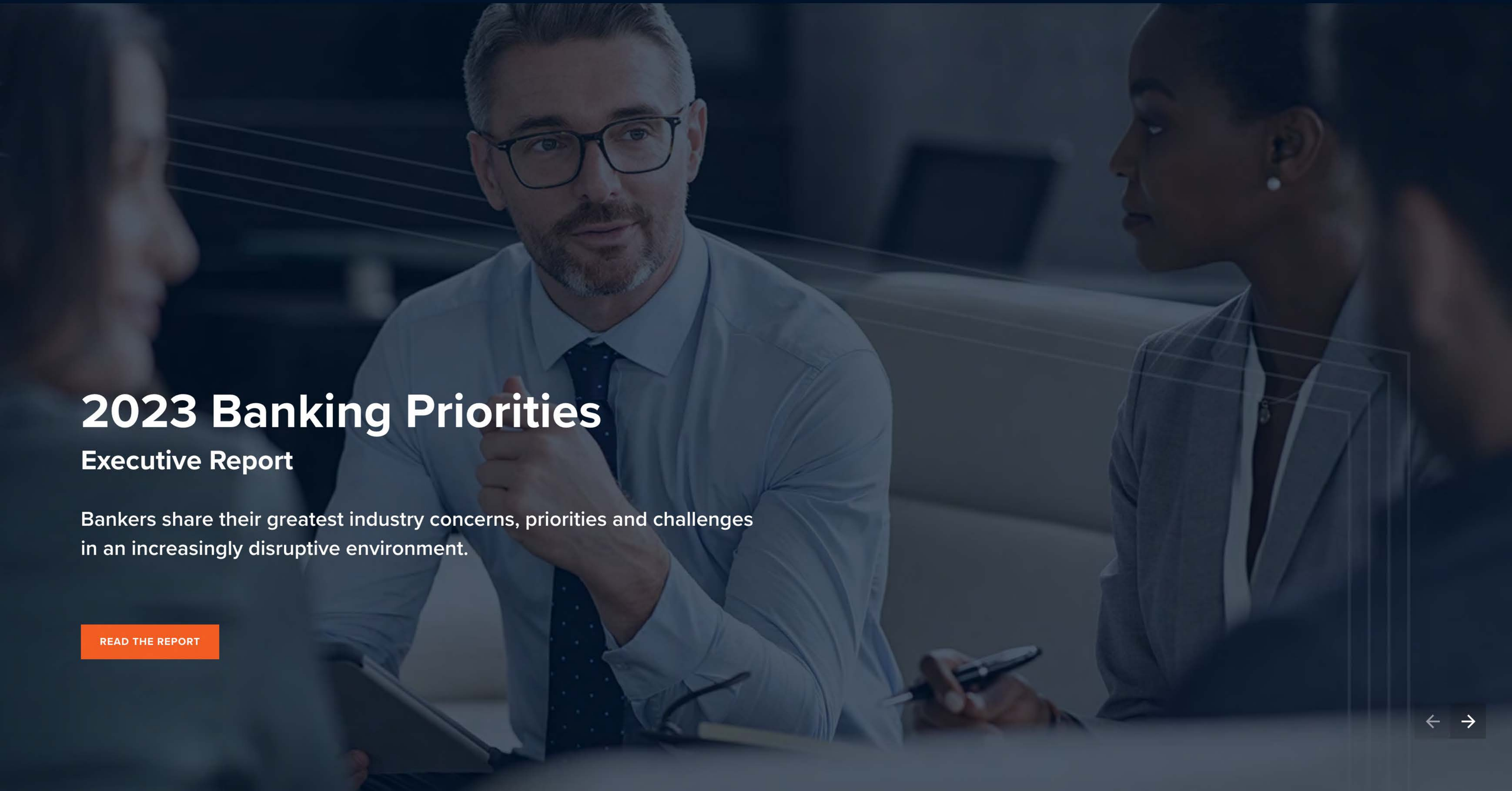


2023 Banking Priorities

Executive Report

Bankers share their greatest industry concerns, priorities and challenges in an increasingly disruptive environment.

READ THE REPORT

Contents

03
Introduction to the 2023 Report

04
An Aerial View of the Landscape

05
The Banking Forecast at a Glance

06
Industry Voices: Bankers Discuss Head and Tail Winds

07
Leading Technology Initiatives

08
Modern Banking: Emerging Technologies Energize the Atmosphere

09
Cybersecurity: Active Threats Persist on the Horizon

10
Regulatory Compliance: Requirements Continue to Flood the Landscape

11
Finding Calm in a Disruptive Atmosphere

12
Appendix

13
Resources

2023 Forecast

Increasingly Cloud-Based with a Chance of Disruption

We invite you to click through our interactive report to explore what bankers said, coupled with analysis from CSI's Fintexperts and pointers for financial institutions' success throughout 2023. All percentages are rounded to the nearest full percent.

As the United States embraced the "new normal" of 2022, the financial services industry saw continued innovation and disruption. Consumers expect the latest financial technologies, making digital banking and flexibility table stakes. Meanwhile, the rise of open banking, cloud services, enhanced cybersecurity and new regulatory concerns broaden the areas of focus financial institutions must consider. But these complications also represent a tremendous opportunity for those that adapt.

This year's *Banking Priorities Survey* reflected both familiar challenges and emerging opportunities while revealing the strategies community institutions are deploying to stay competitive. While those strategies vary as much as each organization's unique business needs, they also indicate a common theme. Institutions see an imperative to continue digital evolution and strengthen their most distinct competitive advantage—customer relationships.

"In the current environment, community banks are faced with a change or perish moment that is becoming crystal clear to all of us."

Source: Survey Participant

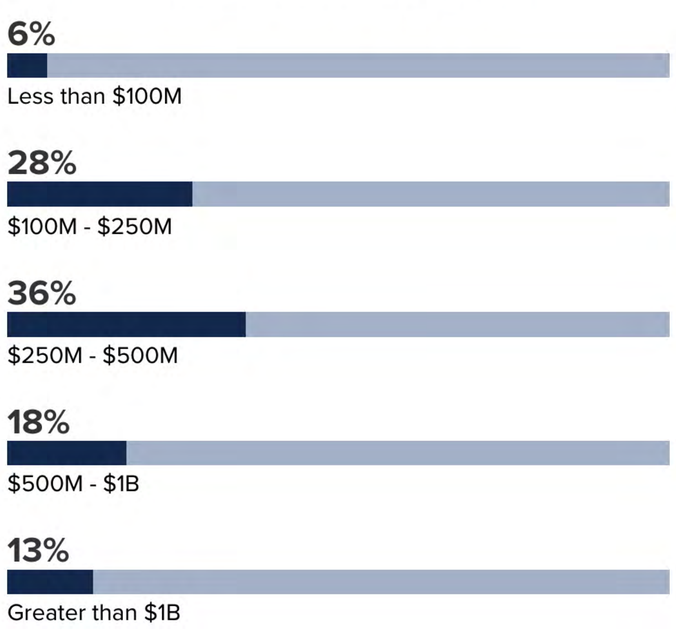
About CSI's 2023 Banking Priorities Survey

Every year, CSI surveys financial institutions across the country to gauge their confidence, strategies to gain market share and priorities for the year to come. This annual research initiative aims to inform bankers of their peers' approaches to staying competitive and equip them with expert guidance.

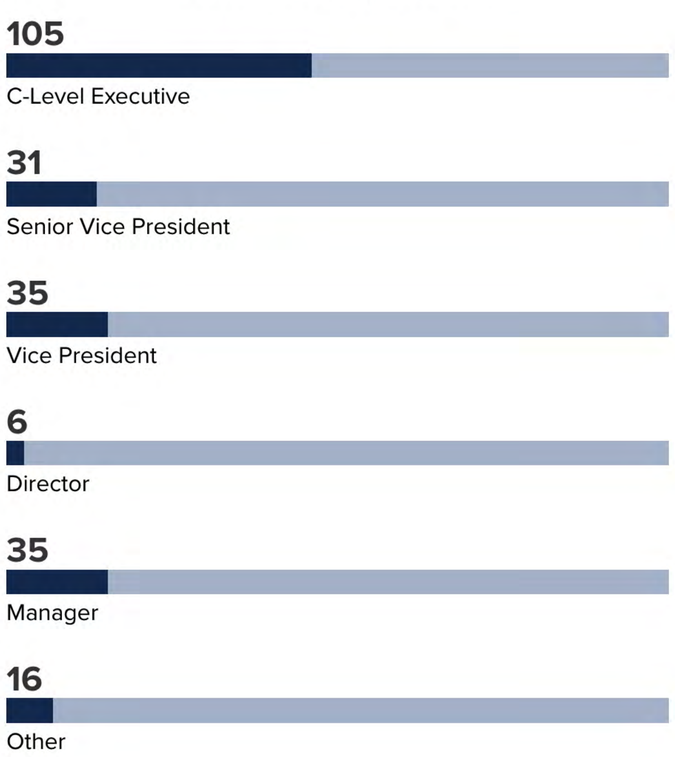
As with previous years, the eighth annual Banking Priorities survey asked bank representatives to take stock of their performance across various categories and select the technologies they expect to drive the financial sector in 2023. This year's research also incorporates new elements, including questions surrounding emergent technologies as well as quotes from respondents.

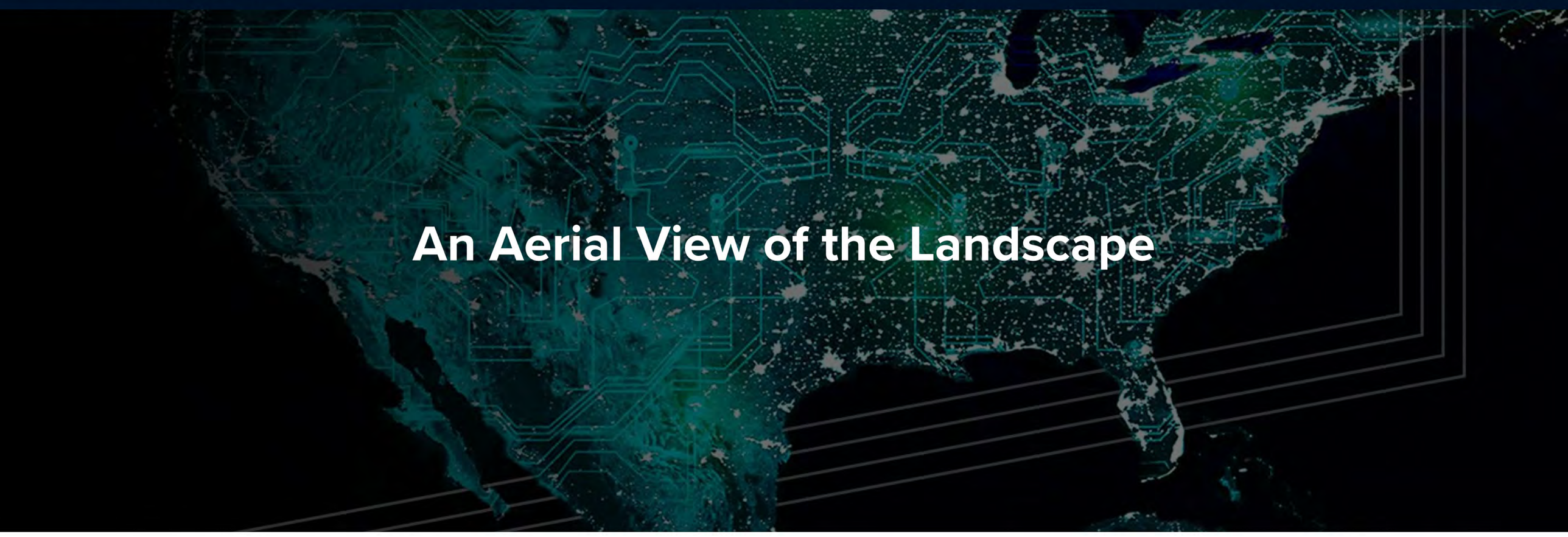
Community bankers, representing the backbone of the traditional U.S. banking system, made up the bulk of the 228 responses, with asset sizes and roles distributed as follows:

Institution Asset Size



Role of Respondent





An Aerial View of the Landscape

The results of CSI's annual Banking Priorities survey reveal that the established financial services industry is still working to fully leverage the growth opportunities of the digital age. A broad cross-section of bankers shared their thoughts after a year in which high employee churn persisted,[1] and deposits at challenger banks continued to grow.[2] These disruptions were set against a backdrop of ever-present cybersecurity threats[3] and costly regulatory enforcement actions.[4]

Banker Concerns Track with Industry Trends

732,000

Employee Churn

732,000 employees quit jobs in the financial services sector between May and September 2022.

Source: Bureau of Labor Statistics

46.4%+

New Competition

Though slowing, the number of U.S. neobank account holders is expected to grow 46.4% by 2026.

Source: Insider Intelligence

$220M

Enforcement Actions

The Consumer Financial Protection Bureau (CFPB) alone issued over $220 million in civil money penalties in 2022, almost all exclusively related to Unfair, Deceptive or Abusive Acts and Practices (UDAAP).

Source: CFPB Enforcement Actions

$5.97M

Cybersecurity Challenges

The 2022 average cost of a data breach in financial services is $5.97 million, second only to healthcare.

Source: IBM Cost of a Data Breach Report 2022

For the first time, the annual survey included an open-ended question asking bankers what else they would like to share. Bankers participating in the survey provided frank commentary on the new challenges of the "new normal." They also discussed familiar ones as they identified their plans.

The participants' revealing quotes appear throughout this report, along with their perspectives on the following issues:

- The current and future state of their institutions' performance and strategy
- The technologies they're already using and those they plan to explore
- Their assessment of cybersecurity threats compared to their defenses
- Their challenges meeting existing regulatory obligations and preparedness for those that are impending

Beyond sharing the perspective of surveyed bankers, this year's executive report presents an environmental analysis of their responses by CSI industry experts. In addition, it provides insight into undercurrents in the present climate that deserve a bit more attention.

The Banking Forecast at a Glance

The 2023 survey forecasts ongoing turbulence in key areas, while highlighting potential stabilizing forces.

The Voices of the Industry

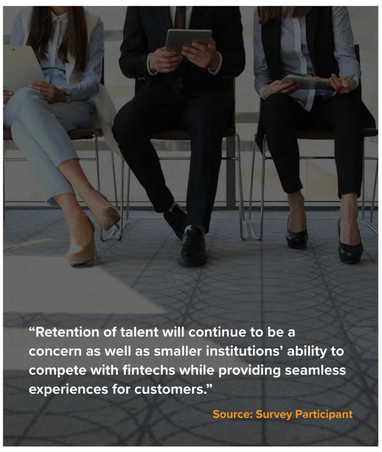
Over 60% of respondents view employee churn (34%) or regulatory change (27%) as the most significant issue expected to affect the industry in 2023.

Despite such challenges, 88% of respondents feel highly confident in their ability to retain their customers. Their top three strategies for increasing market share revolve around continued digital transformation and utilizing data.

Most significant issue expected to affect the industry

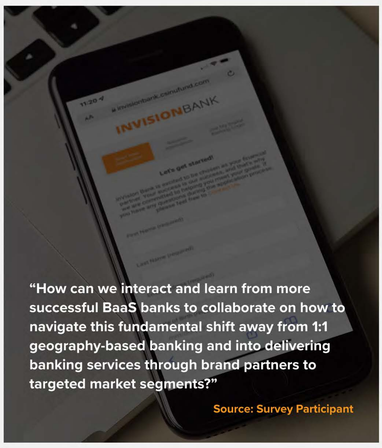
34%
Employee Churn

27%
Regulatory Change



"Retention of talent will continue to be a concern as well as smaller institutions' ability to compete with fintechs while providing seamless experiences for customers."

Source: Survey Participant



"How can we interact and learn from more successful BaaS banks to collaborate on how to navigate this fundamental shift away from 1:1 geography-based banking and into delivering banking services through brand partners to targeted market segments?"

Source: Survey Participant

The Digital Keys to Modern Banking

Bankers plan to prioritize technologies that enhance the customer experience, such as digital account opening (55%) and digital lending (41%).

However, bankers have lingering questions about critical aspects of modern technology, including APIs, Banking as a Service (BaaS) and the public cloud. This year's data suggests a need to better understand these concepts to fully benefit from the digital age.

Technologies bankers plan to prioritize to enhance the customer experience

55%
Digital Account Opening

41%
Digital Lending

The Persistent Cybersecurity Threat

P2P fraud topped respondents' cybersecurity concerns, followed by data breaches and ransomware.

Even so, 77% of bankers claim they clearly understand their cyber risk, and 80% say their institution knows how to respond to a cyber incident within their walls.

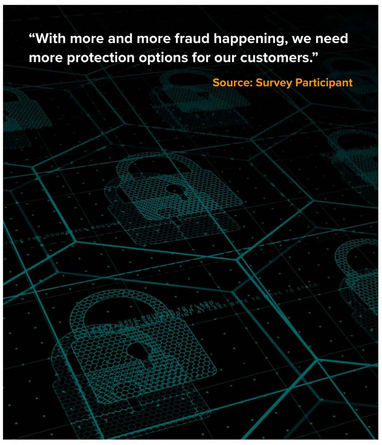
Bankers' top cybersecurity concerns

29%
P2P or Other Digital Fraud

23%
Data Breach/Disclosure

"With more and more fraud happening, we need more protection options for our customers."

Source: Survey Participant



"Increased regulation and negative pressure on earned fees could not come at a worse time for community banks."

Source: Survey Participant

The Challenging Regulatory Environment

As for compliance obligations, Unfair, Deceptive or Abusive Acts and Practices (UDAAP), cybersecurity and Bank Secrecy Act (BSA) modernization are taking up the most banker headspace, while fraud is viewed overwhelmingly as their most concerning compliance risk.

Industry Voices

Bankers Discuss Head and Tail Winds

According to Banking Strategist, those with less than $10 billion in total assets comprise 97% of traditional banks.[5]

Survey representatives from this overwhelming majority help identify how traditional bankers view the current digital environment. In their responses, they reveal the forces pushing against them and those that will drive them forward.

Predictions about Upcoming Industry Challenges

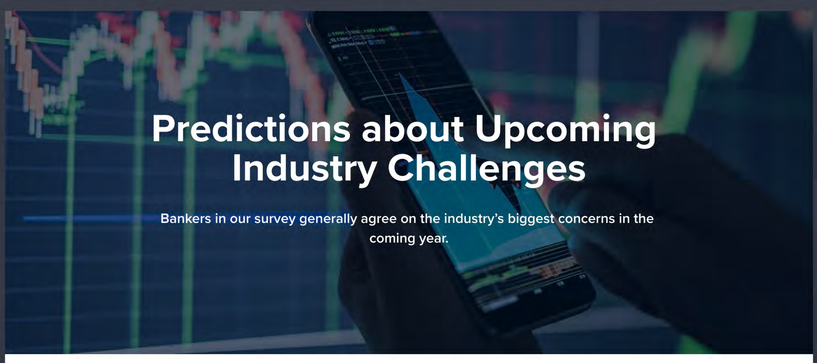
READ MORE

Ground Assessment of Current Institutional Performance

READ MORE

Prevailing Strategies for Gaining Market Share

READ MORE

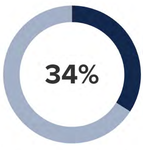


Predictions about Upcoming Industry Challenges

Bankers in our survey generally agree on the industry's biggest concerns in the coming year.

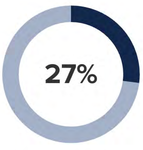
Forecasting the Most Impactful Industry Issues for 2023

Over 75% of bankers chose one of three issues expected to have the greatest influence in 2023:



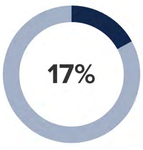
Recruiting/Retaining Employees

Over one-third (34%) of bankers described this as the biggest issue in the coming year, rising from 21% going into 2022.



Regulatory Change

Over one-quarter (27%) viewed impending changes to banking regulations as the most pressing issue.



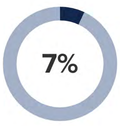
APIs/Open Banking

This issue rounded out the top three, receiving 17% of the vote.

"APIs and data analytics are the two most important things for our institution from an IT standpoint next year."

Source: Survey Participant

Less than 10% of the respondents selected the remaining options as one of the top three most impactful issues:



BaaS

Just 7% of bankers selected Banking as a Service, but the low response can be misleading, as this model overlaps with APIs and Open Banking.

Other

At 6%, almost all write-in options focused on economic concerns, such as rising inflation, a possible recession and interest rates.

Mergers/Acquisitions

Like last year, bankers do not anticipate consolidation in the market to cause much of an immediate impact, only garnering 5% of the vote.

Cryptocurrencies

Only 4% expect digital assets to make a significant splash in 2023.

Environmental Analysis

With the Great Resignation still rippling through the employment market, it's no surprise that respondents identified employee recruitment and retention as their biggest concern. "Banking has and always will be about people servicing people. Institutional leaders realize this, which is why this concern tops all others, including technology," explains Steven Ward, manager of CSI Advisory Services.

Largely instigated by the COVID-19 pandemic and the rise of remote work, the challenge is far from limited to the financial sector. The U.S. Bureau of Labor Statistics estimated that four million voluntary resignations occurred in October 2022 alone, continuing the high rate established in late 2020.[1] 2022 was also rife with layoffs in the technology sector, causing massive shifts in the workplace.

The outflow of workers from the service and tech industries, paired with growing interest from young applicants, creates an opening to attract customer-oriented and tech-savvy talent. To do so, many financial institutions are focusing on improving the employee experience, upping their compensation package game and even offering remote or hybrid work.

Depending upon their success in outreach and budget, institutions can also consider automating or outsourcing certain tasks and roles. Some banks are already turning to outsourced customer service models or outsourcing IT experts to lighten the load.

Advisory Insight

Industry experts agree that APIs demand more attention from bankers. Notably, the way this advanced technology integrates systems and aggregates information can streamline front- and back-end operations. Additionally, there is an opportunity to build in some intelligence and leverage robotic process automation (RPA), especially for repetitive tasks. Systems can now accommodate a relatively sophisticated level of decisioning and routing of information and processes. Along with adding the adaptability to incorporate new technologies, RPAs used well can also blunt the effects of staffing shortages and changing regulations. They likewise undergird the BaaS model, enabling financial institutions to introduce new digital products and services to access new markets or revenue streams.

RETURN TO MAIN SECTION

Ground Assessment of Current Institutional Performance

As stated by the Federal Reserve, "Community bankers are committed to meeting the diverse needs of their respective communities."[6] By their own account, bankers in our survey continue to achieve that mission with their current customers.

Rating Institutional Performance on a Scale of 1 - 5, with 5 Being the Highest

Over 75% of bankers gave themselves the highest marks in these three areas, which repeated their rank order from last year:

Retaining Current Customers

4.1/5 for the third year in a row

4.1/5

Compliance Readiness

3.9/5, continuing a downward trend from 2022 (4.0/5) and 2021 (4.1/5)

3.9/5

Cybersecurity Readiness

3.9/5, an increase over last year (3.8/5)

3.9/5

In all other categories, except the last, their performance was slightly above average:

In-branch Experience

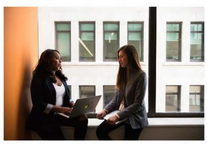
Consistent with the last two years, bankers scored themselves 3.6/5

3.6/5

Attracting New Customers

A score of 3.4/5, an improvement over the average responses leading into 2022 (3.3/5)

3.4/5



Retaining Talent/Acquiring Talent

A score of 3.1/5

3.1/5

Digital Transformation

A score of 3.3/5, the same as in the 2022 report, but less than in the 2021 report (3.5/5)

3.3/5

Collecting/Utilizing Customer Data

At 2.6/5, a lower score than last year (2.7/5) or the year before (2.8/5)

2.6/5

Environmental Analysis

Despite the disruptions around them, four out of five bankers continue to express high confidence in their ability to retain customers. This should help stave off competition from non-collaborative megabanks, neobanks (established online fintechs that offer specialized financial products) and other non-bank entities that may be targeting community bank customers.

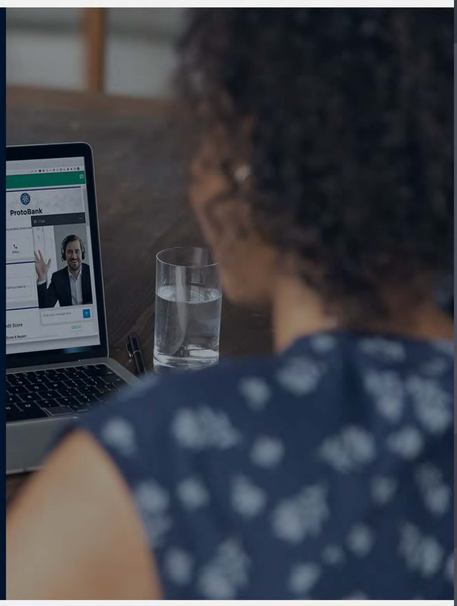
4/5

4 out of 5 bankers continue to express high confidence in their ability to retain customers

Advisory Insight

At a high level, an institution's success at retaining and acquiring talent can directly affect its ability to retain current customers and attract new ones. Right-channeling, or routing customers to the channel and people most likely to provide the appropriate service, supports both. This customer-service approach facilitates customer self-service in the channel of their choice. This reduces the number of requests to be fielded by employees in branches or call centers—areas that typically experience the highest staff churn. It could also include technologies like skills-based routing to save employees and customers time.

Proper channeling also allows interaction to progress as needed to meet more nuanced customer needs. For example, a customer may initially interact with a chatbot via their institution's mobile app to find out what kind of certificates of deposit are available. But if they have more detailed questions, they can progress to a video chat with a live person via their preferred device.



"Right channeling can help institutions make up the difference when staffing is an issue."

Scott Hess, Head of Digital Banking and Strategy at CSI

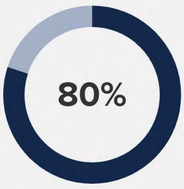
RETURN TO MAIN SECTION

Prevailing Strategies for Gaining Market Share

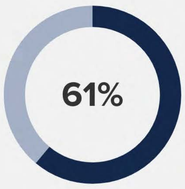
According to Insider Intelligence, traditional financial institutions can expect as many as 41.8 million people in the U.S. to have at least one account with a neobank in 2023. That number is projected to rise to 47.8 million in 2024 and 53.7 million by 2025.[2] These projections underscore the need for traditional financial institutions to adopt effective strategies for maintaining and increasing their market share.

Identifying the Top Three Strategies for Increasing Market Share

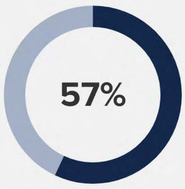
In 2023, bankers will continue to focus on the same three strategies to expand their reach as they did in 2021 and 2022. Each relates to digital transformation:



The vast majority of bankers (80%) will enhance or optimize their current digital channels



Well over half (61%) will invest in new digital technologies



And 57% will utilize customer data

It should also be noted that 45% will enhance branch technology, while 22% will focus their efforts on BaaS and 17% will pursue mergers and acquisitions.

Environmental Analysis

The bankers in our survey recognize the importance of continued digital transformation and a successful partnership with a core technology vendor. "They all realize the digital world is where they can attract additional customers in new markets," notes Steve Sanders, CSI's Chief Information Security Officer (CISO). To improve the success of market share strategies, he recommends that institutions set clear objectives about what they want to achieve over the next 12 to 24 months.

"According to Bankers Helping Bankers, BaaS banks are drastically more profitable than traditional branch-focused banks."

Source: Survey Participant

Advisory Insight

Utilizing customer data to better understand and fulfill account holder needs in real-time is an integral part of any digital banking strategy. It's equally important to understand the data privacy issues related to using customer data.

While targeting markets beyond traditional geographic footprints, financial institutions need to identify and follow the data privacy regulations in all states where their customers reside. For example, some regulations like the Illinois Biometrics Information Privacy Act require written customer releases to use biometric information.[7]

"As institutions continue to figure out how to use customer data to support digital strategies, they also need to factor in the legal implications of that."

Steve Sanders, CISO at CSI

RETURN TO MAIN SECTION

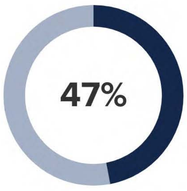
Leading Technology Initiatives

Financial institutions must make smart choices about where to use their limited technology resources. This will ensure they meet the demands of a population that collectively grows more tech-savvy by the minute. This year's survey reveals where respondents plan to deploy these valuable dollars.

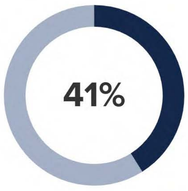
Determining the Top Three Technologies Institutions Will Prioritize

Heading into 2023, more bankers plan to focus on the following technologies than any others:

As with the last two years, digital account opening remains the top technology priority at 55%.

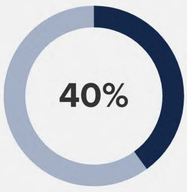


Data analytics and reporting is a bigger priority this year at 47% versus 29% last year.

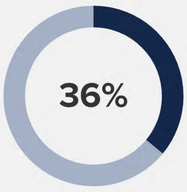


Digital lending is favored by 41%, maintaining its number three spot for the third year.

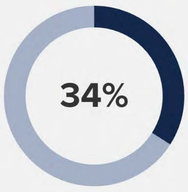
More than a third of bankers will invest in the following technologies, all of which help institutions stay in touch with their customers in one way or another:



Mobile banking app



In-branch technologies



Customer relationship management

At present, fewer bankers plan to prioritize online chat or video bots (16%), financial wellness technologies (10%) or some "other" technology (11%).

Environmental Analysis

The continued push for improved digital account opening and digital lending reflects an environment in which many non-traditional institutions have created a seamless digital experience for customers. Bankers in our survey are acutely aware of the need to be at the top of their game at these critical gateways.

They are also aware of the capability of data and analytics to inform their strategic investments. A strong response in favor of reporting suggests an intensification of data utilization in the coming year.

In-branch technologies also rose in the ranks for 2023, a trend caused by increased foot traffic in branches and institutions' efforts to attract talent by way of improving the workplace for frontline staff.

"Based on their self-assessments, surveyed bankers aren't particularly satisfied with their performance in data analytics and reporting. So, it makes sense that they've elevated it as a priority to make bigger strides this year."

Scott Hess, Head of Digital Banking and Strategy at CSI

Advisory Insight

As institutions expand their digital presence, they don't want to lose their sense of community and customer familiarity. An integrated CRM provides the means to build and maintain a strong connection with individual customers who previously relied on in-person interaction. Further, a truly integrated CRM does the same thing for the increasing universe of digital-first customers.

Modern Banking

Emerging Technologies Energize the Atmosphere

Technology advancements made the digital banking revolution possible, and the latest developments continue to move the financial services industry forward. The potential beneficiaries of such innovation include the financial institutions currently competing against megabanks and non-traditional newcomers. Where do traditional institutions stand in leveraging technology to their advantage?

The Open Banking Ecosystem

READ MORE

A BaaS Barometer Reading Among Bankers

READ MORE

The Growing Groundswell for Faster Payments Technologies

READ MORE

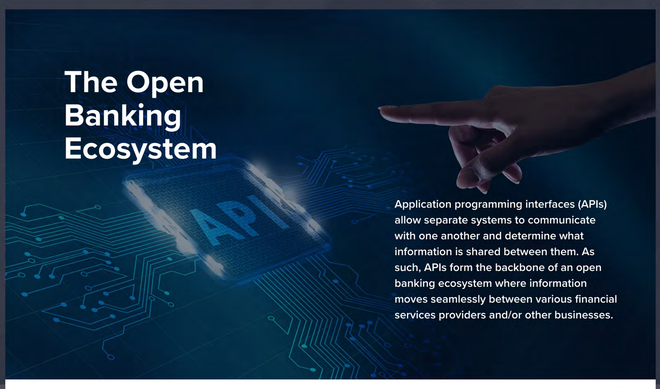
The Expanse of Public Cloud Investments

READ MORE

"Banks must evolve their business models and strategy to avoid becoming a Kodak or Blockbuster. Technology and change make business models obsolete quickly."

Source: Survey Participant

The Open Banking Ecosystem



Application programming interfaces (APIs) allow separate systems to communicate with one another and determine what information is shared between them. As such, APIs form the backbone of an open banking ecosystem where information moves seamlessly between various financial services providers and/or other businesses.

"Open APIs create tremendous opportunities for efficiency within our bank, and we hope this would allow for more collaboration between third parties and other banks."

Source: Survey Participant

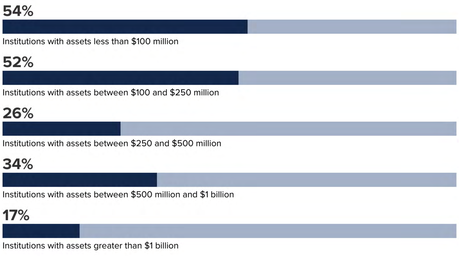
Revealing All Applicable Aspects of Institutions' Open API Ecosystem Strategies

The most popular open API strategy among surveyed bankers this year is platform banking (39%), wherein a financial institution offers third-party products and services to its customers.

This selection is unsurprising, given that most banks rely on third parties to provide digital technologies like digital account opening, digital loan origination and payments technologies.

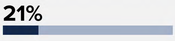
Another 39% of respondents selected None of the Above strategies. While this selection may point to confusion around industry jargon (open banking, platform banking, banking as a service and embedded finance to name a few), it is noteworthy that this option garnered a larger proportion of responses from institutions with the fewest assets. This could suggest a lack of resources to pursue more sophisticated open banking models.

% Of Respondent Institutions that Answered None of the Above



The remaining strategies are less widely used:

Only 21% are embedding their data, products and services into third-party workflows.



Just 16% are offering APIs for third parties to access their data.

15% are enabling fintechs or other businesses to offer financial products.

Fewer still (13%) are using APIs from other financial institutions to improve their services.

Environmental Analysis

Based on their responses, bankers are still in the early stages of leveraging the open banking ecosystem to their advantage. It is only a matter of time before they fully realize how much it can do for them, suggests Scott Hess, CSI's Head of Digital Banking. "APIs facilitate self-customization of their own platforms, and they foster collaboration with fintechs to offer new products and services," he explains.

Advisory Insight

APIs make both platform banking and Banking as a Service (BaaS) possible. Understanding the difference between the two is essential to navigating the current open banking system. This is the simplest way to think of them:

Platform Banking

A financial institution allows its own customers to seamlessly access and integrate another provider's products or services within their customer experience. This allows the institution to expand its offerings beyond its own capabilities.

BaaS

A financial institution enables another business to offer financial products. Alternatively, the two collaborate to offer new, innovative products. Each strategy allows the institution to further expand its market reach.

"An open banking strategy empowers financial institutions to innovate at their own pace and enables market and revenue expansion through BaaS and embedded finance opportunities."

Tara Schultz, VP of Open Banking at CSI

RETURN TO MAIN SECTION

A BaaS Barometer Reading Among Bankers

According to Bankers Helping Bankers, community banks involved in BaaS rank "in the top 1% in both profitability and innovation." The association even goes so far as to say that BaaS represents "the greatest hope in a generation for the future of community banking."[8]

BaaS uses the foundation of open banking to connect financial institutions with fintechs and neobanks to offer innovative products or reach new markets. How do bankers in our survey view this opportunity?

Identifying Institutions' Most Significant Opportunity in BaaS

When asked what they saw as their institution's most significant BaaS opportunity:

32%

Just under a third (32%) see BaaS as an opportunity to streamline operations

23%

Almost a quarter (23%) see potential to create new revenue streams through BaaS

As much as 17% chose *None of the Above* as their answer, an option that once again garnered a larger proportion of responses from institutions with the fewest assets:

% Of Respondent Institutions that Answered None of the Above

31%
Institutions with assets less than $100 million

17%
Institutions with assets between $100 and $250 million

17%
Institutions with assets between $250 and $500 million

12%
Institutions with assets between $500 million and $1 billion

10%
Institutions with assets greater than $1 billion

The remaining options were selected by less than 10% of bankers:

8%

8% view leveraging BaaS opportunities as a way to cut costs

7%

7% selected regulatory compliance as their primary BaaS opportunity

7%

7% see BaaS predominately as an opportunity to increase product speed to market

6%

6% see it as enabling novel, integrated solutions

Environmental Analysis

Even though only around 25% of bankers envision BaaS as an opportunity to create new revenue streams, the untapped potential of this API-facilitated technology is significant. According to research from Future Market Insights, global revenue from BaaS was $2.5 billion in 2020. It is expected to grow to $12.2 billion by 2031. The researchers predict a 15% annual increase in demand for BaaS in the U.S. between 2021 and 2031.[9]

"What used to be a fear is now seen as an opportunity. Many fintechs need FIs to provide exceptional, secure and compliant customer experiences. They will continue to seek out BaaS partners that can demonstrate scalability as users seek expanded banking services."

Tara Schultz, VP of Open Banking at CSI

Advisory Insight

Collaboration with technology providers to provide BaaS helps traditional financial institutions enhance the user experience and tailor innovative banking products to new customer segments. This also helps a bank expand into new market areas, diversify its customer base and create additional revenue streams. BaaS is particularly promising for Sub-Durbin banks, as they stand to greatly increase interchange revenue.

"Participation in a BaaS marketplace allows financial institutions to leverage the scale of a larger provider that builds and maintains the technical infrastructure and connects participating members to partners. It will also likely reduce friction around dealing with regulatory issues and make addressing concerns from auditors and examiners easier."

Steven Ward, manager of CSI Advisory Services

RETURN TO MAIN SECTION

The Growing Groundswell for Faster Payments Technologies

"Overall, the use of real-time disbursements has tripled since 2020,"[10] according to PYMNTS. Both individuals and businesses see cash-flow benefits from having their payments clear immediately, whether on the sending or receiving end. Against this backdrop, how do surveyed bankers feel about real-time payments (RTP) technologies versus other modern payments technologies?

Ranking Seven Payments Technologies by Priority and Interest

The top four priorities identified this year by bankers follow the same order as last year:

46%

Real-Time Payments Technology

Matching consumer demand, almost half (46%) of bankers ranked real-time payments technology as their highest priority, significantly higher than those who did last year (27%) and the year before last (23%). Moreover, three-quarters (75%) ranked it as their first or second priority.

16%

Digital Wallets

Digital wallets are prioritized first by 16% of bankers and first or second by 37%.

18%

P2P Payments

P2P payments came in second, with 18% of bankers ranking it as their top priority and 43% ranking it as a first or second priority.

14%

Same-Day ACH

The only other payments technology that garnered significant interest was same-day ACH, with 14% prioritizing it first and 31% prioritizing it first or second.

Very few bankers selected the following payments technologies as their top priority: credit cards (4%), cryptocurrencies (2%) or Central Bank Digital Currency (0.4%).

Environmental Analysis

The FedNow Service, expected to go live in the summer of 2023, likely influenced surveyed bankers' responses to this question. FedNow will support a broad variety of instant payment types.[11] "This should help to orchestrate the behind-the-scenes processing of real-time payments related to products like P2P that consumers already view as instantaneous," indicates Matt Herren, director of Payment Strategy at CSI.

Advisory Insight

Instability and negative headlines plagued the cryptocurrency market in 2022. Between that and crypto's uncertain regulatory status, it isn't surprising that bankers expressed little interest in payments technologies related to it. However, many younger consumers are still embracing crypto. The U.S. Treasury also released exploratory summaries to weigh the pros and cons of a central bank digital currency (CBDC) in early 2022.[12]

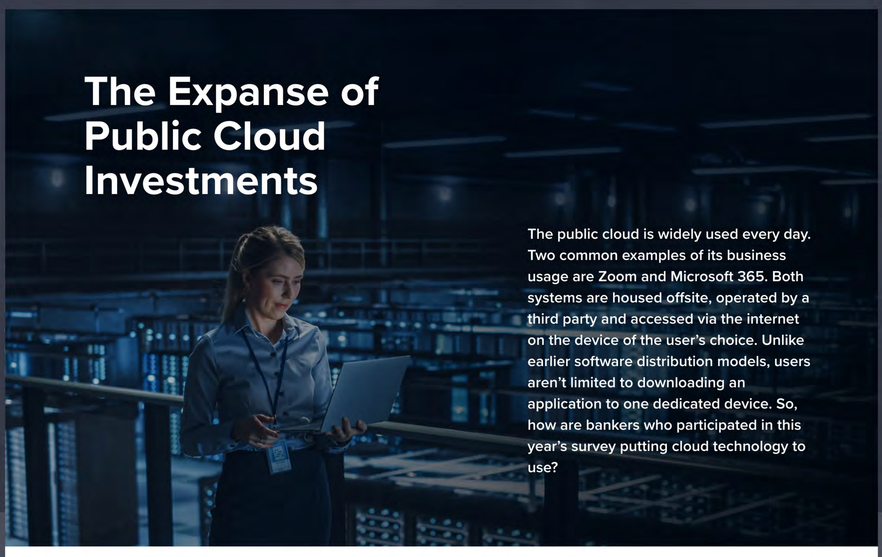
Given consumer and media interest, financial institutions should pay attention to crypto to maintain their position as preeminently trusted financial advisors.

"Emerging channels like cryptocurrencies and CBDC are still very much in the proof-of-concept stage. However, creating strategies for them now will be critical to avoid playing catchup once these become more mainstream. It never hurts to have more options."

Matt Herren, director of Payment Strategy at CSI

RETURN TO MAIN SECTION

The Expanse of Public Cloud Investments



The public cloud is widely used every day. Two common examples of its business usage are Zoom and Microsoft 365. Both systems are housed offsite, operated by a third party and accessed via the internet on the device of the user's choice. Unlike earlier software distribution models, users aren't limited to downloading an application to one dedicated device. So, how are bankers who participated in this year's survey putting cloud technology to use?

Determining How Institutions Plan to Invest in the Public Cloud

Over half of bankers (55%) either don't plan to invest in the public cloud in 2023 (21%), or don't know or don't have enough information to answer the question (34%).

21%

Bankers who don't plan to invest in the public cloud in 2023

34%

Bankers who don't know or don't have enough information to answer the question

The latter equals the same percentage of bankers (34%) investing in one or more cloud technologies. Here is where those investments will be spent:

18%
Data backup and recovery

17%
Cybersecurity solutions

16%
IT infrastructure

11%
Digital banking

10%
Lending

7%
Core

Environmental Analysis

Comparatively, more bankers report using the public cloud than ever before, with 34% of respondents planning to invest this year and 29% in 2022. The overall percentage of respondents has also tripled since 2021. However, the percentage who don't plan to invest in it is identical to last year at 21%.

This could represent a lost opportunity for increasing operational efficiency at those institutions. The public cloud can also help financial institutions create a strong IT environment conducive to remote or hybrid workforces, which could help them recruit and retain employees.

"Cybersecurity and data backup and recovery are two areas where public cloud solutions increasingly make good sense for financial institutions. Such public cloud usage will continue to grow in importance as institutional digital transformation expands."

Steve Sanders, CISO at CSI

Advisory Insight

As long as the provider is a trusted resource within the financial services industry, the public cloud yields several benefits for financial institutions, including these:

Cost optimization
Usage can be scaled up or down based on needs.

Regulatory compliance
It's factored into the application.

Technology deployment
Implementation is quick and easy.

Business continuity
Operational redundancy is ensured through multiple servers.

Remote work
Employees can use the applications no matter where their office is located.

RETURN TO MAIN SECTION

Cybersecurity

Active Threats Persist on the Horizon

As part of our country's critical infrastructure, financial institutions are prime targets of cyberattacks perpetrated by criminal and state-sponsored hacking organizations. Financial institutions also play a critical role in helping their customers learn how to avoid online scams and financial fraud that indirectly harm institutions. As a result, dealing with direct cyber threats will always be a 24x7x365 activity. How do the bankers in our survey feel about this never-ending cybersecurity responsibility?

The Chilling Effect of Cyber Threats

READ MORE

A Temperature Check on Cybersecurity Readiness

READ MORE

Institutional Alignment with the FFIEC AIO Handbook

READ MORE

The Chilling Effect of Cyber Threats

Although cybersecurity is an ever-present issue for financial institutions, the dominant threat types change over time, as do cybersecurity measures.

Revealing the Greatest Forward-Looking Cybersecurity Concerns

Four cybersecurity concerns worry bankers the most going into 2023:

P2P or Other Digital Fraud

Over one-quarter (29%) chose P2P or other digital fraud

Data Breach/Disclosure

Just under one-quarter (23%) selected data breach/disclosure

Ransomware

One-fifth (20%) picked ransomware

Breach at a Third Party

15% indicated a breach at a third party with whom they do business

Bankers expressed little concern about identity theft (4%), unavailable/unaffordable cyber insurance (4%), geopolitical risk (3%), denial of service attacks (2%) and website defacement (0.9%).

Environmental Analysis

The four biggest U.S. banks have faced the most public scrutiny related to P2P fraud to date. Sen. Elizabeth Warren, D-MA, broadcast the results of a recent investigation into Zelle based on the four banks' internal data. It showed that the banks had collectively received $90 million in fraudulent claims associated with the P2P platform in 2020. The investigation also indicated that such claims at these banks were on pace to reach $255 million in 2022, a 183% increase.[13]

That investigation, paired with reported increases in P2P fraud across the industry, explain why bankers in our survey voted it their biggest cybersecurity concern.[14]

"The rising rates in P2P fraud across the industry have institutions wondering if such incidents are the result of data breaches. This perspective likely explains why bankers ranked breaches second on their worry list."

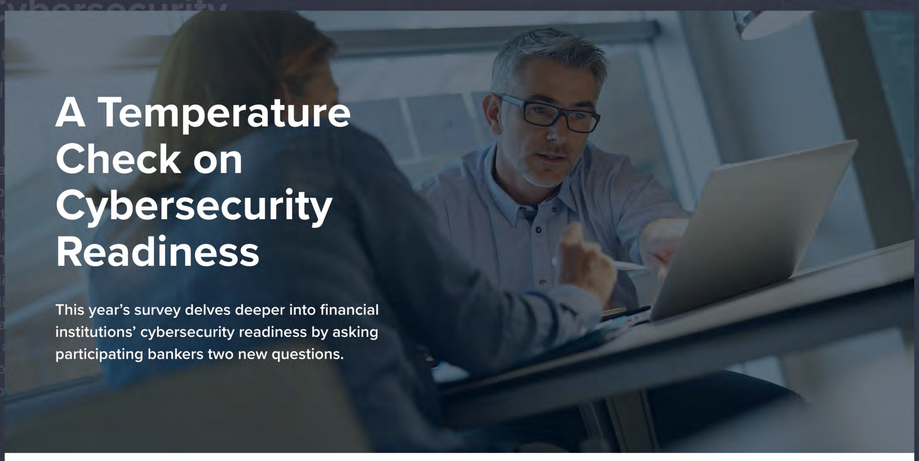
Steve Sanders, CISO at CSI

Advisory Insight

Even though it didn't generate concern in this year's survey, the geopolitical risk posed by enemies of the U.S. shouldn't be overlooked. In April 2022, the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint warning with the FBI and NSA about the threat from one of these enemies. As part of the Russian playbook, the CISA Director emphasized, "that the Russian government is exploring options for potential cyberattacks against U.S. critical infrastructure."[15]

China and North Korea have also developed sophisticated cyber capabilities that are frequently aimed in the same direction as the Russians, which includes financial institutions.

RETURN TO MAIN SECTION



A Temperature Check on Cybersecurity Readiness

This year's survey delves deeper into financial institutions' cybersecurity readiness by asking participating bankers two new questions.

Agreeing or Disagreeing with Various Cybersecurity Statements

The 2023 Banking Priorities Survey asked bankers whether they agree, disagree or neither agree nor disagree with the following statements:

I clearly know what to do if my institution experiences a cyber event.

- 80% Agreed or Strongly Agreed
- 16% Neutral
- 4% Disagreed or Strongly Disagreed

3.9/5 Average, with 5 Being Strongly Agree

I clearly understand our cyber risk.

- 77% Agreed or Strongly Agreed
- 19% Neutral
- 4% Disagreed or Strongly Disagreed

3.9/5 Average, with 5 Being Strongly Agree

I have a reliable source of trustworthy cybersecurity news.

- 72% Agreed or Strongly Agreed
- 24% Neutral
- 4% Disagreed or Strongly Disagreed

3.8/5 Average, with 5 Being Strongly Agree

Our cybersecurity education program is effective.

- 68% Agreed or Strongly Agreed
- 26% Neutral
- 6% Disagreed or Strongly Disagreed

3.7/5 Average, with 5 Being Strongly Agree

If we suffered a data breach, I am confident we would not be found negligent.

- 51% Agreed or Strongly Agreed
- 39% Neutral
- 10% Disagreed or Strongly Disagreed

3.5/5 Average, with 5 Being Strongly Agree

Our CISO can produce a strategic business case for cyber spending.

- 47% Agreed or Strongly Agreed
- 45% Neutral
- 8% Disagreed or Strongly Disagreed

3.5/5 Average, with 5 Being Strongly Agree

Cybersecurity and privacy laws/regulations have improved our processes.

- 36% Agreed or Strongly Agreed
- 52% Neutral
- 12% Disagreed or Strongly Disagreed

3.3/5 Average, with 5 Being Strongly Agree

I find cybersecurity reporting to be clear and easy to understand.

- 31% Agreed or Strongly Agreed
- 48% Neutral
- 21% Disagreed or Strongly Disagreed

3.1/5 Average, with 5 Being Strongly Agree

Environmental Analysis

Bankers feel the least comfortable reviewing cybersecurity reporting provided to them. So, it is possible that survey respondents could be inadvertently overstating answers to some of the other statements. But even with that potential inflation, barely one-half of bankers are confident that their institution would not be found negligent in a breach, which could have catastrophic consequences.

"Based on their responses, there appears to be a certain amount of cybersecurity exhaustion among bankers. This is understandable, but it's still important for institutions to remain vigilant."

Steve Sanders, CISO at CSI

Advisory Insight

It would be beneficial for financial institutions to have internal discussions between their CISO and other C-suite executives to ensure everyone is on the same page and comfortable with the consensus agreement to these statements.

RETURN TO MAIN SECTION

Determining Whether Institutions are in Line with Recommendations from the FFIEC AIO Handbook

Financial institutions have had over a year to digest the most recent addition to the FFIEC's Information Technology Examination Handbook, titled Architecture, Infrastructure and Operations.[16] Consequently, this year's survey asked bankers which of the handbook's recommendations they are using.

Over 50% of Bankers are Using these AIO Recommendations

58%
Conducting Risk Assessments and Impact Analysis Studies

50%
Implementing Safeguards for Hardware, Telecommunications and Software

Over 40% of Bankers are Using these AIO Recommendations

47%
Increasing Cybersecurity Training for Senior Management and Board

43%
Establishing a Risk Tolerance

Over 30% of Bankers are Using these AIO Recommendations

31%
Using a Cybersecurity Framework, such as NIST or CIS

Over 20% of Bankers are Using these AIO Recommendations

29%
Partnering with a Consultant for IT Governance Services

25%
Having Dedicated Architect, Data Officer, & IT Operations Management Roles

Over 10% of Bankers are Using these AIO Recommendations

15%
Establishing a Board-Level IT Governance Committee

Environmental Analysis

As the above results show, none of the FFIEC's AIO Handbook recommendations are being used by more than 58% of bankers. Half of the recommendations are being used by less than one-third of bankers, including the use of a cybersecurity framework, an issue that regulators are now actively examining within financial institutions.

Even more concerning: The two areas that the fewest bankers are following—dedicated AIO roles and a board-level IT governance committee—are specific mandates in the new handbook.

Advisory Insight

More than one-quarter (27%) of bankers participating in the survey indicated that they weren't sure or didn't have enough information to determine whether their institution was using any of these recommendations. This warrants a C-level discussion about the intent of this new handbook and institutional alignment with it.

RETURN TO MAIN SECTION

Regulatory Compliance

Requirements Continue to Flood the Landscape

Regulatory obligations are another perennial issue for financial institutions. Recently, the topic has been further complicated by the struggle to recruit and retain employees, specifically those with the expertise to fill various compliance roles. How do surveyed bankers feel heading into this environment?

Regulatory Concerns Expected to Inundate Bankers

READ MORE

The Surging Risk of Financial Crime

READ MORE

Regulatory Concerns Expected to Inundate Bankers

Regulatory compliance is heating up at the start of 2023. In addition to existing rules and regulations, the Current Expected Credit Loss (CECL) methodology goes into effect for the final group of financial institutions this year. Additionally, everyone is anxiously awaiting the final rule on Section 1071 of the Dodd-Frank Act and the Financial Crimes Enforcement Network's (FinCEN) beneficial owner database.

"Section 1071 and the FinCEN direct registration of beneficial owners will suck up all of the available labor. There will be little time to do anything else."

Source: Survey Participant

Measuring Concern About the Following Regulatory Issues

Amid such flux, bankers express widespread concern about several pressing regulatory issues. To offer more visibility into how UDAAP affects specific areas within a financial institution, this year's survey separated this regulation into two categories – those reflecting operations and those reflecting lending practices.

Regulatory Concern	Percent Who are Very or Somewhat Concerned	Percent Who were Neutral	Percent Who are Very or Somewhat Unconcerned	Average Concern, with 5 being the Most Concerned
UDAAP (Overdraft Fees and the Proposal to Ban Junk Fees)	74%	18%	8%	4.0/5
Cybersecurity Compliance	68%	23%	9%	3.7/5
BSA/AML Modernization	57%	33%	9%	3.6/5
UDAAP (Discrimination and Fair Lending)	55%	32%	13%	3.2/5
Cryptocurrencies	31%	39%	30%	3.0/5
The Community Reinvestment Act (CRA)	29%	52%	19%	3.1/5
Sanctions Compliance (including OFAC)	29%	47%	24%	3.0/5

Environmental Analysis

"Complying with ever-growing and ever-changing regulations is consuming more and more staffing resources at the same time that financial institutions are worried about employee retention," says Steven Ward, manager of CSI Advisory Services. "It's no wonder more than half of bankers are very or somewhat concerned about four of the seven regulatory issues listed in this year's survey."

Advisory Insight

Most bankers are concerned about overdraft fees and potential UDAAP violations. According to CSI Chief Risk Officer, Keith Monson, financial institutions can protect themselves from this risk by:

- Strictly following applicable state laws and usury limits, if any, regarding overdraft fees
- Ensuring what is written in Reg E, Reg DD and Reg CC disclosures matches actual institutional policies, procedures and practices

RETURN TO MAIN SECTION

The Surging Risk of Financial Crime

Risks associated with regulatory compliance have historically posed reputational and financial problems, in the form of monetary penalties, for some financial institutions.

Identifying the Financial Crime that Poses the Greatest Compliance Risk to Institutions

Out of four options, one risk currently dominates all others:

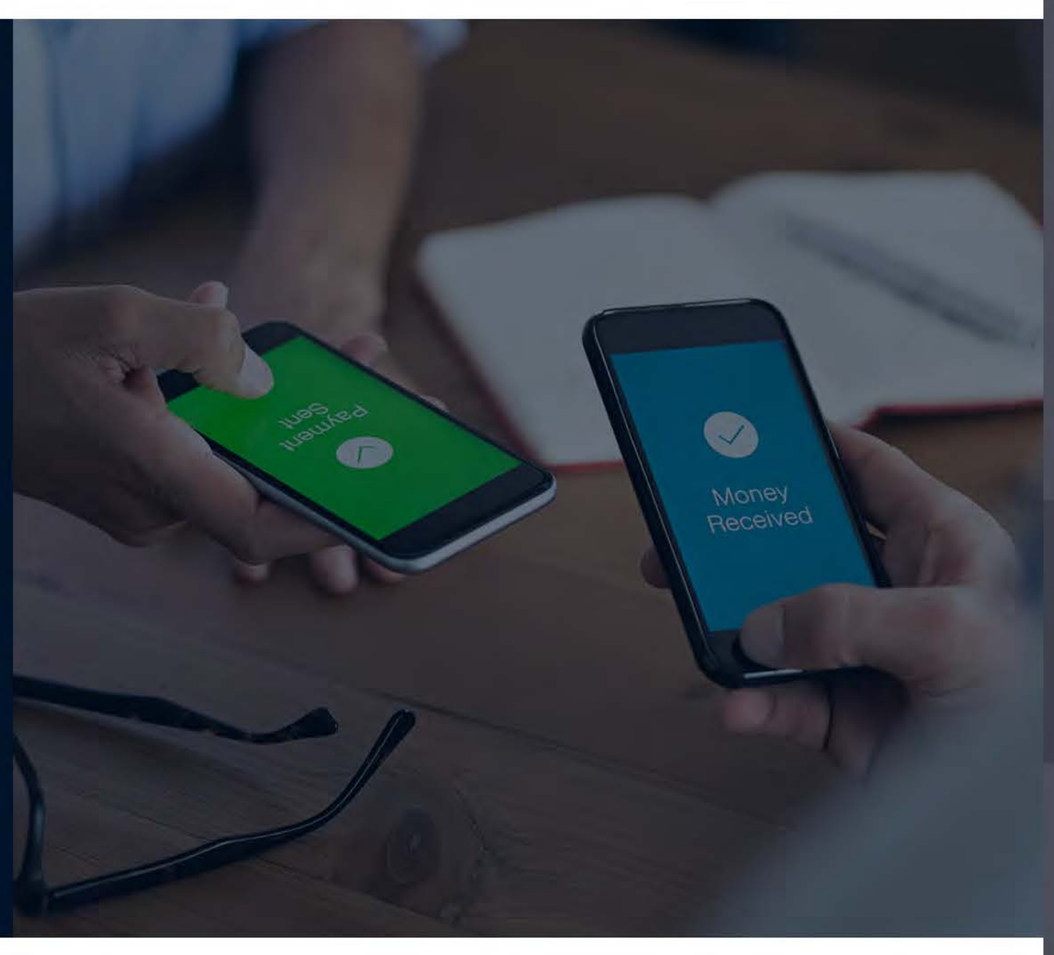
91%

of bankers cited fraud as the greatest compliance risk

Money laundering came in a very distant second at **8%**, with sanctions and terrorist financing receiving scant notice at **0.4%**.

Environmental Analysis

The lopsided response to this question reflects the industry's increasing concern about the Regulation E implications of P2P and other digital fraud. This stems from a recent Wall Street Journal report that the Consumer Financial Protection Bureau (CFPB) is poised to issue new guidance related to P2P fraud. It would consider "fraudulently induced transactions" as unauthorized, making institutions responsible for investigating such claims and compensating their customers.[17]



"Fraudsters have figured out how to manipulate consumers into unwittingly authorizing P2P transactions. This makes their payday that much easier to achieve."

Keith Monson, Chief Risk Officer at CSI

Advisory Insight

According to the independent, bipartisan Center for a New American Security, the U.S. "imposed more than 1,500 discrete sanctioning actions on over 800 targets related to Russia's invasion of Ukraine" in the first four months of the war.[18]

The U.S. continues to impose fresh sanctions as the conflict progresses. As a result, financial institutions should focus on their sanctions and compliance programs, even as they deal with fraud and risks related to all other regulations.

RETURN TO MAIN SECTION

Finding Calm in a Disruptive Atmosphere

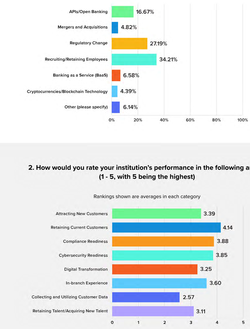
Disruptive periods are always challenging for industry veterans who must consistently adapt. CSI's 2023 Banking Priorities survey confirms that today's digital banking age is no different for traditional financial institutions. But amid this change, one thing remains true: Society still has a penchant for community even as interactions enter the virtual realm and so much is stored in the cloud.

A comforting sense of community has always been a key competitive advantage for financial institutions creating that feeling for their customers. 2023's ecosystem offers such institutions an exciting opportunity to confidently navigate to this true north with new tools at their disposal. Moreover, it allows them to expand their reach beyond their pre-digital imaginations.

Appendix

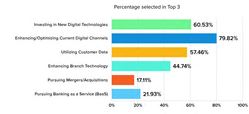
CSI's annual Banking Priorities Survey poses questions to bankers that are designed to reveal the top financial industry issues and trends this year. Below, you'll find charts containing the complete results of the survey.

1. Which one issue will most affect the financial industry in 2023?



2. How would you rate your institution's performance in the following areas? (1 - 5, with 5 being the highest)

3. What are your institution's top 3 strategies to increase market share in 2023?

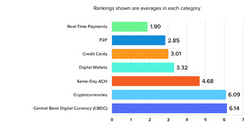


4. What are the top 3 technologies your institution will prioritize in 2023?

5. What is your institution's open API ecosystem strategy? Please select all that apply.

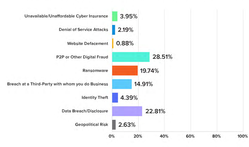
6. What is your institution's most significant opportunity in Banking as a Service (BaaS)?

7. Please rank the following payment technologies by priority and interest: (lower being a top priority)

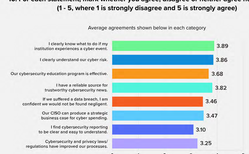


8. Does your institution plan to invest in the public cloud for any of the following technologies in 2023? Please select all that apply.

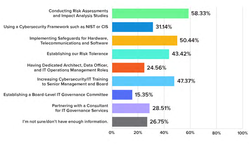
9. Regarding cybersecurity, what is your greatest forward-looking concern?



10. For each statement, mark whether you agree, disagree or neither agree nor disagree. (1 - 5, where 1 is strongly disagree and 5 is strongly agree)



11. How are you bringing your institution in line with recommendations from the FFIEC AIO Handbook? Please select all that apply.



12. How concerned are you about the following regulatory issues? (1 - 5, with 1 being least concerned and 5 being the most concerned)

13. Which financial crime poses the greatest compliance risk to your institution?

Resources

[1] Bureau of Labor Statistics, Economic News Release, Table 4, Quit levels and rates by industry and region, seasonally adjusted

[2] Insider Intelligence, What neobanks are, how they work and the top neobanks in the US & world in 2023

[3] IBM, Cost of a Data Breach Report 2022

[4] Consumer Financial Protection Bureau, Enforcement Actions

[5] Banking Strategist, Community Banks: Number by State and Asset Size

[6] The Federal Reserve, Community Bank Access to Innovation through Partnerships

[7] Illinois General Assembly, Biometric Information Privacy Act

[8] Bankers Helping Bankers, The BHB BaaS Association

[9] Future Market Insights, Banking-as-a-Service (BaaS) Platform Industry Snapshot

[10] PYMNTS, How Consumers Are Driving Demand for Real-time Payments

[11] Board of Governors of the Federal Reserve System, FedNow Service

[12] Federal Reserve, Federal Reserve Board releases discussion paper that examines pros and cons of a potential U.S. central bank digital currency (CBDC)

[13] Warren.Senate.gov, New Report by Senator Warren: Zelle Facilitates Fraud, Based on Internal Data from Big Banks

[14] The Regulatory Review, The P2P Fraud Conundrum

[15] Cybersecurity and Infrastructure Security Agency, CISA, FBI, NSA and International Partners Issue Advisory on Demonstrated Threats and Capabilities of Russian State-Sponsored and Cyber Criminal Actors

[16] FFIEC, Financial Regulators Update Examiner Guidance on Financial Institutions' Information Technology Architecture, Infrastructure, and Operations

[17] Wall Street Journal, CFPB to Push Banks to Cover More Payment-Services Scams

[18] Center for a New American Security, Sanctions by the Numbers: Economic Measures against Russia Following Its 2022 Invasion of Ukraine