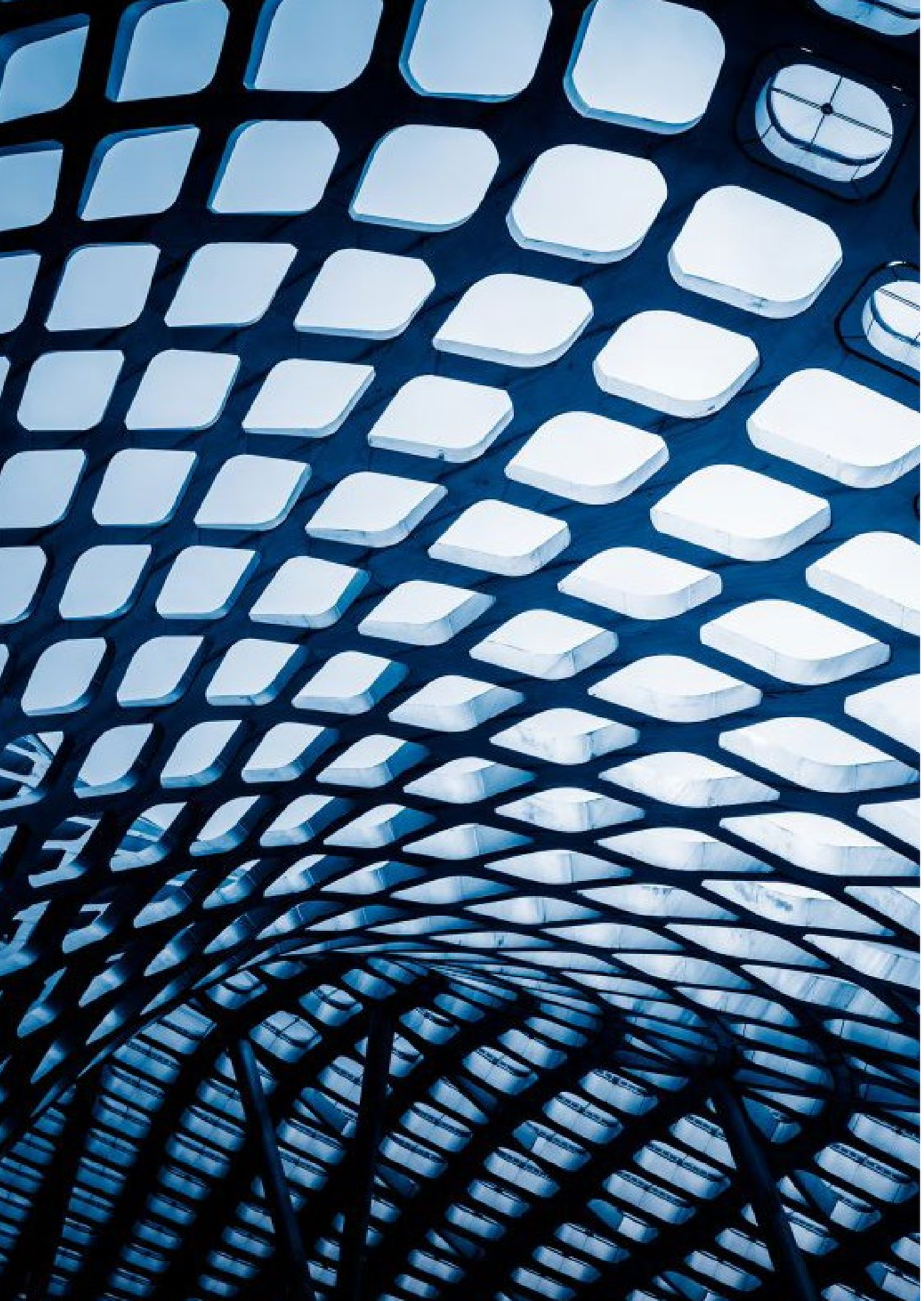
Banking Industry Perspectives

Winter 2023

mazars



Contents

5 Introduction
6 Overview of regulatory releases
8 US Department of the Treasury updates
11 Federal Reserve updates
12 Cybersecurity update
14 Conclusion

Banking Industry Perspectives: Winter 2023

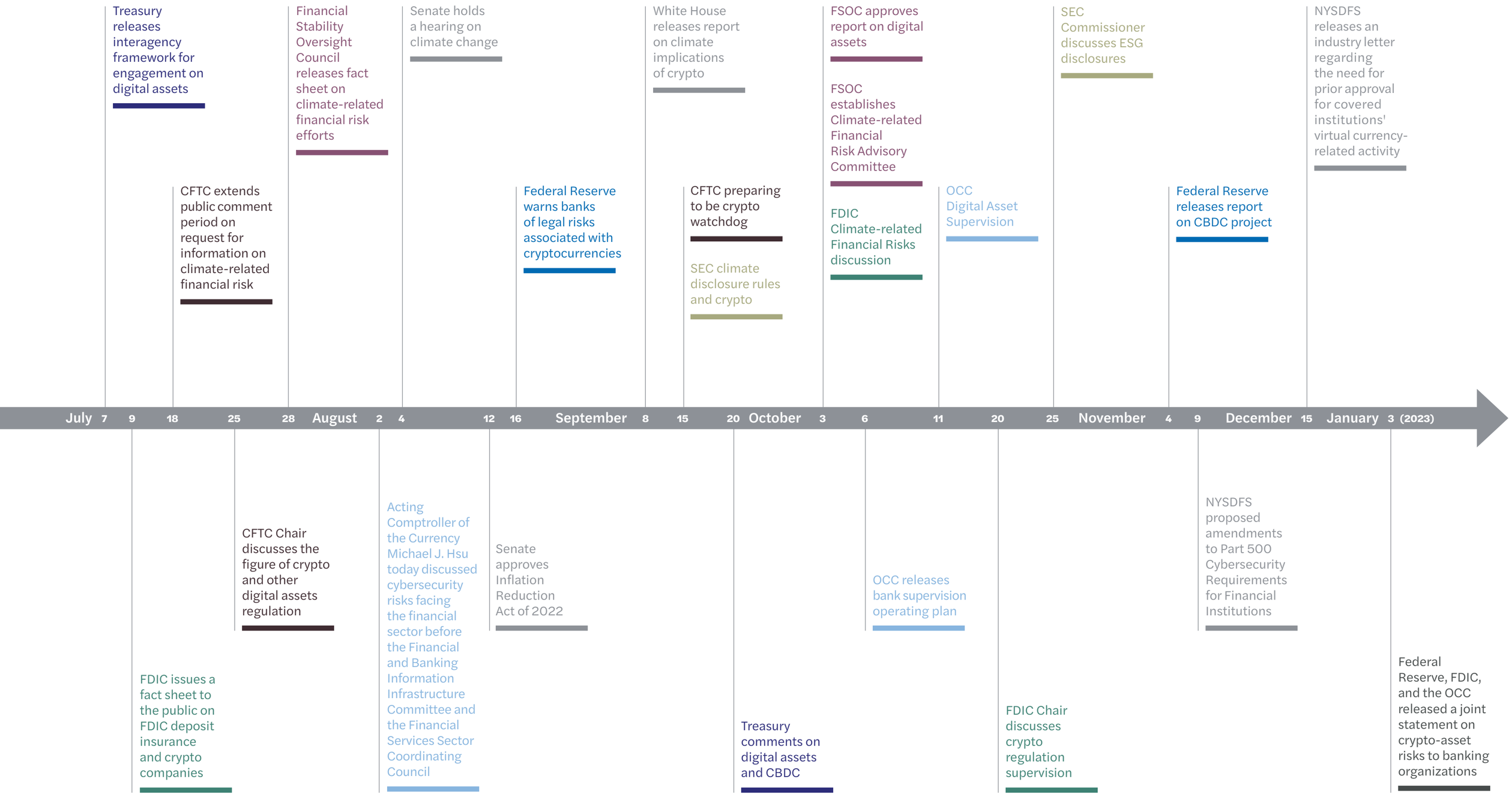
Introduction

The last six months has seen several significant events that have impacted the economy and the financial services industry. High inflation continues to dictate consumer spending behavior despite the Federal Reserve's unprecedented increase in interest rates. Regulators continue to provide guidance about digital assets and the growing importance of embracing the reporting of climate risks. We see a wave of customer experience changing through digital transformation, which has led to increasing cybersecurity risks that must be effectively monitored.

Meanwhile, regulators continue to address the key topics that lacked clarity during these two quarters. We've seen the FDIC, SEC and OCC release guidance on key topics including digital assets, stable coins, ESG and cybersecurity to create more uniformity and consistency within the industry. Regulators were concerned with the vulnerabilities in the digital asset ecosystem and volatility with the stable coins. They moved swiftly by providing clear guidance and heightened security on these topics to protect people from scams and frauds. Meanwhile, climate risk continues to get more attention, and there was additional guidance on the disclosure requirements.

Charles Abraham
US Financial Services
Practice Leader

Overview of regulatory releases



US Department of the Treasury updates
OCC 2023 Supervisory Plan

The Office of the Comptroller of the Currency (OCC) recently released its bank supervision operating plan for fiscal year (FY) 2023. The plan provides the foundation for policy initiatives and for supervisory strategies as applied to individual national banks, federal savings associations, federal branches, federal agencies and technology service providers. The OCC staff uses this plan to guide its supervisory priorities, planning and resource allocations.

Key areas of heightened focus for supervisory strategies in FY 2023:

- Strategic and operational planning
- Operational resiliency
- Third parties and related concentrations
- Credit risk management
- Allowances for credit losses
- Interest rate risk
- Liquidity risk management
- Consumer compliance
- Bank Secrecy Act
- Fair lending
- Community Reinvestment Act
- New products and services
- Climate-related financial risks

The operating plan offers some insights into what OCC examiners will be focusing on, but nothing in the plan should come as a surprise. The financial landscape is changing rapidly with support from third-party vendors to drive digital transformation, which has triggered regulators to keep the pressure on key topics such as cybersecurity, third-party risk management and operating resilience to ensure safety and soundness of the institutions. Regulators also called for banks to be on the lookout for rapidly changing credit market conditions, especially after a period of historical low levels of credit losses. The volatile economic conditions have forced regulators to evaluate the new products and services launched by the various institutions.

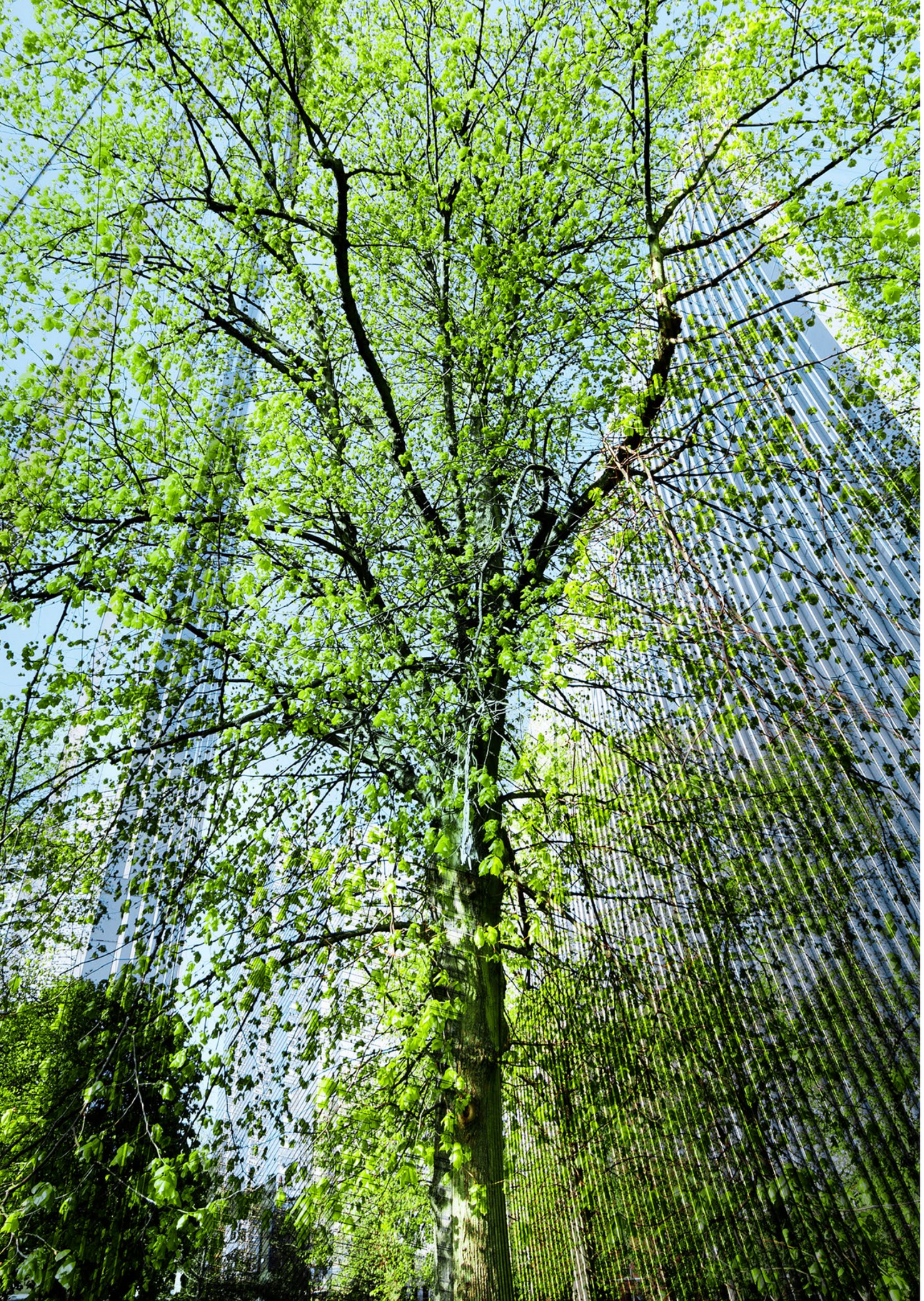
US Department of the Treasury updates
Treasury Releases Interagency Framework for Engagement on Digital Assets

The Treasury Department, in partnership with the State Department and other relevant agencies, released an interagency framework for international engagement on digital assets as directed in the President's March 2022 Executive Order on Ensuring Responsible Development of Digital Assets.

The objectives of this framework are to:

- Protect consumers, investors and businesses in the US and globally by promoting technology and regulatory standards that reflect US values
- Protect US and global financial stability and mitigate systemic risk
- Mitigate illicit finance and national security risks posed by misuse of digital assets and counter and respond to efforts by foreign adversaries to drive standards and promote their protocols
- Reinforce US leadership in the global financial system and in technological and economic competitiveness, including through the responsible development of payment innovations and digital assets and by advancing technology and regulatory standards that align with US values
- Promote access to safe and affordable financial services; and
- Support technological advances that promote responsible development and use of digital assets by advancing research and relationships that increase shared learning

This is a step in the right direction to provide institutions with an ability to identify, measure and monitor the risks from digital assets. It also provides a stable platform to promote cross-border payments.



Federal Reserve update

Pilot climate scenario analysis exercise announced for early 2023

The Federal Reserve Board (Fed) will commence its first bottom-up climate scenario analysis exercise at the beginning of 2023, as announced on Sept. 29, 2022. The exercise will be exploratory in nature and will not result in extra capital requirements. The list of designated participants consists of six of the largest US banks: Bank of America, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley and Wells Fargo.

Overview

The format of the exercise is expected to resemble the Bank of England's Climate Biennial Exploratory Exercise conducted in 2021 and the European Central Bank's Climate Stress Test of 2022. At the start of the exercise, the Fed will share a set of climate scenario narratives with predefined macro financial and climate variables and initial shocks. In the next stage, banks are expected to analyze the scenario pathways, translate the shocks, and assess the impacts on their portfolios and business strategies. Subsequently, the banks will share their findings with the Fed. Later in 2023, the Fed will review the analysis and engage with banks to bolster capacity to manage climate-related financial risks.

The Fed is expected to conclude the exercise with a report consisting of insights gained from the exercise at an aggregate level, reflecting what has been learned about climate risk management practices at the largest banks, and how insights from scenario analysis will help identify potential risks and promote risk management practices. The Fed affirms that no firm-specific information will be released.

Additional details on the exercise and scenarios will be shared later this year.

Further remarks

Although the list of participating banks has been limited by the Fed, the US and international banking industries are advised to follow the pilot exercise and incorporate the methodological considerations, if made public, into their climate-related and environmental risk management frameworks and internal scenarios.

Cybersecurity update

On Nov. 9, 2022, the New York State Department of Financial Services (NYSDFS) published a proposed amendment to its 2017 cybersecurity regulation (Part 500), which requires certain NYSDFS-regulated financial services companies to, among other things, safeguard consumer data and adopt and implement a cybersecurity program. Here are some key changes in the proposed amendments:

1. Increased accountability

The proposed amendment has increased accountability of senior governing body for cybersecurity governance practices. This amendment adds a new dimension that senior leaders/executives (CISO/CTO) must have sufficient cybersecurity expertise and take ownership to approve the written policies and procedures annually.

2. Enhanced reporting

The proposed amendments provide three new cybersecurity events that covered entities must report to NYSDFS via the NYSDFS online cybersecurity portal within 72 hours:

- Unauthorized access to privileged accounts
- Deployment of ransomware within a material part of the covered entity's systems
- Any cybersecurity event that affects a third-party service provider that also affects the covered entity

3. Monitoring of privileged accounts

The proposed amendment focused on the key vulnerability deployed by cybercriminals of gaining access through privileged accounts. Hence the proposed amendment provides certain limitations to control such privileged accounts through:

- Limiting the number of privileged accounts
- Limiting access to privileged accounts to only those users who need access to perform their job
- Limiting the use of privileged accounts to only when performing functions requiring use of such accounts
- Annual review of all user access privileges and removal of accounts and access that are no longer necessary
- Employing multifactor authentication (MFA) for all privileged accounts
- Promptly terminating access following departures
- Implementing a privileged access management solution
- Implementing an automated method of blocking commonly used passwords

4. Increased controls

As part of bolstering the cybersecurity program, here are several key controls that companies must implement:

- Monitor authorized users and detect unauthorized users tampering with nonpublic information
- Monitor web traffic to block malicious content
- Centralized logging and security event alerting
- Increased cybersecurity awareness training of employees
- Incident response plan. Incident response plans shall be designed to promptly respond to, and recover from, any cybersecurity event materially affecting the confidentiality, integrity or availability of the covered entity's information systems or the continuing functionality of any aspect of the covered entity's business or operations
- Business continuity and disaster recovery plan (for purposes of this Part, BCDR plan). BCDR plans shall be reasonably designed to ensure the availability and functionality of the covered entity's services and protect the covered entity's personnel, assets and nonpublic information in the event of an emergency or other disruption to its normal business activities
- Annual testing of its incident response plan, BCDR plan and ability to restore its systems and backups

5. Revised definition of Class A companies

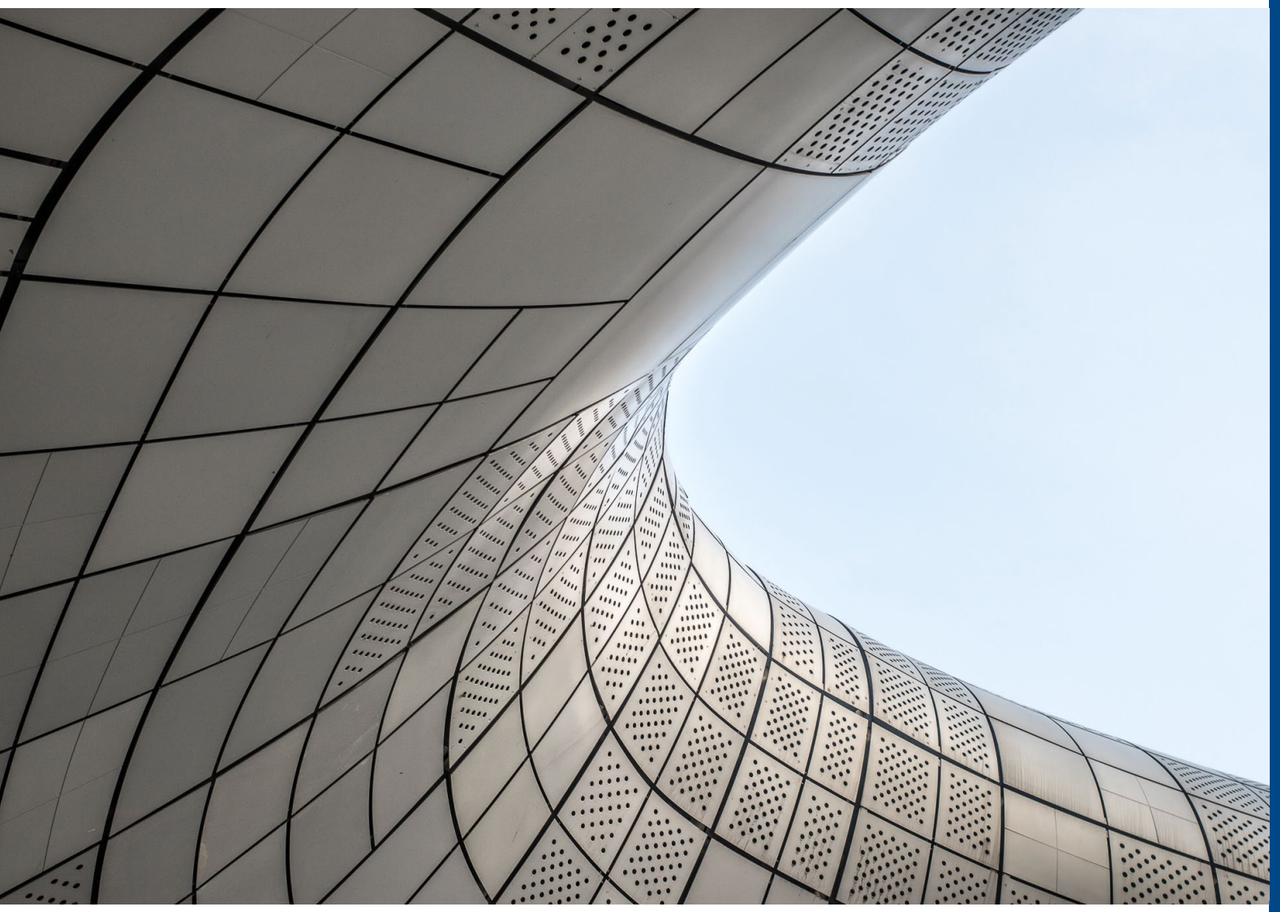
Class A companies are those covered entities with at least $20 million in gross annual revenue in each of the last two fiscal years from business operations of the covered entity and its affiliates in this state and:

(1) over 2,000 employees averaged over the last two fiscal years, including those of both the covered entity and all its affiliates no matter where located; or

(2) over $1 billion in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and all its affiliates. Covered entity means any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law, regardless of whether the covered entity is also regulated by other government agencies

Conclusion

We will continue to see more traction on cybersecurity, cryptocurrency and ESG in 2023 as well. The other evolving risks such as paucity of resources, increased interest rates, onset of innovation and recession fears will guide the strategies that the banks will resort to. The larger financial institutions will continue to invest in digital transformation, system advancement and cloud migration to strengthen their cybersecurity and reduce long-term operating costs. We will also continue to see the trend of smaller community banks being merged with or acquired by large banks to expand their footprint.



Key contributor

Shiv Venkatraman, Principal, Mazars
+1 (818) 414-0738
shiv.venkatraman@mazarsusa.com

Contacts

Charles Abraham, US Financial Services Practice Leader, Mazars
+1 (212) 408-1779
charles.abraham@mazarsusa.com

Emmanuel Dooseman, Partner, Global Banking Leader, Mazars
+1 (646) 315-6189
emmanuel.dooseman@mazarsusa.com

mazars

About Mazars
Mazars is an internationally integrated partnership, specializing in audit, accountancy, advisory, tax and legal services*. Operating in nearly 100 countries and territories around the world, we draw on the expertise of more than 47,000 professionals – 30,000+ in Mazars' integrated partnership and 17,000+ via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*Where permitted under applicable country laws

Mazars USA LLP
Mazars USA LLP is an independent member firm of Mazars Group, an international audit, tax and advisory organization with operations in nearly 100 countries and territories. With roots going back to 1921 in the US, the firm has significant national presence in strategic geographies, providing seamless access to 30,000+ professionals around the world. Our industry specialists deliver tailored services to a wide range of clients across sectors, including individuals, high-growth emerging companies, privately-owned businesses and large enterprises.

www.mazars.us

© Mazars 2023