Acting Comptroller of the Currency Michael J. Hsu

"Thoughts on Operational Resilience"

Remarks at the Institute of International Bankers

Annual Washington Conference

March 12, 2024

Thank you for the opportunity to join you at this year's Institute of International Bankers (IIB) Annual Washington Conference. The IIB has a long history of bringing together senior government officials and industry leaders to address policy and business issues of importance to the international banking community in the United States. The annual conference has always provided a great forum to exchange ideas and discuss important issues, and I'm pleased to have another opportunity to be a part of it.

I would like to focus my remarks today on operational resilience. This topic is often overlooked or overshadowed by debates about capital and liquidity. It shouldn't be. The operational resilience of critical banking services is important to the safety and soundness of banks and to financial stability. It warrants our full attention, especially in our highly interconnected world.

What do I mean by "operational resilience"? Operational resilience is the ability of a bank to prepare for, adapt to, and withstand or recover from disruptions. Disruptions may result from external events, like natural disasters, malicious actors, pandemics, or global conflicts, or from weak internal systems, controls, or risk management. Disruptions may impede the provision of services, like payments, clearing and settlement, or adversely impact systems or corrupt data.

Both the *probability* of disruptions occurring and the potential *impacts* from those disruptions are increasing. As banking services continue to grow and as technology and third parties play a greater role in the provision of those services, the threat surface for disruptions is expanding.

Notably, the impacts of most concern here are *not* financial, i.e., this is not a problem that capital or liquidity can solve. Ensuring that critical operations and banking services can withstand or recover from disruptive events requires good planning, prudent investment, well-designed systems, and regular testing. It is this that I would like to discuss today.

The Growing Risk of Disruptions

To help give a sense of how the risk of disruptions is growing, consider the following:

- Twenty years ago, the top four custodian banks safe-kept $24 trillion of assets. Today, they safe-keep over $108 trillion.
- In 2014 the ACH Network processed 18 billion payments totaling $40 trillion. In 2023, it processed 31 billion payments totaling $80 trillion.[1]
- Trading activity has also grown considerably. The notional amount of derivative contracts held by U.S. banks increased from $70 trillion in 2003 to $193 trillion at the end of 2023.[2]

The sheer magnitude of what can be disrupted has increased significantly – a trend likely to continue for the foreseeable future.

---

[1] See Nacha, "Overall ACH Network Volume: 2023 Volume and Value," available at https://www.nacha.org/content/ach-network-volume-and-value-statistics.

[2] See Consolidated Reports of Condition and Income ("Call Report"), Schedule RC-L. Current and historic Call Report data are available at https://www.ffiec.gov/reports.htm.

At the same time, banks have distributed their processes and people across the globe – for instance, the banking industry has tens of thousands of employees in India, Poland, and other countries supporting risk management systems, reconciling trades, managing technology support, and executing back-office functions. In addition, banks continue to expand their partnerships with third parties to support an increasingly wide range of tasks.

The provision of banking services increasingly resembles global manufacturing supply chains, with their efficiencies, complexities, and vulnerabilities.

These trends and their interactive effects have been largely invisible to most people. Just as many consumers and businesses were blissfully unaware of the complexities of supply chains until the pandemic hit, most consumers and users of banking services today are similarly unaware of the growing risks of disruptions in today's banking system. Take, for instance, the recent ransomware attacks on EquiLend,[3] a securities trading provider, on Ion Markets,[4] a capital markets technology firm, and on the Industrial and Commercial Bank of China, one of the largest banks in the world.[5] Most observers could be forgiven for shrugging these off as minor incidents, when in fact, they should be seen as early warning signs of the complexity of the financial system and its vulnerability to disruption.

Supervisory Expectations

Regulatory agencies like the OCC expect financial institutions to be operationally resilient.

[3] Matthews, Laura, and Manya Saini, "Equilend restores some services after cybersecurity incident," February 2, 2024.

[4] Robertson, Harry, "ION brings clients back online after ransomware attack – source," February 7, 2023.

[5] "ICBC partners wary to resume trading with bank after cyberattack - Bloomberg News," November 22, 2023.

These expectations were first laid out in the Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, which was released following the September 11, 2001, attack on the World Trade Center.[6] That paper provided guidance on geographic diversity and resiliency of data centers and operations, as well as on recovery and settlement expectations for significant firms in critical financial markets.

Of course, the operating environment evolved significantly with advances in technology, rapid and widespread digital adoption, and increases in cyber attacks. In October 2020 the federal banking agencies issued a paper titled "Sound Practices to Strengthen Operational Resilience,"[7] which integrated existing guidance, common industry practices, and the work of the Basel Committee on Banking Supervision's Operational Resilience Group.[8] Additionally, the Federal Financial Institutions Examination Council (FFIEC) *Information Technology Examination Handbook* was updated to include a booklet on Business Continuity Management.[9] In 2021, the federal banking agencies adopted the Computer-Security Incident Notification Rule to bolster cyber defenses.[10] And then last year, the federal banking agencies issued interagency guidance on third-party risk management, building off of the OCC's longstanding guidance on the topic.[11]

---

[6] OCC Bulletin 2003-14, "Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System: Business continuity sound practices developed by the FRB, SEC, and OCC to ensure the continued functioning of critical financial services," April 8, 2013.

[7] OCC Bulletin 2020-94, "Operational Risk: Sound Practices to Strengthen Operational Resilience," October 30, 2020.

[8] Bank for International Settlements, "Principles for operational resilience," March 31, 2021.

[9] FFIEC, "Business Continuity Management" booklet, *IT Examination Handbook*.

[10] OCC Bulletin 2021-55, "Computer-Security Incident Notification: Final Rule," November 23, 2021.

[11] OCC Bulletin 2023-17, "Third-Party Relationships: Interagency Guidance on Risk Management," June 6, 2023.

The OCC has been active in calling out operational resilience and cybersecurity risks, for instance in the OCC's December 2023 *Semiannual Risk Perspective*[12] and Fiscal Year 2024 Bank Supervision Operating Plan.[13]

Taken together, these have promoted operational resilience through strengthened risk management and operational recovery capabilities. They are clearly necessary. As banking continues to evolve, however, a key policy question we must consider is whether they are sufficient, especially for critical operations.

Strengthening Operational Resilience

Other jurisdictions have taken steps to strengthen the operational resilience of their critical financial infrastructure through the adoption of rules. For instance, the European Union's (EU) Digital Operational Resilience Act (DORA) provides clear expectations for information and communication technology (ICT) at covered firms. These include requirements for ICT risk management, incident response and reporting, operational resilience testing, third-party risk management, and information sharing. DORA is significant in that it will not only set operational requirements for financial institutions, but also will cover designated critical service providers as being subject to the same requirements and examination under the rule.

Like the EU, both the United Kingdom and Japan have proposed similar operational resilience rules that require firms to identify important business services, map processes, set impact tolerances, test under different scenarios, and establish standards for outsourcing and

[12] OCC *Semiannual Risk Perspective* (Fall 2023).

[13] OCC News Release 2023-109, "OCC Releases Bank Supervision Operating Plan for Fiscal Year 2024," September 28, 2023.

third-party risk management.[14] Other international counterparts have taken similar steps to strengthen operational resilience within their jurisdictions.

Domestically, the federal banking agencies are considering what changes to our operational resilience framework might be appropriate. Our current focus is on exploring baseline operational resilience requirements for large banks with critical operations, including third-party service providers. Such baseline requirements could include establishing clear definitions for identifying critical activities and core business lines; defining tolerances for disruption; requiring testing and validation of resilience capabilities; incorporating third-party risk management expectations; stipulating clear communication expectations among stakeholders and counterparties; and addressing expectations for critical service providers, with emphasis on governance and risk management expectations.

Gathering input from the industry and other stakeholders will be important. To ensure consistency across institutions and over time, careful consideration will need to be given to how critical systems are defined, what the relationship is between similar concepts (e.g., recovery time objectives, tolerance for disruptions, maximum allowable downtime), and whether expectations vary under different scenarios (e.g., loss of a data center due to fire versus a ransomware attack).

With operational resilience, collaboration is key. One of the most effective forums for incident response and resilience has been the Financial and Banking Information Infrastructure

[14] In the United Kingdom, a new operational resilience regime, introduced by the Prudential Regulation Authority, Financial Conduct Authority, and Bank of England (BoE), took effect on March 31, 2022. See BoE, "Operational Resilience: Statement of Policy," March 29, 2021. In April 2023, Japan's Financial Services Agency published a "Discussion Paper on Ensuring Operational Resilience," setting forth policies to strengthen financial institutions' operational resilience.

Committee (FBIIC). The FBIIC is composed of 18 member organizations[15] across the federal and state financial regulatory community. It helps coordinate interagency efforts to improve the reliability and security of the financial sector infrastructure by sharing near real-time threat information and effective security practices. It also coordinates responses to cybersecurity incidents and other significant events that affect the financial sector. The FBIIC coordinates with the private sector via the Financial Services Sector Coordination Council (FSSCC). This partnership has been beneficial in speeding communication and enhancing transparency across stakeholders during significant operational outages and cyber events.

As your members know well, disruptions can easily spread across boundaries. We are committed to improving coordination with key partners internationally, building on existing bilateral relationships and dialogues, as well as further developing multilateral relationships through various standard setting bodies and forums.

Conclusion

In conclusion, I want to re-emphasize that the resilience of large banks' critical operations deserves our full time and attention. As the threat surface for disruptions expands, and as authorities in other jurisdictions begin implementing their rules to ensure operational resilience, we are assessing and working with our interagency peers to develop the right approach here in the U.S. We look forward to working with the industry and other stakeholders on this.

[15] FBIIC members are available at https://www.fbiic.gov/fbiic-members.html.