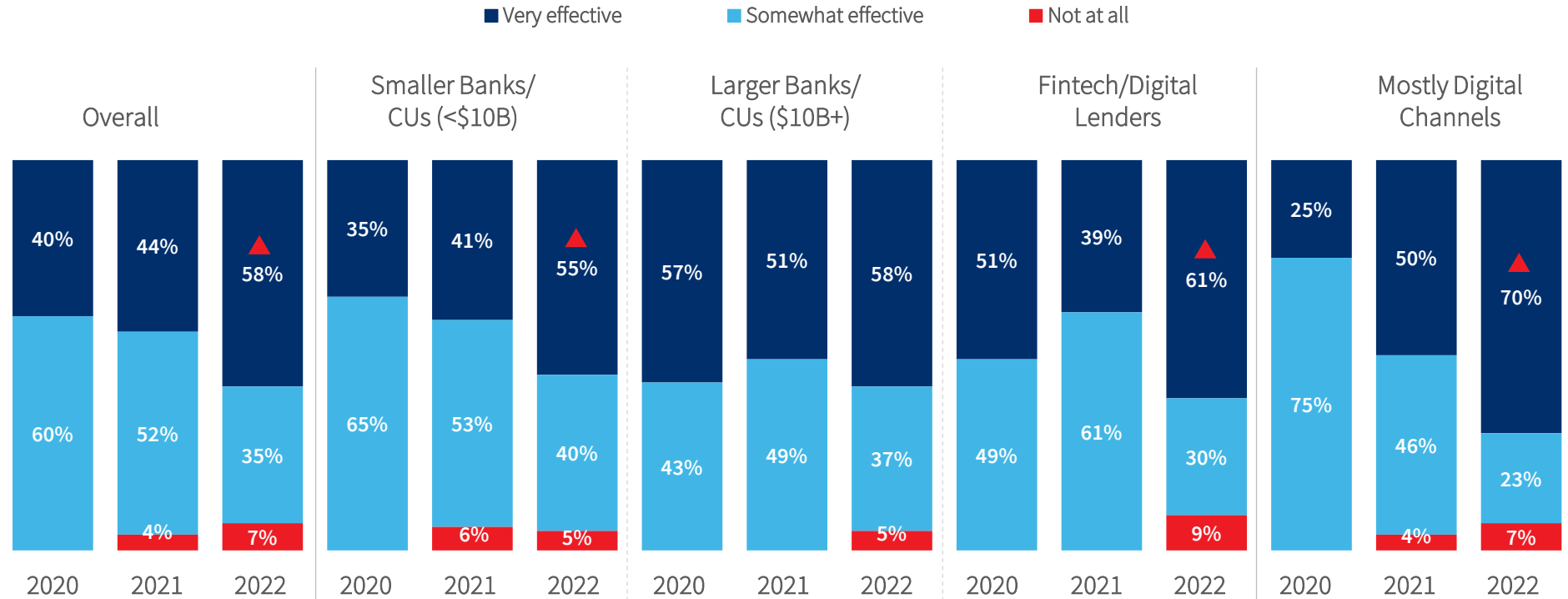
Barriers to Investing in Fraud Mitigation Solutions



Q4A. How effective do you think your company is at identifying small and midsize business (SMB) lending fraud targeting your company?

However, more SMB lenders are perceiving their organizations as being very effective at identifying fraud targeting their companies.

Effectiveness at Identifying SMB Lending Fraud



▲ = significantly or directionally different from 2021, within segment

Key Findings: Smart Practices



Study findings show that lenders which use a multi-layered solutions approach that integrates with cybersecurity and the digital channel operations can be more effective at detecting and mitigating fraud and its costs early.

This also includes solutions that assess both the physical and digital identity attributes, as well as the risk of the transaction itself.

Findings show that firms following this smart practice can achieve a lower percentage of fraud costs to annual revenues by being more effective at detecting fraud at the point of origination.

	Overview
	Key Findings
	Fraud Trends
	Fraud Costs
	Channel Risks
	Solutions Use
	Smart Practices
	Recommendations

	Overview
	Key Findings
	#1 Fraud Trends
	#2 Fraud Costs
	#3 Channel Risks
	#4 Solutions Use
	#5 Smart Practices
	Recommendations

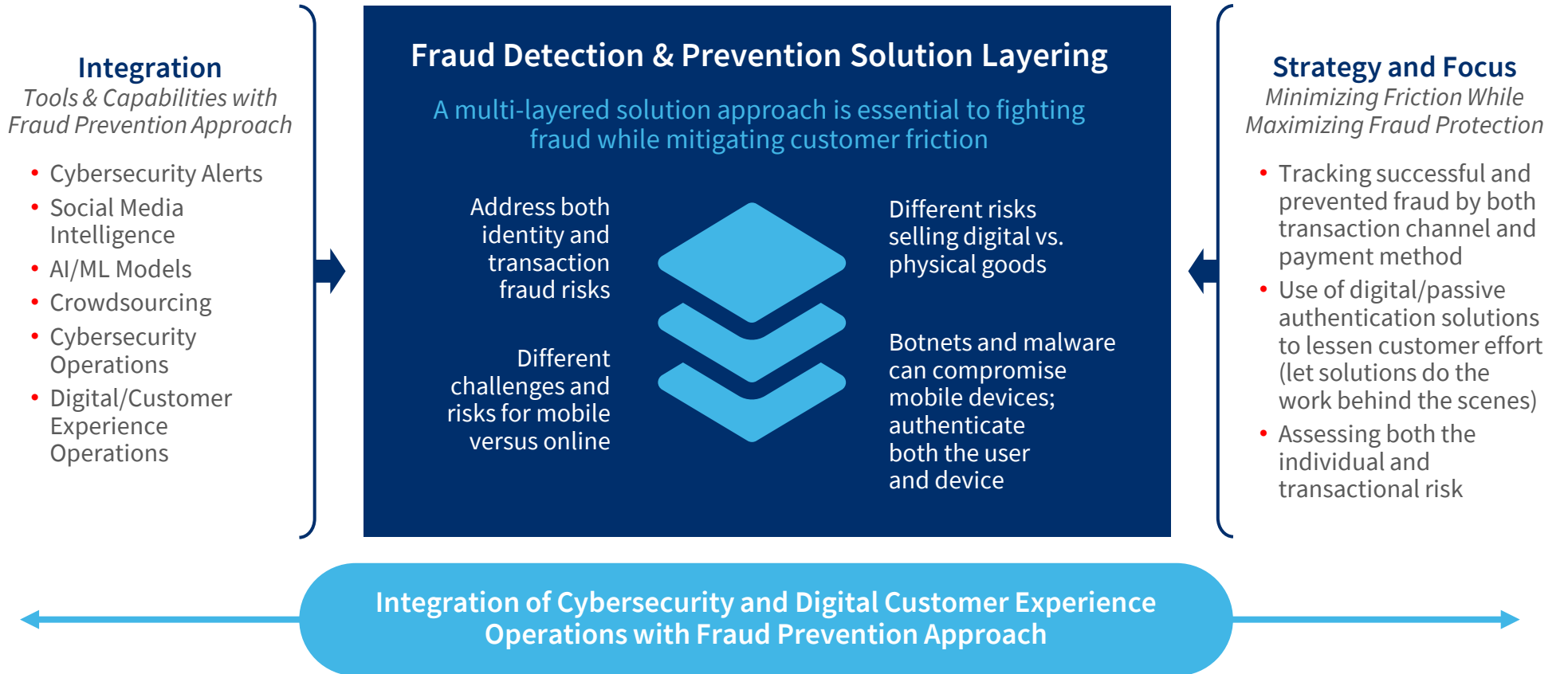
Fraud has become more complex; various risks can occur at the same time with no single solution. Fraud tools need to authenticate both digital and physical criteria, as well as both identity and transaction risk.









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: 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/two-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.	

	Overview
	Key Findings
	#1 Fraud Trends
	#2 Fraud Costs
	#3 Channel Risks
	#4 Solutions Use
	#5 Smart Practices
	Recommendations

Smart practice fraud detection and mitigation involves a layering of different solutions to address unique risks from different channels, payment methods and products. And it goes farther by integrating cybersecurity and digital channel operations with fraud prevention efforts.











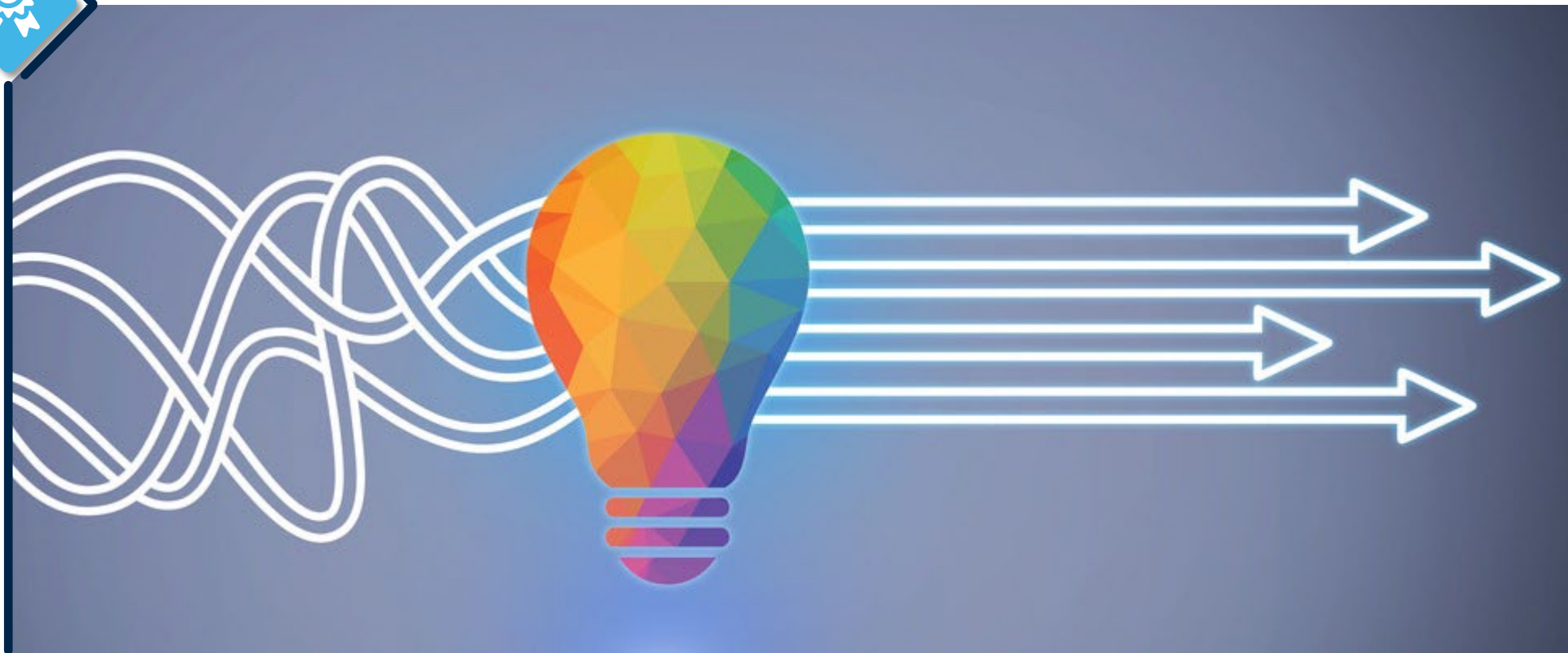
-  Overview
-  Key Findings
-  #1 Fraud Trends
-  #2 Fraud Costs
-  #3 Channel Risks
-  #4 Solutions Use
-  #5 **Smart Practices**
-  Recommendations

Study findings show that SMB lenders using a smart practice approach of multi-layered solutions that includes integration with cybersecurity/digital channel operations can be more effective at detecting fraud early and experience a lower cost of fraud impact on revenues.

Smart Practice Use of a Multi-layered Solutions Approach Including Integration with Cybersecurity and Digital Channel Operations		No	Yes
Fraud cost as a % of annual revenues		5.6%	4.3%
% that catch SMB lending fraud at the point of origination		18%	50%
% very effective at detecting and mitigating SMB lending fraud		36%	85%
% of SMB lending fraud attributed to COVID impacts		60%	40%
<p>Layers of Protection</p> <p>Common Core Solutions Authenticate using payment instrument, name/address/DOB verification, positive and negative lists, government-issued ID</p> <p>Advanced ID Authentication Solutions Challenge questions/quiz, OTP/2-factor, biometrics, behavioral biometrics, email risk and verification, phone # risk and verification, browser/malware tracking, geolocation, device ID</p> <p>Advanced ID and Transaction Verification Solutions Automated transaction scoring, real-time transaction scoring</p>		<p>Limited</p> <p>Many</p> <p>Minimal</p> <p>Minimal</p>	<p>Multi-layered with Digital Identity</p> <p>✓</p> <p>✓</p> <p>✓</p>
Average # advanced solutions used		4	11

Recommendations

	Overview
	Key Findings
	#1 Fraud Trends
	#2 Fraud Costs
	#3 Channel Risks
	#4 Solutions Use
	#5 Smart Practices
	Recommendations











Recommendation #1: Assess Digital Identity Attributes



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

- Identity proofing involves both verification and authentication. **Verification** relates to self-provided data (date of birth, national ID number, address, etc.) to determine if the person/identity is real and that the data relates to a single identity; this is particularly important with the rise of synthetic identity fraud. **Authentication** is about confirming that the person is legitimate (who they say they are).
- To minimize fraud, organizations can no longer rely on manual processes with the assistance of limited technologies to reduce challenge rates, manual reviews and costs.
- The digital transformation among consumers to more online and mobile transactions means that more of these transactions are occurring in an anonymous environment compared to traditional in-person interactions. Businesses need to also assess the device risk, as well as the online/mobile behaviors and transaction risk. Assessing only the physical identity attributes (name, address, date of birth, Social Security Number, etc.) will not help businesses authenticate the identity.
- Businesses need a robust fraud and security technology platform that helps them adapt to this changing digital environment, offering strong fraud management and resulting in reduced friction for genuine customers.
- Deploying technologies that are able to recognize legitimate customers, mitigate fraud and build the fraud knowledge base to streamline on-boarding can prevent account takeovers and detect insider threats.
- Using valuable data attributes like users' login from multiple devices, locations and channels is essential for identifying risks.
- Enabling integrated forensics, case management and business intelligence can help to improve productivity.

	Overview
	Key Findings
	Fraud Trends
	Fraud Costs
	Channel Risks
	Solutions Use
	Smart Practices
	Recommendations

	Overview
	Key Findings
	#1 Fraud Trends
	#2 Fraud Costs
	#3 Channel Risks
	#4 Solutions Use
	#5 Smart Practices
	Recommendations

Recommendation #2: Multi-Layered Solution Approach



A multi-layered solution approach is required — customized to each phase of the customer journey and transaction channel.

- Single point protection is inadequate and results in single point of failure
- As consumers transact across locations, devices and geographies, user behaviors, such as transaction patterns, payment amounts and payment beneficiaries are becoming more varied and less predictable.
- Further, each stage of the customer journey is a unique interaction, requiring different types of identity verification, data and solutions to let your customers in and keep the fraudsters out.
- We recommend adopting a multi-layered, strong authentication defense approach. This includes a single authentication decision platform that incorporates real-time event data, third-party signals and global, cross-channel intelligence.

Recommendation #3: Protect Endpoints



Mitigate fraud at the first point of the customer journey by protecting endpoints and using digital identity solutions and behavioral analytics that assess risk while minimizing friction.

- New account opening is the customer journey point where fraudsters can become established, causing problems at later stages. It is also the first point of contact for many legitimate customers; too much friction and they may abandon the effort.
- Use technologies that recognize your customers, determine their point of access and distinguish them from fraudsters and malicious bots. Layered solutions empower your organization to apply more or less fraud assessment in order to optimize this with the customer experience.
- Add transaction risk technology to the layering of digital attributes, behavioral analytics and device assessment solutions during the transaction/distribution of funds journey point.

	Overview
	Key Findings
	Fraud Trends
	Fraud Costs
	Channel Risks
	Solutions Use
	Smart Practices
	Recommendations



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.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Other products and services may be trademarks or registered trademarks of their respective companies.
Copyright © 2023 LexisNexis Risk Solutions Group. NXR15786-00-0123-EN-US

CONFIDENTIAL