

Acting Comptroller of the Currency Michael J. Hsu

Remarks at FDX Global Summit

“Open Banking and the OCC”

April 19, 2023

Thank you for inviting me to speak at this year’s Spring FDX Global Summit. It is an honor and pleasure to be here.

The timing of this gathering is fortuitous. Last month’s high profile bank failures revealed how innovations and changes in technology, information flows, and customer capabilities can impact the risk profiles of banks. While it would be an overstatement to attribute those bank runs solely to social media and mobile banking, it would be equally naïve to ignore the impact that they, and other changes, have had on the industry. We, bank regulators, need to pay closer attention to how changes in technology and associated practices may impact risks in banking. Gatherings like this certainly help.

With this in mind, I would like to talk today about how the Office of the Comptroller of the Currency (OCC) is approaching open banking. The OCC supervises and regulates national banks and federal savings associations, roughly 1,100 institutions with over \$15 trillion in assets.

The potential for open banking to provide consumers with greater control over their financial data, to increase the portability of banking accounts, and to foster greater competition and fairness in the provision of financial services is significant and may impact banking in a variety of ways. I would like to discuss how these potential impacts may intersect with the OCC’s mission of ensuring that the operations of federally chartered banks are safe, sound, and fair.

Open Banking

Let me start by providing some context.

Definitions vary, but in general, open banking is understood to be about enabling consumer-permissioned sharing of financial data with third parties to empower consumers, foster competition, and expand financial inclusion.¹ The OCC supports these objectives.

Historically, federal oversight regarding financial data sharing in the U.S. focused primarily on consumer privacy, security, and protection, through the Gramm–Leach–Bliley Act (GLBA) and various state privacy laws. This approach was updated and expanded with the passage of the Dodd–Frank Act in 2010, specifically section 1033, which authorizes the Consumer Financial Protection Bureau (CFPB) to issue rules regarding consumer data access rights. Last October, the CFPB issued a Small Business Regulatory Enforcement Fairness Act (SBREFA) outline of rulemaking proposals on “personal financial data rights” under section 1033—a step towards potential issuance of a notice of proposed rulemaking (NPR) on open banking.²

Open banking is not unique to the U.S. The UK, Australia, and the EU, for instance, have implemented varying degrees of structured open banking frameworks, with defined requirements for the sharing of certain information among participants.³ Many other countries are also on paths to greater sharing of consumer-permissioned data. Open banking frameworks vary across individual jurisdictions but generally address similar issues such as consumer authorization standards; articulation of rights and responsibilities for data providers and data users; enforcement of privacy requirements; security expectations for sharing of information; and standards for third parties engaging in information sharing, such as data aggregators.

¹ Consumer Financial Protection Bureau, “[Final Report of the Small Business Review Panel on the CFPB’s Proposals and Alternatives Under Consideration for the Required Rulemaking on Personal Financial Data Rights](#)” (March 30, 2023); Bank for International Settlements, “[API standards for data-sharing \(account aggregator\)](#)” (October 2022).

² This marked the culmination of several years of engagement on the issue by the CFPB. In 2017, the CFPB released guidance that listed nine principles intended to help safeguard consumer interests. Then in November 2020, the CFPB indicated its intent to issue a rule to implement section 1033, and in October 2022, the CFPB issued several documents outlining proposals and alternatives under consideration as part of its rulemaking efforts. Earlier this month, the CFPB released its final report as part of the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA) process. The final report includes findings and recommendations made by the SBREFA panel, which will inform the CFPB’s future rulemaking efforts. Refer to note 1.

³ Open banking in the EU has been driven primarily by the second Payment Services Directive, also known as PSD2. Open banking in the UK is driven by the Payment Services Regulations (PSR). Australia’s path to open banking has been led through the Consumer Data Right Act (CDR).

The catalyst for these efforts, of course, has been the digitalization of banking and finance and the associated promises of innovation and value creation. Initially, there was a dichotomy between bank and nonbank approaches to consumer financial data. Banks tended to emphasize security, privacy, and compliance (as required under GLBA), while technology firms tended to focus on innovation and growth (to meet the expectations of their investors). The evolution of the market and emergence of consortiums like FDX has led to some convergence and even a blurring of the line between banking and commerce—a topic I will return to later.

To date, the OCC’s communications on open banking have been fairly limited.⁴ Our supervision has focused primarily on banks’ compliance with GLBA. But we are evolving. In 2016, the OCC established the Office of Innovation recognizing the rapid pace of change in financial services, especially related to digitalization. Those innovations are increasingly table stakes for banks and financial services providers. Reflecting the importance of these innovations, we recently expanded and rebranded the unit as the Office of Financial Technology, which is now headed by a Chief Financial Technology Officer, Prashant Bhardwaj. Prashant started in this role last week and is here with us today.

Open Banking and Bank Safety and Soundness

The mission of the OCC is to ensure that federally chartered banks operate in a safe and sound manner, provide fair access to financial services, treat customers fairly, and comply with applicable laws and regulations. The evolution of open banking may impact what and how we supervise, from liquidity risk to operational risk to third-party risk management to compliance risk.

Take, for instance, account portability. For some consumers, this is one of the most promising aspects of open banking, as it may eventually allow consumers to easily move checking and savings accounts from one bank to another. While such portability will be empowering for consumers, in isolation this would likely increase the liquidity risk of retail deposits for banks.

⁴ See [OCC Bulletin 2020-10](#), “Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29,” (March 5, 2020).

Historically, retail deposits have been viewed as a relatively stable source of funding for banks. Under the Liquidity Coverage Ratio (LCR), banks subject to the liquidity rule must hold high-quality liquid assets sufficient to meet expected stressed outflows over a 30-day period.⁵ The LCR runoff rate for retail deposits is quite low—around 5 percent.⁶ But with instant and seamless account portability, retail outflows in the future could be higher. Already, there is a sense that online and mobile banking may have facilitated unusually large and rapid outflows of wholesale deposits at Silicon Valley Bank and Signature Bank last month.⁷

Of course, banks will likely respond to account portability by taking steps to retain customers, much as wireless carriers did after cell phone number portability was adopted. In time, such steps by banks could actually increase the stickiness of retail deposits and *lower* their liquidity risk, despite consumers having the ability to easily move accounts. I believe such a state is possible, even likely, but the *transition* to that state warrants careful monitoring.

Security is a prerequisite for the sharing and receiving of consumer financial data. Already, banks are expected to implement effective information security programs to safeguard sensitive consumer information.⁸ An increase in the volume and complexity of consumer-permissioned sharing may introduce new risks and necessitate new controls. Consider for example the possible complexities due to the distributed nature of the underlying technological infrastructure that may present risks to data integrity and security. As practices evolve, cyber threats and other security risks will need to be reassessed and certain controls strengthened, such as authentication processes, secure data transmission protocols, and limitations on what is shared and received.

Stepping back, open banking’s promise of greater innovation, efficiency, and competition will rely to a great extent on a richer and more complex financial ecosystem. Banks as data providers will need to interact with aggregators, fintechs, technology firms, and competitor

⁵ Refer to 79 Fed. Reg. 61440 (October 10, 2014). The LCR rule is codified at 12 CFR 50 (OCC).

⁶ Ibid.

⁷ Remarks by Martin J. Gruenberg, Chairman, Federal Deposit Insurance Corporation, “[Recent Bank Failures and the Federal Regulatory Response](#),” before the Committee on Financial Services, United States House of Representatives (March 29, 2023); remarks by Travis Hill, Vice Chairman, Federal Deposit Insurance Corporation, “[Recent Bank Failures and the Path Ahead](#)” at the Bipartisan Policy Center (April 12, 2023).

⁸ 12 CFR 30 appendix B.

banks. They will need to expand from reliably handling their customers' money, to also reliably handling their financial data. While this may bring significant benefits to consumers and generate new avenues of value creation, it will also likely raise accountability challenges when mistakes are made and consumers are hurt, especially as the set of players in the space grows and proliferates. Nonbank participants will have varying capabilities, strengths, and weaknesses. The OCC's third-party risk management expectations provide a foundation for banks to assess those relationships.⁹ But some evolution and refinement of those expectations may be needed as open banking and the fintech landscape evolve.

Zooming In on Data, Zooming Out to Banking and Commerce

Having now covered some of the safety and soundness considerations related to open banking, I would like to spend a moment zooming in on data and zooming out to banking and commerce. Keeping both of these in mind will be important to how open banking evolves and will help ensure that it develops in a way that builds trust among consumers and the public.

First, let's zoom in on data.

Data are made, not found. This important reminder is a key theme in Chris Wiggins and Matthew L. Jones's recent history of data.¹⁰ The following excerpt from their book, How Data Happened, is worth quoting in full:

The study of data threatened to displace other forms of expertise, from science to shop floors to the drug store. Rather than lush descriptions of countryside, a counting of flora and fauna. Rather than an ethical discussion of values, an attempt to model the effects of a given policy quantitatively. Rather than the gruesome reality of death, tables of mortality statistics. Rather than expertise about potential desires of consumers, the collection and analysis of every purchase. Rather than the clinical experience of individual physicians with a drug, randomized trials to gauge effectiveness and safety. Rather than a

⁹ Refer to OCC Bulletin 2013-29, "[Third-Party Relationships: Risk Management Guidance](#)" (October 30, 2013); OCC Bulletin 2020-10, "[Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29](#)" (March 5, 2020).

¹⁰ Wiggins, C., & Jones, M.L. (2023). "How Data Happened: A History from the Age of Reason to the Age of Algorithms." National Geographic Books.

judgment of the character of a student applying to college, the use of standardized tests to supply an 'objective' measurement.

The authors go on to note: “Statistics doesn’t simply represent the world. It transforms how we categorize and view the world. It transforms how we categorize others and ourselves. It changes the world. And, as we’ll see, contemporary data science does this—at hyperspeed.”

I raise this as a reminder and caution not to reify data as reality and confuse means and ends. The data that underpin the digitalization of finance and open banking are a tool—a means, not an end. The end—the underlying reality—is about people and communities and helping them realize their economic potential. Collecting and sharing data can help, but—if we are not careful—it can also hurt.

The hyper focus of current data science, AI, and machine learning on *prediction* has proven to be extremely powerful and enormously profitable for the tech industry. In banking, it has similar potential, for instance by making those with bank accounts but without credit scores ‘visible’ to lenders. The flip side of predictive data, however, is prejudicial data. If we become too starstruck with data and too wedded to statistical prediction, we risk locking people and communities in and overlooking their potential and the possibility of change and progress simply because of “what the data say.”

I encourage those working on open banking and financial innovation to read James Scott’s *Seeing Like a State*.¹¹ The book details how governments have developed and relied on *statistics*—the data and science of the state—to make their polities “legible” and thus manageable. Statistics and power are linked. They can be used for good and for ill, for private profit and for the common good. Neutral they are not. If open banking advocates can absorb that lesson and abide by inclusive governance, I believe it will improve the chances of open banking succeeding as envisioned.

Zooming out, we also need to be cognizant of the blurring of the line between banking and commerce. Open banking cannot be accomplished by banks alone. Data aggregators and fintechs already play a significant role, which will expand as open banking is more fully adopted.

¹¹ Scott, J.C. (1999). “Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed.” Yale University Press.

In addition, large technology firms, like Apple, Google, Amazon, and Meta, continue to increase their reach and capabilities in payments and other financial services, such as lending.¹² For some banks, large fintechs and technology firms are simultaneously key vendors, partners, and competitors. It is, in short, getting harder and harder to distinguish between banking and commerce in the digital arena.

Why does this matter? Traditionally, we have sought to maintain a separation of banking and commerce in order to mitigate excessive concentrations of power, threats to bank safety and soundness, and systemic financial risk. I will skip the history lesson here but will note that the power of network effects with digital businesses seems to drive technology firms towards constant expansion into adjacent fields, including banking. This bears careful monitoring and close collaboration among government agencies.

Conclusion

In conclusion, I would like to make an observation and plea with regards to culture.

Banks and banking used to be synonymous. As Tabor et al. put it in their history of banking regulation, “Because you do, you are; and because you are, you do.”¹³ In other words, banks were defined by the activity of banking and the activity of banking could only be done by chartered banks.

Today, this is no longer the case. A wide range of entities engage in “banking” to some degree, and banks rely significantly on nonbanks to operate. Open banking adds to this trend. This decoupling of banks and banking raises a host of questions with regards to regulation and competition, some of which I’ve noted in past remarks.¹⁴

It also raises questions about culture. The culture of banking is small-c conservative. Because a bank’s greatest vulnerability is a loss of confidence, bank culture is defined by

¹² Refer to Bank for International Settlements, [“Big Tech vs Banks”](#) (August 2022).

¹³ Tabor, Nicholas K., Katherine E. Di Lucido, and Jeffery Y. Zhang. [“A Brief History of the U.S. Regulatory Perimeter.”](#) Board of Governors of the Federal Reserve System, February 8, 2021.

¹⁴ Acting Comptroller Michael J. Hsu, [“Safeguarding Trust in Banking: An Update.”](#) Remarks at the TCH + BPI Annual Conference, September 7, 2022; Acting Comptroller Michael J. Hsu, [“Leveling Up Banking and Finance.”](#) Remarks before the American Fintech Council, November 3, 2021.

stability, prudence, and governance. By contrast, the culture of the tech industry believes in disruption, “moving fast and breaking things,” and the superiority of code.

How these cultures coexist to promote open banking matters immensely. In the 1990s and early 2000s, the culture of banking and trading met, and trading won, setting the conditions for the 2008 financial crisis. (I know this from painful firsthand experience.)

In banking, trust is everything. It cannot be engineered or manufactured or bought. It must be earned, carefully maintained, and vigorously protected. An open banking culture that recognizes that and puts trust above other objectives, including growth and profit, will succeed and thrive over time.

My colleagues and I at the OCC are open-eyed and excited about what the future may bring. And we look forward to working with you as open banking and the banking system evolve.

Thank you.