european corporate governance institute

Banking, Technology, and Instability

Law Working Paper N° 901/2026
February 2026

Dan Awrey
Cornell University and ECGI

© Dan Awrey 2026. All rights reserved. Short sections of text, not to exceed two paragraphs, may be quoted without explicit permission provided that full credit, including © notice, is given to the source.

This paper can be downloaded without charge from:
https://doi.org/10.67929/ecgi-law-901-2026

european corporate governance institute

ECGI Working Paper Series in Law

Banking, Technology, and Instability

Working Paper N° 901/2026

February 2026

Dan Awrey

I would like to thank Yun-chien Chang, Ed Kitch, Takashi Kubota, and the participants of workshops organized by Cornell Law School, Waseda University, and the University of Virginia School of Law for their thoughtful comments and suggestions. All errors remain my own.

© Dan Awrey 2026. All rights reserved. Short sections of text, not to exceed two paragraphs, may be quoted without explicit permission provided that full credit, including © notice, is given to the source.

Abstract

The business of banking is under threat from the forces of technological disruption. Banks have long outsourced critical technology functions. Yet as technology has become more critical to the business of banking, a new breed of technology-driven "fintech" platforms have started to flip this conventional outsourcing script. Rather than banks outsourcing technology, these fintech platforms are instead outsourcing core elements of the banking franchise like deposit-taking, credit and debit card issuance, and payments. This "banking-as-a-service"—or BaaS—model is rooted in the comparative technological and organizational advantages these platforms enjoy over traditional banks. Yet it is also deeply rooted in regulatory arbitrage. This Article shines a spotlight on how the business model instability unleashed by the shift from conventional bank outsourcing to BaaS has contributed to growing instability in customer expectations regarding the scope of the financial safety net, and hence the legal protections to which these customers are entitled. It then explores how this combination of business model and expectations instability could trigger or amplify bank runs and, perhaps one day, even more widespread banking panics. The Article concludes by identifying and evaluating potential policy reforms targeting this triple cocktail of instability: ranging from relatively modest changes to bank recordkeeping requirements, to new liability rules for bank-fintech partnerships, to more fundamental reforms to the perimeter of bank regulation and the scope of the financial safety net.

Keywords: banks, banking, technology, banking-as-a-service, BaaS, financial regulation, financial stability, financial safety net, industrial organization, outsourcing

JEL Classifications: G20, G21, G23, G33, G38, K22, L22

Dan Awrey
Professor of Law
Cornell University, Cornell Law School
312 Myron Taylor Hall, Cornell Law School, Ithaca, New York 14853
Ithaca, New York 14853, United States
phone: + 1 607 882 1443
e-mail: aja288@cornell.edu

Banking, Technology, and Instability

Dan Awrey†

The business of banking is under threat from the forces of technological disruption. Banks have long outsourced critical technology functions. Yet as technology has become more critical to the business of banking, a new breed of technology-driven "fintech" platforms have started to flip this conventional outsourcing script. Rather than banks outsourcing technology, these fintech platforms are instead outsourcing core elements of the banking franchise like deposit-taking, credit and debit card issuance, and payments. This "banking-as-a-service"—or BaaS—model is rooted in the comparative technological and organizational advantages these platforms enjoy over traditional banks. Yet it is also deeply rooted in regulatory arbitrage.

This Article shines a spotlight on how the business model instability unleashed by the shift from conventional bank outsourcing to BaaS has contributed to growing instability in customer expectations regarding the scope of the financial safety net, and hence the legal protections to which these customers are entitled. It then explores how this combination of business model and expectations instability could trigger or amplify bank runs and, perhaps one day, even more widespread banking panics. The Article concludes by identifying and evaluating potential policy reforms targeting this triple cocktail of instability: ranging from relatively modest changes to bank recordkeeping requirements, to new liability rules for bank-fintech partnerships, to more fundamental reforms to the perimeter of bank regulation and the scope of the financial safety net.

TABLE OF CONTENTS

INTRODUCTION 2

I. WHY FIRMS OUTSOURCE 9

A. Contractability Problems 10

B. Comparative Advantages 14

C. Vertical Legal Constraints 16

D. Regulatory Arbitrage 17

II. THE RISE OF BANKING-AS-A-SERVICE 20

A. Conventional Bank-IT Outsourcing 21

B. The Banking-as-a-Service Model 26

† Beth and Marc Goldberg Professor of Law, Cornell Law School. I would like to thank Yun-chien Chang, Ed Kitch, Takashi Kubota, and the participants of workshops organized by Cornell Law School, Waseda University, and the University of Virginia School of Law for their thoughtful comments and suggestions. All errors remain my own.

III. BANKING WITHOUT A NET 31
A. The Conventional Financial Safety Net 31
B. The Regulation of Bank Outsourcing Relationships 34
C. BaaS and the Financial Safety Net 38
IV. OUTSOURCING INSTABILITY 43
A. Correlated Liquidity Demands 43
B. The New Shadow Intermediation Chains 46
C. The Threat of Information Contagion 48
V. OPTIONS FOR POLICY REFORM 49
A. Recordkeeping Reform 50
B. Liability Rules for Bank-Fintech Partnerships 52
C. Tighten the Financial Safety Net 53
D. Expand the Regulatory Perimeter 56
CONCLUSION 59

INTRODUCTION

If you only know one thing about banks and bank regulation, it's probably encapsulated by the statement "FDIC-Insured". For almost a century, this statement and others like it have been displayed at the entrance to every bank branch in America, on the desk at every teller window and, more recently, in the fine print on every bank TV commercial, smartphone app, and website.[1] This statement is designed to serve a single and incredibly important purpose: instilling depositors with confidence and trust in the safety and soundness of their bank and in the stability of the wider banking system.

The credibility of this statement is backed by some of the most sophisticated and costly legal engineering the world has ever seen. This engineering includes a combination of federal and state banking law, prudential regulatory frameworks imposing strict entry, activity, capital, liquidity, and other requirements, and ongoing examinations by federal bank supervisors.[2] Residing behind these legal, regulatory, and supervisory frameworks is then a comprehensive financial safety net that includes the Federal Reserve System's emergency lending facilities, a

[1] *See* 12. U.S.C. 1828(a)(1)(A); 12 CFR Part 328: FDIC Official Signs and Advertising Requirements, False Advertising, Misrepresentation of Insured Status, and Misue of the FDIC's Name or Logo, 89 Fed. Reg. 3528 (Jan. 18, 2024). Depending on the context, banks and other insured depository institutions can also use other statements such as "Member FDIC".

[2] *See* HOWELL JACKSON & MARGARET TAHYAR, *FINANCIAL REGULATION: LAW & POLICY*, 4TH ed. (2025), chapters 2.2-2.7, 6.1-6.3; RICHARD CARNELL, JONATHAN MACEY, GEOFFREY MILLER, & PETER CONTI-BROWN, *FINANCIAL INSTITUTIONS*. 7th ed. (2021), chapters, 3, 4, and 7 (both describing the onerous regulatory and supervisory frameworks to which banks are subject).

special bankruptcy or "resolution" framework for failing banks, and of course the Federal Deposit Insurance Corporation's (FDIC) deposit insurance program.[3] And residing behind this first safety net is a second and even more powerful backstop: the full faith and credit of the U.S. Government.[4] Viewed in this light, it is absolutely no exaggeration to say that the United States has thrown the full weight of its considerable legal, economic, and political resources behind the safety of U.S. banks and their depositors.

Almost a century after it was first woven together, this safety net is under threat from the forces of technological disruption. Banks have long outsourced critical technology functions. These functions include everything from accounting, customer relations management, and transaction processing, to website and mobile app development, cloud storage and computing power, and cybersecurity.[5] Importantly, this conventional bank-IT outsourcing model reflects a very specific division of labor: with technology firms providing the software, hardware, and technical expertise necessary to perform a wide range of "back office" functions, and chartered banks maintaining direct "front office" relationships with their depositors, borrowers, and other customers.

Yet as technology has become more critical to the business of banking, a new breed of technology-driven financial services—or "fintech"[6]—platforms has started to flip this conventional outsourcing script. Rather than banks outsourcing technology, these fintech platforms are outsourcing core elements of the banking franchise like deposit-taking, credit and debit card issuance, and payments to their partner banks.[7] This emerging "banking-as-a-

[3] *See* Gary Gorton & Andrew Metrick, *The Federal Reserve and Panic Prevention: The Roles of Financial Regulation and Lender of Last Resort*, 27:4 J. Econ. Perspectives 45 (2013); Mark Carlson & David Wheelock, "The Lender of Last Resort: Lessons from the Fed's First 100 Years," Fed. Reserve Bank of St. Louis Working Paper No. 2012-056B (2013)**;** Kathryn Judge, *Three Discount Windows*, 99 Cornell L. Rev. 795 (2014); Dan Awrey, *The Puzzling Divergence of the Lender of Last Resort Regimes in the U.S. and UK*, 45:3 J. Corp. L. 597 (2019) (all describing the evolution and use of the Federal Reserve's and other emergency lending facilities); FDIC, "About FDIC: What We Do," (May 15, 2020), https://www.fdic.gov/about/what-we-do/index.html; John Armour, "Making Bank Resolution Credible," in NIAMH MOLONEY, EILÍS FERRAN & JENNIFER PAYNE (EDS.), *THE OXFORD HANDBOOK OF FINANCIAL REGULATION* 453 (2015) (both describing the rationale and mechanics of the FDIC's resolution framework for banks). *See also* JACKSON & TAHYAR, *supra* note __, chapters 9.1-9.2 and CARNELL, MACEY, MILLER & CONTI-BROWN, *supra* note __, chapter 8 (both describing the various policy tools that U.S. bank regulators use to reduce the probability and impact of bank failure).

[4] *See* 12 U.S.C. §1828(a)(1)(B) (requiring FDIC deposit insurance signage displayed by banks to include a statement that insured deposits are backed by the full faith and credit of the United States Government). *See also* FDIC, "Understanding Deposit Insurance" (Apr. 1, 2024), https://www.fdic.gov/resources/deposit-insurance/understanding-deposit-insurance ("The [Deposit Insurance Fund] is backed by the full faith and credit of the United States government").

[5] *See* Section II.A *infra.*

[6] For a general introduction to fintech business models and regulation, see ROSS BUCKLEY, DOUGLAS ARNER & DIRK ZETZSCHE, *FINTECH: FINANCE, TECHNOLOGY AND REGULATION* (2024). *See also* Chris Brummer & Yesha Yadav, *Fintech and the Innovation Trilemma*, 107:2 Georgetown L. J. 235 (2019); Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. Rev. 232 (2018); Thomas Philippon, "The Fintech Opportunity," Bank for International Settlements Working Part No. 655 (2017).

[7] *See* Robert Hockett & Saule Omarova, *The Finance Franchise*, 102 Cornell L. Rev. 1143 (2017) (coining the term "finance franchise" to describe the public-private partnership between the government and chartered

service"[8] or BaaS model is effectively an inversion of conventional bank-IT outsourcing relationships: with fintech platforms instead of chartered banks outsourcing key back office functions and assuming a critical customer-facing role.

By just about any measure, this BaaS model is rapidly growing in both popularity and importance. In 2022, researchers at the Office of the Comptroller of the Currency (OCC), the federal banking agency responsible for chartering national banks, estimated that there were at least 10 banks that had entered into more than 50 fintech partnerships.[9] Today, while available data is still scare and highly fragmented, estimates suggest there are now hundreds of BaaS partner banks,[10] each typically serving dozens of fintech platforms,[11] and collectively holding hundreds of billions of dollars in assets.[12] And while many of the fintech platforms these banks serve are still relatively small, some of the largest platforms—like the digital banking app Chime—hold billions of dollars in customer funds through their partner banks.[13] Ultimately, all these partner banks, fintech platforms, and deposits add up: with some estimates forecasting that the revenue generated by BaaS will grow tenfold between 2021 and 2026, from

banks, along with their respective roles in supporting socially useful functions like money and payments). *See also* MORGAN RICKS, *THE MONEY PROBLEM: RETHINKING FINANCIAL REGULATION* (2016) and Lev Menand, *Why Supervise Banks? The Foundations of the American Monetary Settlement*, 74 Vand. L. Rev. 951 (2021) (both framing bank chartering and regulation in broadly similar terms).

[8] As of writing, there has still been relatively limited scholarly treatment of BaaS. For a detailed introduction to the BaaS business model, *SEE* JASON MIKULA, *BANKING AS A SERVICE: OPPORTUNITIES, CHALLENGES, AND RISKS OF NEW BANKING BUSINESS MODELS* (2024). For some of the emerging scholarly literature on BaaS, *see e.g.* Nydia Remolina, "From Open Banking to Banking-as-a-Service: Regulatory Challenges in the Evolution of Financial Intermediation," Singapore Management University Yong Pung How School of Law Working Paper (September 2025); Braeden Hodges, *Banking-as-a-Service: FinTechs Walking the Regulatory Perimeter*, 17:2 Brooklyn J. Corp., Fin. & Comm. L. 127 (2023); Luca Enriques & Georg Ringe, *Bank-Fintech Partnerships, Outsourcing Arrangements and the Case for a Mentorship Regime*, 15:4 Capital Markets L. Rev. 374 (2020).

[9] *See* Acting Comptroller of the Currency Michael Hsu, "Safeguarding Trust in Banking: An Update," Remarks at the TCH+BPI Annual Conference (Sept. 7, 2022), https://www.occ.gov/news-issuances/speeches/2022/pub-speech-2022-106.pdf.

[10] *See e.g.* Yishu Wang & Thomas Mason, "Small Group of Banking-as-a-Service Banks Logs Big Number of Enforcement Actions," S&P Global Market Intelligence (Jan. 23, 2024), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/small-group-of-banking-as-a-service-banks-logs-big-number-of-enforcement-actions-80067110 ("it is estimated that fewer than 100 community banks are in the business of BaaS"). In contrast, the U.S. Treasury Department, looking beyond community banks, and adopting a somewhat broader definition of fintech partnerships, has estimated that two thirds of all insured depository institutions entered into fintech partnerships between 2018 and 2021; U.S. Department of the Treasury, "Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets," Report to the White House Competition Council 28 (Nov. 2022), https://home.treasury.gov/system/files/136/Assessing-the-Impact-of-New-Entrant-Nonbank-Firms.pdf.

[11] *See* MIKULA, *supra note* __, at 122 ("BaaS banks typically do not have just one or two fintech partners, but rather would be supporting dozens of programs").

[12] *Id.,* at 120.

[13] *Id.*

roughly $1.7 billion to over $17 billion.[14] There is no doubt that BaaS is increasingly big business. The question is whether it's a big problem.

There is no easy or straightforward answer to this question. The principal reason is that there are two critical and opposing drivers behind the rise of BaaS. The first driver reflects ongoing structural changes in customer demand and, specifically, the desire for faster, cheaper, more seamless, and more convenient digital banking experiences.[15] In the United States, traditional banks have often been relatively slow in responding to these changes. While the reasons for this vary from bank to bank, many smaller community banks have been reluctant to make large scale capital investments in the type of modern web-based technology platforms that would enable them to provide the full range of internet banking, mobile banking, and payment products that their customers now increasingly demand.[16] At the other end of the spectrum, the scale, organizational complexity, and entrenched bureaucracy of many larger banks have made it difficult for them to keep pace with the rapid technological changes unleashed over the past quarter century.[17] Whatever the underlying reasons, the resulting underinvestment has opened the door for fintech platforms to exploit both their comparative technological advantages and more nimble organizational structures to meet this growing demand and, in the process, drive the shift from conventional bank-IT outsourcing toward the BaaS model.

In theory, this customer-driven shift from conventional bank-IT outsourcing to BaaS should have no impact whatsoever on the application of federal bank regulation, the scope of the financial safety net, or the stability of the U.S. banking system. As a consequence, customers should not be exposed to fundamentally different risks depending on whether their bank outsources critical technology functions or their fintech platform outsources core elements of the banking franchise. Yet in practice, that is often exactly what it means. Most

---

[14] *See e.g.* MasterCard, "Open, Embedded, Modular, and on a Platform: The Opportunities of Banking as a Service" 3 (2022) [on file with author] (citing a report from Juniper Research forecasting that BaaS revenue will reach $17.3 billion by 2026). *See also* Letter from Senators Elizabeth Warren and Chris Van Hollen to Martin Gruenberg, Chairman of the FDIC, Michael Hsu, Acting Comptroller of the Currency, and Michael Barr, Vice Chair for Supervision, Federal Reserve Board of Governors (Sept. 11, 2024) [on file with author] ("BaaS revenue alone is expected to rise tenfold, from $1.7 billion in 2021 to over $17.3 billion in 2026, and the risks to consumers will rise accordingly.") [internal citations omitted].

[15] *SEE* DAN AWREY, *BEYOND BANKS: TECHNOLOGY, REGULATION, AND THE FUTURE OF MONEY* (2024) (describing this shift in consumer demand and the failure of many traditional banks to effectively respond to it).

[16] *See e.g.* Conference of State Banking Supervisors, Annual Survey of Community Banks (Oct. 7, 2025), https://www.csbs.org/sites/default/files/other-files/2025CBSurvey_web_CSBS.pdf (reporting that 78 percent of surveyed banks identified the *cost of technology* as either an "extremely important" or "very important" external risk, with over 60 percent separately identifying the *speed of technology*).

[17] *SEE* AWREY, *BEYOND BANKS*, *supra* note __, at 120 ("This is especially the case for many larger banks that have grown through mergers and acquisitions, which have often been forced to grapple with the enormous complexity and costs of managing a patchwork of legacy information systems"). To take just one example, Citigroup was recently forced to allocate more than 30,000 staff members to addressing lingering IT integration issues; see David Benoit, "Federal Reserve Wants Citigroup to Move Faster to Fix Problems with Its Risk Systems," *WALL STREET JOURNAL* (Sept. 15, 2022).

importantly, as a growing number of fintech customers are now starting to learn, the bankruptcy of a fintech platform can leave them struggling to recover their hard-earned money—even when that money is held with an FDIC-insured partner bank.[18]

This in turn highlights the second critical driver behind the rise of the BaaS model: *regulatory arbitrage*. As a starting point, obtaining a bank charter, paying FDIC deposit insurance premiums, and ensuring ongoing compliance with bank activity, capital, liquidity, risk management, and other regulations is extremely costly.[19] By outsourcing the core elements of the banking franchise, fintech platforms exploiting the BaaS model can replicate many of the financial products and services provided by banks, but without the need to incur these significant and ongoing costs. Accordingly, as this divergence in regulatory compliance costs becomes more pronounced, we should expect to observe an increase in the number of firms forgoing a traditional bank charter in favor of the BaaS model.

The hydraulic effects of regulatory arbitrage are further compounded by the fact that the BaaS model does not fall squarely within the scope of the regulatory framework currently governing conventional bank-IT outsourcing relationships. The twin cornerstones of this framework are the Federal Reserve Board, OCC, and FDIC Interagency Guidance on Third-Party Relationships[20] and the Bank Service Company Act of 1962 (BSCA).[21] The Interagency Guidance sets out broad principles that banks should follow when managing their relationships with technology firms and other third party service providers.[22] Importantly, the Interagency Guidance makes it clear that banks are ultimately responsible for any conduct by these service providers that harms customers or violates federal banking law. Operating in parallel, the BSCA envisions that these service providers may themselves be brought under the direct prudential regulation and supervision of federal banking agencies.[23] Together, the Interagency Guidance and BSCA have arguably played a useful role in addressing the risks stemming from conventional bank-IT outsourcing relationships. Yet they were clearly designed for a world in which banks were the orchestrators of these outsourcing relationships, the sole recipients of outsourced services, and at all times maintained direct customer-facing relationships. Put simply: they were not made for the brave new world of BaaS.

---

[18] *See* Section III.C *infra*.

[19] While reliable data is somewhat scarce, it has been estimated that the biggest banks can spend over $1 billion a year on regulatory compliance; see Peter Farley, "Spotlight on Compliance Costs as Banks Get Down to Business with AI," *INTERNATIONAL BANKER* (Jul. 4, 2017). At the other end of the spectrum, regulatory compliance also represents a significant component of the total operating costs for smaller community banks; see Drew Dahl, Andrew Meyer, & Michelle Clark Neeley, "Scale Matters: Community Banks and Compliance Costs," Federal Reserve Bank of St. Louis (Jul. 14, 2016) (describing the results of a survey conducted by the Federal Reserve Bank of St. Louis that found that, on average, regulatory compliance costs represent 8.7 percent of the noninterest expenses of banks with assets under $100 million).

[20] Federal Reserve Board, OCC, and FDIC, Interagency Guidance on Third-Party Relationships: Risk Management, 88:111 Fed. Reg. 37920 (Jun. 9, 2023) [hereinafter, the "Interagency Guidance"].

[21] 12 U.S.C. 1861 *et seq*.

[22] *See* Section III.B *infra* for a more detailed description of the Interagency Guidance.

[23] *See* Section III.B *infra* for a more detailed description of the BSCA.

The collision of these two drivers exposes a fundamental tension at the heart of the BaaS model. On the one hand, to the extent that the rise of BaaS reflects a market-driven response to ongoing technological shocks, shifting customer demand, and the failure of incumbent banks to adapt to these rapidly unfolding changes, its emergence and growth hold out potentially significant benefits for competition and innovation within the financial services industry and, ultimately, for consumer choice. On the other hand, to the extent that this growth is fueled by the hydraulic effects of regulatory arbitrage, the rise of BaaS outside the perimeter of bank regulation and the conventional financial safety net poses clear and mounting risks for consumers, for microprudential safety and soundness and, perhaps one day, for financial stability.

This Article chronicles the shift from conventional bank-IT outsourcing to BaaS and identifies the three intertwined types of instability it potentially creates. The first type—*business model instability*—stems from the inversion of conventional bank-IT outsourcing relationships and the corresponding need to address the unique policy, legal, technological, and operational risks posed by the rise of the BaaS model. The second—*expectations instability*—stems from the risk that this business model instability can confound the expectations that the customers of fintech platforms have regarding the scope of FDIC deposit insurance and other elements of the financial safety net and, hence, the legal protections to which they are entitled in the event of a platform's bankruptcy. The third—*financial instability*—reflects the risk that the continued growth of the BaaS model, the complex and opaque interconnections it creates, and its impact on customer behavior could potentially sow the seeds of future banking panics. Together, these three intertwined sources of instability are already stretching the fabric of the banking system. One day soon, they may tear it.

Having described this triple-cocktail of potential instability, this Article goes on to explore the challenges and tradeoffs that policymakers will inevitably face should they seek to address it. The first and perhaps most obvious option is for policymakers to tighten the regulatory perimeter by restricting the ability of banks to outsource core elements of the banking franchise. Yet while this would almost certainly succeed in killing the BaaS model, it would also undercut consumer choice, reduce competition and, by protecting incumbent banks, exacerbate the well-known "too-big-to-fail" problem.[24] At the other end of the spectrum, policymakers could embrace BaaS by incorporating fintech platforms into the conventional financial safety net. However, while this would almost certainly enhance consumer protection, it would also demand that policymakers design and implement entirely new regulatory and supervisory frameworks governing a vast, diverse, and still expanding universe of fintech platforms. Should these frameworks be poorly designed or calibrated, this could both undermine ongoing technological experimentation and amplify latent moral hazard problems. Viewed together, these options put policymakers between a rock and a hard place.

---

[24] *See* Maureen O'Hara & Wayne Shaw, *Deposit Insurance and Wealth Effects: The Value of Being 'Too Big to Fail'*, 45 J. Fin. 1587–1601 (1990) (defining the too-big-to-fail problem and quantifying the resulting funding subsidy). Two decades later, the concept of too-big-to-fail would play a central role in the narrative around the global financial crisis; see e.g. ANDREW ROSS SORKIN, *TOO BIG TO FAIL: THE INSIDE STORY OF HOW WALL STREET AND WASHINGTON FOUGHT TO SAVE THE FINANCIAL SYSTEM—AND THEMSELVES* (2010).

And yet if policymakers do nothing, the combination of strong customer demand, the comparative advantages enjoyed by many fintech platforms, and the hydraulic effects of regulatory arbitrage will continue to drive the growth of BaaS—putting more and more customers and their money at risk.

The rise of BaaS is ultimately an important plotline in a far bigger story about the complex and evolving relationship between finance, technology, and regulation. From BaaS to fintech, artificial intelligence to crypto, new technology has triggered a tectonic shift in the financial landscape. This shift has placed growing pressure on the perimeter of financial regulation: including foundational legal categories like "banks" and "banking," "securities," "futures contracts," and "insurance".[25] In the process, this shift has further blurred the already fuzzy legal boundaries that demarcate the scope of the conventional financial safety net. In many ways, the rise of BaaS is simply a microcosm of this bigger story. Yet for precisely this reason, it also holds out important insights about both the complex and often contradictory drivers of this shift and how policymakers can effectively respond to it.

This Article proceeds as follows. Drawing on key insights from industrial organization, law and economics, and corporate law, Section I identifies and describes the core economic rationales for business outsourcing: including contractability problems, comparative advantages, vertical legal constraints, and regulatory arbitrage. Section II traces the emergence and evolution of conventional bank-IT outsourcing relationships, along with the recent rise of the BaaS model. Importantly, while both of these outsourcing models reflect well-understood contractability problems and pronounced comparative advantages, the BaaS model is also deeply rooted in regulatory arbitrage. Section III describes both the current financial safety net protecting banks and their depositors and the regulatory framework governing bank outsourcing relationships. Using the recent bankruptcy of Synapse Financial Technologies as a case study, it then demonstrates how the BaaS model falls largely outside the scope of these regulatory frameworks, exposing customers to risks that stand fundamentally at odds with their expectations regarding the scope of FDIC deposit insurance and other elements of the financial safety net. Section IV describes how the continued growth of the BaaS model, its complexity and opacity, and its impact on customer behavior could one day contribute to both destabilizing bank runs and broader banking panics. Section V concludes by identifying and evaluating potential policy reforms targeting the instability at the heart of the BaaS model: ranging from relatively modest changes to bank recordkeeping requirements, to new liability rules for bank-fintech partnerships, to more fundamental reforms to the perimeter of bank regulation and the financial safety net.

[25] *See e.g.* Katherine Lucido, Nick Tabor & Jeffery Zhang, *Fenceposts Without a Fence*, 76 Vand. L. Rev. 1215 (2023) (unpacking the concept of a regulatory "perimeter," how it is operationalized in the context of U.S. banking regulation, and how new technology has exposed its weaknesses); Howell Jackson, "The Nature of the Fintech Firm and its Implications for Financial Regulation" in HOWELL JACKSON & MARGARET TAHYAR (EDS.), *FINTECH LAW: THE CASE STUDIES* 9 (2020) (examining how changes unleashed by financial technology "raise challenging questions as to the appropriate contours of regulatory perimeters").

I. WHY FIRMS OUTSOURCE

To understand the opportunities and risks presented by the rise of BaaS, it is helpful to first understand the key drivers of business outsourcing. The question of why firms outsource has long been one of the central obsessions of industrial organization,[26] law and economics,[27] and corporate law.[28] On an elemental level, a firm is simply a collection of inputs—capital, labor, technology, real and intellectual property, and other raw materials—coordinated under common ownership. For any given firm, some of these inputs will be produced by the firm itself, while others will be purchased on the open market or pursuant to longer term supply contracts. To take just one example, while Apple's internal design team is responsible for the distinctive look and feel of the iPhone, iPad, and MacBook, the firm outsources the vast majority of its manufacturing to firms like Foxconn, Micron, and Taiwan Semiconductor (TSMC). Similarly, most of the apps available in the Apple Store are developed by independent software firms and engineers. This raises an important question: what factors determine whether a firm like Apple organizes production of a given input internally or outsources it to other firms in the marketplace? For legal scholars and economists following in the Coasian tradition, this question is a typically framed as an exploration of the efficient

[26] *See e.g.* Daron Acemoglu, Simon Johnson & Todd Mitton, *Determinants of Vertical Integration: Financial Development and Contracting Costs*, 64:3 J. Fin. 1251 (2009); Benjamin Klein, *Fisher–General Motors and the Nature of the Firm*, 43 J. Law & Econ. 105 (2000); Richard Caves & Ralph Bradburd, *The Empirical Determinants of Vertical Integration*, 9 J. Econ. Behavior & Org. 265 (1988); Paul Joskow, *Asset Specificity and the Structure of Vertical Relationships: Empirical Evidence*, 4 J. Law, Econ. & and Org. 95 (1988); Benjamin Klein, *Vertical Integration as Organized Ownership: The Fisher Body–General Motors Relationship Revisited*, 4 J. Law, Econ. & Org. 199–213 (1988); Paul Joskow, *Vertical Integration and Long Term Contracts: The Case of Coal-Burning Electric Generating Plants*, 1 J. Law, Econ. & Org. 33 (1985); Benjamin Klein, Robert Crawford & Armen Alchian, *Vertical Integration, Appropriable Rents, and the Competitive Contracting Process*, 21 J. Law & Econ. 297 (1978).

[27] There are two parallel and, in many respects, complementary schools of thought in law and economics regarding the determinants of vertical integration and, by implication, outsourcing. The first is the "transaction cost" school pioneered by Ron Coase, Oliver Williamson, and others; *see e.g.* Ronald Coase, *The Nature of the Firm*, 4 Econometrica 386 (1937); OLIVER WILLIAMSON, *MARKETS AND HIERARCHIES: ANALYSIS AND ANTITRUST IMPLICATIONS* (1975), and Oliver Williamson, *Transaction-Cost Economics: The Governance of Contractual Relationships*, 22:2 J. Law & Econ. 233 (1979). *See also* Ian MacNeil, *The Many Futures of Contract*, S. Cal. L. Rev. 691 (1973-1974). The second is the "property rights" school developed by economists including Oliver Hart, John Moore, and Sanford Grossman; *see e.g.* Sanford Grossman & Oliver Hart, *The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration*, 94:4 J. Pol. Econ. 691 (1986) and Oliver D. Hart & John Moore, *Property Rights and the Nature of the Firm*, 98:6 J. Pol. Econ. 1119 (1990). For a scholarly treatment comparing both schools, see Michael Whinston, *Assessing the Property Rights and Transaction-Cost Theories of the Firm*, 91:2 Am. Econ. Rev. 184 (2001).

[28] *SEE E.G.* FRANK EASTERBROOK AND DANIEL FISCHEL, *THE ECONOMIC STRUCTURE OF CORPORATE LAW* 8-15 (1991).

boundaries of the firm.[29] For a firm's managers, it often boils down to the quintessential business decision of whether to *make or buy*.[30]

A. Contractability Problems

Outsourcing patterns vary significantly from industry to industry, from firm to firm, and from input to input.[31] So what accounts for these different patterns? There are several key factors. The first is *contractability*. The concept of contractability can be traced back to the prediction, first articulated by economist Ronald Coase, that a firm will outsource production where the transaction costs of producing a given input internally are greater than the transaction costs of purchasing it in the marketplace.[32] Where production takes place within a firm, these transaction costs include the costs of coordinating the flow of information and other resources, monitoring the firm's managers, employees, and others agents, and incentivizing these agents to exert maximum effort and make decisions that increase the value of the firm.[33] In effect, these costs reflect the size and complexity of the bureaucratic machinery

[29] Coase, *supra* note __, at 393-394 ("The question which arises is whether it is possible to study the forces which determine the size of the firm. Why does the entrepreneur not organize one less transaction or one more?").

[30] *SEE E.G.* ROBERT NEWTON ANTHONY, *MANAGEMENT CONTROL SYSTEMS* (1965) (first introducing the "make-or-buy" framing). *See also* Gordon Walker & David Weber, *A Transaction Cost Approach to Make-or-Buy Decisions*, 29:3 Admin. Sci. Q. 373 (1984) (explicitly connecting the "make-or-buy" decision to transaction cost considerations).

[31] As Coase observed in 1937: "the amount of vertical integration, involving as it does the supersession of the price mechanism, varies greatly from industry to industry and from firm to firm."; Coase, *supra* note __, at 388-389. *See also* Acemoglu, Johnson & Mitton, *supra* note __ (exploring the different patterns of vertical integration and outsourcing across countries).

[32] *See* Coase, *supra* note __, at 394 ("Naturally, a point must be reached where the costs of organising an extra transaction within the firm are equal to the costs involved in carrying out the transaction in the open market"); Oliver E. Williamson, *The Vertical Integration of Production: Market Failure Considerations*, 61:2 Am. Econ. Rev. 112, 113 (1971) ("As the frictions associated with administrative coordination [i.e. firms] become progressively more severe, recourse to market activities becomes more attractive"); Grossman and Hart, *supra* note __, at 691 ("When it is costly to list all the specific rights over assets in the contract, it may be optimal to let one party purchase all the residual rights"). Of course, "markets" and "firms" are ultimately only two points at opposite ends of a diverse spectrum; *see* Joskow, *supra* note __, at 97 ("The boundary between a firm and a market provides a very rough distinction between the two primary institutional mechanisms for allocating resources, but this is the beginning, not the end, of the inquiry. Firms can take on many different organization structures. Market transactions can take many different forms ranging from simple spot market transactions to complex long-term contracts. The specific set of institutional arrangements chosen would represent the governance structure that minimized the total cost of consummating the transactions of interest.").

[33] *See e.g.* Kenneth Arrow, *Vertical Integration and Communication*, 6:1 Bell J. Econ. 173 (1975) (arguing that *intra*-firm communication may be less costly than *inter*-firm communication); Bengt Holmström, & Paul Milgrom, *The Firm as an Incentive System*, 84 Am. Econ. Rev. 972 (1994) (demonstrating that firms can use a variety of mechanisms to incentivize managers, employees, and other agents); Williamson (1971), *supra* note __, at 114 ("The firm may also resort to internalization on account of economies of information exchange… It is widely accepted, for example, that communication with respect to complex matters is facilitated by a common training and experience and if a compact code has developed in the process. Repeated interpersonal interactions may

needed to run a firm, along with the corresponding need to ensure that the individual cogs within this machinery are working in lockstep to advance the firm's objectives.

Where a firm instead decides to outsource production of an input, the nature of these transaction costs fundamentally changes. Reflecting the shift from a bureaucratic to a more market-oriented model, these transaction costs include the costs of determining the prevailing market price for the input, writing legally binding contracts that set out the rights and obligations of the buyer and seller and, at least in the context of longer term relationships, periodically renegotiating these contracts in response to changing circumstances or new information.[34] They also include the costs of monitoring and, if necessary, enforcing compliance with these contracts.[35] Where the costs of writing, monitoring, and enforcing these incomplete contracts are relatively high, the resulting contractability problems will make it more likely that firms will decide to produce a given input internally. Conversely, where these costs are relatively low, firms may find it more desirable to outsource production.

These contractability problems are likely to be particularly acute in the presence of two additional and related factors. The first is *technological uncertainty*. As first explained by Frank Knight, a future event is uncertain if the probability of its occurrence is not technically susceptible to measurement.[36] Thus for example, if you were to ask a statistician at the dawn of the twentieth century to place a wager on whether the internet would be invented at some point over the next 100 years, they would have absolutely no way of calculating the probability of this event. Importantly, the reason for their lack of foresight would have nothing to do with the ever present challenges of predicting the future, but rather because the very concept of the internet would not yet exist. In fact, under these circumstances, to write a complete contract memorializing this wager, including the precise conditions under which the statistician would be entitled to payment, would be tantamount to inventing the internet!

As this example illustrates, technological shocks can be an important source of Knightian uncertainty and, hence, contractual incompleteness.[37] In industries where these

---

permit even further economies of communication"). *See also* Margaret Blair, Erin O'Hara O'Connor & Gregg Kirchhoefer, *Outsourcing, Modularity, and the Theory of the Firm*, 2011:2 BYU L. Rev. 263, 286 (2011) (observing that contractability may be impacted where relationships between firms are characterized by "thick" crossing points for the transfer of information).

[34] *See* Coase, *supra* note __, at 390 ("The most obvious cost of 'organising' production through the price mechanism is that of discovering what the relevant prices are."); Grossman & Hart, *supra* note __ (describing how the transaction costs of writing complex state-contingent contracts result in incomplete contracting), and Oliver Hart & John Moore, *Incomplete Contracts and Renegotiation*, 56:4 Econometrica 755 (1988) (describing the dynamics of renegotiating complex state-contingent contracts).

[35] *See* Grossman & Hart, *supra* note __ and Hart & Moore, *supra* note __ (both describing the costs of observing and verifying contractual compliance to courts and other third-party dispute resolution mechanisms). For a more general discussion of these observation and verification costs, see Albert Choi & George Triantis, *Completing Contracts in the Shadow of Costly Verification*, 37:2 J. Legal Stud. 503 (2008).

[36] FRANK KNIGHT, *RISK, UNCERTAINTY, AND PROFIT* (1921).

[37] *See* Tim Holcomb & Michael Hitt, *Toward A Model of Strategic Outsourcing*, 25 J. Op. Man. 464, 472 (2007); Michael Song & Mitzi Montoya-Weiss, *The Effect of Perceived Technological Uncertainty on Japanese New Product Development*, 44:1 Aca. Man. J. 61 (2001); Thomas Robertson & Hubert Gatignon, *Technology Development Mode: A*

shocks are relatively common, the resulting disruption, uncertainty, and contractability problems can drive firms to outsource the production of technologically sensitive inputs.[38] There are two intertwined rationales for this type of "strategic"[39] outsourcing. First, anticipating future shocks, firms may seek to shift some or all of the inevitable costs of adapting their products, services, and production processes onto their suppliers.[40] Second, these suppliers may ultimately be in a better position to bear these costs: typically because of economies of specialization, scale, or the ability to amortize them across a large number of customers.[41] Returning to our earlier example, Apple's decision to outsource the design and manufacturing of the microchips used in its products to firms like Micron and TSMC thus likely reflects both the desire to shift the risks of technological uncertainty and the comparative advantages that these large, hyper-specialist suppliers enjoy in anticipating and responding to these risks.

The second factor is the presence of *asset specificity* in the relationship between firms and their suppliers and the corresponding threat of strategic behavior.[42] Asset specificity is a function of the difference between the value of an input used for its *intended* purpose relative to its *next best* purpose.[43] All other things being equal, it is often desirable for a firm to obtain inputs designed specifically for use in its own products and services. This requires the firm's suppliers to make investments in the development and production of these specialized inputs. Thus, for example, enterprise software developers like SAP, Oracle, and Salesforce are often asked to design more bespoke applications to meet the needs of different clients. Likewise,

---

Transaction Cost Conceptualization, 19:6 Strat. Man. J. 515 (1998); Timothy Folta, *Governance and Uncertainty: The Tradeoff Between Administrative Control and Commitment*, 19:11 Strat. Man. J. 1007 (1998); David Teece, *Economies of Scope and the Scope of the Enterprise*, 1:3 J. Econ. Beh. & Org. 223 (1980).

[38] *See* Williamson (1971), *supra* note __, at 115-116 ("The [contractability] problem is made even more severe where a changing technology poses production redesign issues. Here it is doubtful that, despite great effort and expense, contractual efforts reasonably to comprehend the range of possible outcomes will be successful").

[39] Holmcolm & Hitt, *supra* note __, at 472.

[40] *Id.* ("In the presence of technological uncertainty, greater resource commitments produce more exposure to negative shocks. Thus, relative to arrangements that provide on-demand access to capabilities through intermediate markets, technological uncertainty may serve as a disincentive to internalize because it often requires greater resource commitments. These conditions may prompt firms to pursue strategic outsourcing to reduce their exposure to unforeseen contingencies and to improve financial and operational stability and predictability.") [internal quotations omitted].

[41] *Id.* ("Specialized firms in these markets may be better able to achieve cost efficiencies that are difficult for focal firms to achieve by balancing task requirements across multiple customers. As such, strategic outsourcing not only can provide scale economies during periods of technological uncertainty, but may also act as a coping strategy helping to deal with risk.").

[42] OLIVER WILLIAMSON, *THE ECONOMIC INSTITUTIONS OF CAPITALISM* 55 (1985) (defining asset specificity as "durable investments that are undertaken in support of particular transactions, the opportunity cost of which investments is much lower in best alternative uses or by alternative users should the original transaction be prematurely terminated"). Williamson identifies four different types of asset specificity: site, physical asset, human asset, dedicated asset specificity; see Oliver Williamson, *Credible Commitments: Using Hostages to Support Exchange*, 73 Am. Econ. Rev. 519 (1983).

[43] *Id.*

automotive parts suppliers modify their parts to meet the unique specifications of individual car manufacturers and models. Almost by definition, these specialized inputs will be more valuable to the firm than any substitutes available on the open market. In theory, this difference in value generates a surplus that can then be shared by both the firm and its specialist suppliers.

Yet while firms and their suppliers may have a joint long-term interest in maximizing the value of this surplus, they would both obviously prefer to capture as much of this surplus as possible for themselves. This introduces the prospect of strategic behavior, more commonly known as "hold-up".[44] As a supplier designs inputs for use by a specific firm, and as the firm's products and services become reliant on these specialized inputs, the resulting asset specificity can result in a degree of mutual dependence. Especially in the presence of contractability problems and incomplete contracting, this dependence can expose one or both parties to hold-up.[45] Specifically, when circumstances change in ways that tip the balance of power in their favor, one party may seek to leverage this change to renegotiate the economics of their relationship to secure a larger share of the surplus. Faced with the prospect of losing the entire value of their asset-specific investments, the other party may then have little choice but to agree to the new terms.

The threat of hold-up has two important implications for firm outsourcing patterns. First, where the degree of asset specificity is relatively high, firms may rationally respond to the corresponding threat of hold-up by internalizing the production of the relevant inputs.[46] Second, and conversely, where the degree of asset specificity is relatively low, the absence of a credible threat of hold-up makes it more likely that firms will be comfortable outsourcing production. While definition and measurement problems abound,[47] problems of asset specificity and hold-up have been found to have played an influential role in the level of vertical

---

[44] *See* WILLIAMSON, *MARKETS AND HIERARCHIES*, *supra* note __; Williamson, *Transaction-Cost Economics*, *supra* note __, and Klein, Crawford, and Alchian, *supra* note __ (each describing and analyzing hold-up problems).

[45] *See* Bengt Holmstrom & Paul Milgrom, *Multitask Principal-Agent Analysis: Incentive Contracts, Asset Ownership, and Job Design*, 7 J. L. Econ. & Org. 24 (1991); Bengt Holmstrom & John Roberts, *The Boundaries of the Firm Revisited*, 12 J. Econ. Persp. 73 (1998); Klein et al., *supra* note __; Williamson (1979), *supra* note __; Grossman & Hart, *supra* note __, at 692.

[46] *See* Oliver Williamson, *Outsourcing: Transaction Cost Economics and Supply Chain Management*, 44:2 J. Supply Chain Man. 5, 5 (2008) ("as bilateral dependency builds up, the efficient governance of contractual relations progressively moves from simple market exchange to hybrid contracting (with credibility supports) to hierarchy); Joskow, *supra* note __, at 105 ("Other things equal, we expect the parties to more frequently choose vertical integration or a long-term contract as the quasi-rents associated with specific investments become more important and the associated benefits of precommitment increase.")

[47] *See* Peter Klein, "The Make-or-Buy Decision: Lessons from Empirical Studies," University of Missouri Contracting and Organizations Research Institute Working Paper No. 2004-07 21-27 (Apr. 2004) (describing definitional and measurement problems in the empirical literature on asset specificity).

integration—and hence outsourcing patterns—in a wide range of industries: from aerospace[48] and electricity generation,[49] to oil and gas,[50] trucking,[51] and forestry.[52]

B. Comparative Advantages

A second key factor driving outsourcing decisions is whether a firm or its suppliers enjoy a durable comparative advantage in the production of the relevant inputs. The concept of comparative advantage is closely linked with what has become known as the "resource-based" view of the efficient boundaries of the firm. This resource-based view looks beyond Coasian transaction costs to identify the precise conditions under which firms can develop, nurture, combine, and exploit resources and capabilities more efficiently than both markets and, importantly, *other firms*.[53] As explained by management theorist Margaret Peteraf, the resource-based view thus conceptualizes the firm as a "bundle" of resources and capabilities that vary from firm to firm and which, if combined in specific ways, can generate a competitive

[48] *See* Scott Masten, *The Organization of Production: Evidence from the Aerospace Industry*, 27 J. L. & Econ. 403 (1984).

[49] *See* Stéphane Saussier, *Transaction Costs and Contractual Incompleteness: The Case of Electricitie de France*, 42 J. Econ. Behavior & Org. 189 (2000); Victor Goldberg & John Erickson, *Quantity and Price Adjustment in Long-Term Contracts: A Case Study of Petroleum Coke*, 30 J. L. & Econ. 369 (1987); Joskow, *Vertical Integration and Long Term Contracts*, *supra* note __.

[50] *See* Paul Hallwood, *On Choosing Organizational Arrangements: The Example of Offshore Oil Gathering*, 38 Scottish J. Pol. Econ. 227 (1991).

[51] *See* Jackson Nickerson, & Brian Silverman. *Why Aren't All Truck Drivers Owner-Operators? Asset Ownership and the Employment Relation in Interstate For-Hire Trucking*, 12 J. Econ. & Man. Strat. 91 (2003).

[52] *See* Steven Globerman, & Richard Schwindt, *The Organization of Vertically Related Transactions in the Canadian Forest Products Industries*, 7 J. Econ. Behavior & Org. 199 (1986).

[53] *See e.g.* Kathleen Connor, *A Historical Comparison of Resource-based Theory and 5 Schools of Thought Within Industrial Organization Economics: Do We Have a New Theory of the Firm*, 17(1) J. Management 121 (1991); Jay Barney, *Firm Resources and Sustained Competitive Advantage*, 17(1) J. Man. 99 (1991); Margaret Peteraf, *The Cornerstones of Competitive Advantage: A Resource Based View*, 14:3 Strat. Man. J. 179 (1993); Sumantra Ghoshal & Peter Moran, *Bad for Practice: A Critique of the Transaction Cost Theory*, 21(1) Academy of Man. Rev. 13 (1996); David Teece, Gary Pisano & Amy Shuen, *Dynamic Capabilities and Strategic Management*, 18(7) Strat. Man. J. 509 (1997); Tim Holcomb & Michael Hitt, *Toward a Model of Strategic Outsourcing*, 25 J. Op. Man. 464 (2007); Ronan McIvor, *How the Transaction Cost and Resource-based Theories of the Firm Inform Outsourcing Evaluation*, 27 J. Op. Man. 45 (2009). *SEE ALSO* EDITH PENROSE, *THE THEORY AND GROWTH OF THE FIRM* (1959) and RICHARD LANGLOIS & PAUL ROBERTSON, *FIRMS, MARKETS AND ECONOMIC CHANGE: A DYNAMIC THEORY OF BUSINESS INSTITUTIONS* (1995). As described by Holcolm and Hitt: "Whereas transaction-based perspectives explain different governance mechanisms, resource-based theory considers the relative capabilities of focal firms and exchange partners as important in vertical integration decisions"; *id.*, at 466. While the resource-based view of the firm is often framed in juxtaposition to the Coasian framework, Coase himself arguably anticipated the essence of this view; Coase, *supra* note __, at 395 ("it may be that as the transactions which are organised increase, the entrepreneur fails to place the factors of production in the uses where their value is greatest, that is, fails to make the best use of the factors of production.").

advantage.[54] Where one firm has a comparative advantage over another in the production of a given input, outsourcing the production of the input to the firm that enjoys this advantage will then generate a surplus that can be divided between them.

There are several potential sources of comparative advantage. First, firms may possess *specialized human capital, organizational knowledge, or intellectual property* that gives them a technological advantage in the development, application, or production of specific inputs.[55] Second, firms may enjoy advantages stemming from *economies of scale*. For example, where a firm has a large number of customers within a particular industry, improvements to inputs originally developed for one customer can be adapted and rolled out to other customers.[56] By the same token, the firm may possess a better understanding of the industry-wide challenges impacting these customers and how to address them. Third, firms may employ unique *governance mechanisms*—e.g. board and management reporting structures, human resource strategies, and compensation policies—that enable them to better identify, marshal, and exploit their own internal resources.[57] Along the same vein, some firms may simply be better at coordinating the process of bringing together large and complex constellations of external inputs. Indeed, as explained by Tim Holcomb and Michael Hitt: "managing capabilities is itself a capability."[58] Ultimately, where firms are not able to successfully replicate these comparative advantages, the upshot should be higher levels of outsourcing.

The resource-based view shares a number of important parallels with the concept of *core competencies*. As described by C.K. Prahalad and Gary Hamel, core competencies are "the collective learning in the organization, especially how to coordinate diverse production skills and integrate multiple streams of technologies."[59] The scope of a firm's core competencies will hinge on the idiosyncratic insights that can be gained from this collective learning, along with whether and how these insights can be translated into a durable comparative advantage. For example, viewed from this perspective, Apple's comparative advantage stems not only from its own core competencies in product design and development, but also its strategic decision to outsource the production of its products to firms like Micron and TSMC with core competencies in hardware design and manufacturing.[60] Over the past several decades, the

---

[54] Peteraf, *supra* note __, at 179. *See also* McIvor, *supra* note __, at 46 (describing the resource-based view as conceptualizing the firm as "a bundle of assets and resources that, if employed in distinctive ways, can create competitive advantage").

[55] Blair et al., *supra* note __, at 275-276.

[56] Simultaneously, the costs of developing and producing these inputs can also be amortized across this larger customer base.

[57] Barney, *supra* note __.

[58] Holcomb & Hitt, *supra* note __, at 475.

[59] C.K. Prahalad & Gary Hamel, *The Core Competencies of the Corporation*, Harvard Bus. Rev. (May-Jun. 1990).

[60] Along with the unique governance structures it has developed in connection with these outsourcing relationships; see Ronald Gilson, Charles Sabel & Robert Scott, *Contracting for Innovation: Disintegration and Interfirm Collaboration*, 109 Colum. L. Rev. 431 (2009) (using Apple's supply contracts and governance structures as an example of "contracting for innovation" in vertically disintegrated supply chains).

concept of core—and conversely non-core—competencies have become entrenched in both business school education and management practice.[61] The key takeaway is that firms should focus on what they do best: organizing their internal resources and capabilities to reflect their core competencies, while simultaneously outsourcing the production of inputs that involve non-core competencies to other firms.

C. Vertical Legal Constraints

A third factor influencing firm outsourcing decisions is the law. Perhaps most importantly, the law can force firms to outsource production of one or more inputs through the imposition of *vertical legal constraints*. These constraints can restrict or altogether prohibit firms from taking ownership stakes in both their upstream suppliers and downstream customers. They can also prevent firms from directly entering the markets for the inputs used in their own supply chains, or from directly competing in the same markets as their customers.

These vertical legal constraints take two basic forms. The first are rules of general application like §7 of the Clayton Antitrust Act, which prohibits mergers and acquisitions that "may substantially lessen competition" or "tend to create a monopoly".[62] The second are rules targeting specific industries or supply chains. For example, the franchising laws in many U.S. states have historically prohibited automobile manufacturers from selling their cars directly to the public.[63] Many of these laws also prevent manufacturers from competing *directly or indirectly* with their authorized dealerships, effectively prohibiting them from taking ownership stakes in the firms that sell their products.[64] The practical effect is a form of legally mandated outsourcing pursuant to which manufacturers are forced to enter into franchise agreements with dealers in order to bring their products to market.

Perhaps the most famous example of a vertical legal constraint targeting a specific industry is the historical separation of banking from commerce. The origins of this separation can be found in statutory provisions such as 12 U.S.C. §24 (Seventh), which limits the activities of national banks to "such incidental powers as shall be necessary to carry on *the business of*

[61] McIvor, *supra* note __, at 46.

[62] 15 U.S.C. §18.

[63] As recently as 2009, these prohibitions were on the books in almost every state; see U.S. Department of Justice, "Economic Effects of State Bans On Direct Manufacturer Sales To Car Buyers", EAG 09-1 CA (May 2009) ("In the United States… direct manufacturer auto sales are prohibited in almost every state by franchise laws requiring that new cars be sold only by dealers."). Since then, owing largely to the emergence of new manufacturers like Tesla, many states have now relaxed or eliminated these requirements.

[64] *See e.g.* Cal. Veh. Code §11713.3 ("It is unlawful and a violation of this code for a manufacturer… licensed pursuant to this code to do, directly or indirectly through an affiliate, any of the following: (o) To compete with their franchisees in the sale, lease, or warranty service of new motor vehicles."); Ariz. Rev. Stat. Ann. §28-4460.A ("A factory shall not directly or indirectly compete with or unfairly discriminate among its dealers"); Kan. Stat. Ann. §8-2438 ("… a first stage manufacturer of vehicles or second stage manufacturer of vehicles, factory branch, distributor branch, or distributor, distributor or factory representative, may not directly or indirectly: (1) Own an interest in a new vehicle dealer or dealership").

banking".[65] These activity restrictions are then mirrored—albeit imperfectly[66]—within the Bank Holding Company Act (BHCA), which restricts the ability of corporate groups that include one or more banks to own, control, or exercise a controlling influence over businesses engaged in activities that are not "closely related to banking."[67] Together, these entity and group-level restrictions operationalize the separation of banking from commerce: limiting the ability of banks and their affiliates to own, control, or otherwise directly or indirectly engage in non-financial businesses. Importantly, these non-financial businesses encompass a wide variety of upstream suppliers—including the technology firms upon which banks increasingly rely to carry on the business of banking.

D. Regulatory Arbitrage

The fourth and final factor influencing firm outsourcing decisions is the existence of opportunities for *regulatory arbitrage*. Like all of us, firms are subject to law and regulation at the federal, state, and local level. This regulation includes everything from taxes, to environmental, health and safety, and minimum-wage standards, to industry-specific regulatory frameworks like those governing healthcare, energy, and finance. Importantly, it also includes vertical legal constraints like 12 U.S.C §24 (Seventh) and the BHCA. Invariably, this regulation imposes a variety of direct and indirect costs on firms required to comply with it. As explained by Victor Fleischer, the term regulatory arbitrage is used to describe business strategies that enable a firm to reduce these regulatory compliance costs without fundamentally altering its core activities, functions, or economics.[68]

Professor Fleischer identifies three distinct conditions under which opportunities for regulatory arbitrage may arise. The first—*regulatory regime inconsistency*—arises when the same activity or transaction attracts differential legal treatment under two or more regulatory frameworks.[69] The second—*economic substance inconsistency*—arises when economically identical

---

[65] The precise scope of "the business of banking" has been the subject of considerable debate, giving rise to over a century of litigation; see e.g. *Arnold Tours, Inc.* v. *Camp*, 472 F. 2d. 427 (1st Cir. 1972); *Franklin Nat'l Bank* v. *New York*, 347 U.S. 373 (1957); *First Nat'l Bank* v. *Hartford*, 273 U.S. 548 (1927); *Miller* v. *King*, 223 U.S. 505 (1912); *Merchants' Bank* v. *State Bank*, 77 U.S. (10 Wall.) 604, 19 L. Ed. 1008 (1870).

[66] For a detailed history of the Bank Holding Company Act and the evolution of its core group-level activity constraints, see Saule Omarova & Magaret Tahyar, *That Which We Call A Bank: Revisiting the History of Bank Holding Company Regulations in the United States*, 31 Rev. Banking & Fin. Law 113 (2012).

[67] 12 U.S.C. §1841 *et seq*. A subcategory of bank holding companies known as "financial holding companies" are also permitted to engage in a broader range of activities that are deemed "financial in nature," "incidental to financial activity," or "complementary to financial activity" so long as they do not pose micro- or macro-prudential risks; 12 U.S.C. §1843(k)(1)(A) and (2).

[68] *See* Victor Fleischer, *Regulatory Arbitrage*, 89 Texas L. Rev. 227 (2010).

[69] Fleischer, *supra* note __, at 19 ("[regulatory regime] inconsistency can arise though variations in the way that different doctrinal areas cover subject matters relevant to the same transaction… or inconsistency can arise when regulators in different jurisdictions address the same subject matter… other times… [regulatory regime] inconsistency arises when laws become stale, failing to keep up with the development of new financial products and innovative financial techniques.").

activities or transactions are subject to different categorization, and hence different legal treatment, under the same regulatory framework.[70] Lastly, *time inconsistency* arises when the regulatory treatment of an activity or transaction varies across two or more time periods.[71] Where any one of these conditions is met, firms may be able to exploit these inconsistencies: using the judicious structuring of ownership, control, cash flow, information, contract, or property rights to reduce their regulatory compliance costs.[72]

Ronald Coase was amongst the first to observe that a firm's decisions about vertical integration and outsourcing are often driven by regulatory arbitrage.[73] An infamous example from the world of finance involves so-called "rent-a-bank" strategies designed to circumvent state usury laws.[74] In a nutshell, usury laws impose limits on the interest rates that lenders can charge their customers for loans and other types of credit, typically with the objective of protecting borrowers from predatory lending practices, unsustainable debt burdens, and other harms. Yet pursuant to both Supreme Court jurisprudence and federal law, banks are not subject to the usury laws in each of the states in which they carry on business, with the consequence that banks and are almost invariably subject to different interest rate limits than nonbank lenders.[75]

Rent-a-bank strategies involve these nonbank lenders entering into legally binding agreements with partner banks. While the details of these agreements vary, they typically envision that the nonbank lender will be responsible for the initial screening of potential borrowers, while the bank itself will be responsible for making the actual loans. However, after a loan is made, the nonbank lender will then typically purchase it from the bank.[76] As a result,

---

[70] *Id.*, at 20 ("The ability to carve up economic cash flows in a variety of ways creates opportunities to reduce regulatory costs by changing the formal structure of the transactions while actually changing the underlying business deal as little as possible.").

[71] *Id.*

[72] *Id.*, at 27.

[73] *See* Coase, *supra* note __, at 393 ("Another factor that should be noted is that exchange transactions on a market and the same transactions organized within a firm are often treated differently by Governments or other bodies with regulatory powers.").

[74] *See* Adam Levitin, *Rent-A-Bank Partnerships and the Evasion of Usury Laws*, 71 Duke L. J. 329 (2021) (describing the use of rent-a-bank strategies by nonbank lenders to evade state usuary laws).

[75] There are several reasons for this preferential regulatory treatment. First, following the Supreme Court's decision in *Marquette National Bank* v. *First of Omaha Service Corporation*, 439 U.S. 299 (1978), national banks were permitted to export the interest rate limits in their home states to each other state in which they carried on business. Second, in the wake of the *Marquette* decision, many national banks understandably began relocating to states like Delaware, South Dakota, and Utah with low (or no) interest rate limits. In response to this wave of bank relocations, many states legislated to exempt banks from the application of their usury laws. Lastly, Congress eventually intervened to ensure parity between the legal treatment of national and state chartered banks; see Depository Institutions Deregulation and Monetary Control Act of 1980, 12 U.S.C. §1831d.

[76] For a description of the basic mechanics of these agreements, see Gregory Elliehausen & Simona M. Hannon, "Fintech and Banks: Strategic Partnerships That Circumvent State Usury Laws," Federal Reserve Board Finance and Economics Discussion Series 2023-056, 7 (2023); Matt Scully, "How Bank Partnerships with Marketplace Loan Platforms Really Work," *AMERICAN BANKER* (Feb. 24, 2015).

the bank's role is essentially limited to the initial funding of the loan, along with any contracted servicing support.[77] As explained by Adam Levitin, the key feature of these rent-a-bank strategies is that "the bank is taking its underwriting marching orders from the nonbank and the nonbank is acquiring the majority of the financial exposure on the loans."[78] Yet because the bank is considered the "true lender" under these arrangements, the nonbank lender is effectively able to circumvent state usury laws—often enabling them to charge their customers far higher interest rates than they would without the involvement of a partner bank.[79]

These rent-a-bank strategies were first pioneered by payday lenders in the 1990s.[80] And while these strategies initially attracted a degree of scrutiny from federal bank regulators, their use has subsequently expanded into marketplace lending, small business lending, and other credit markets.[81] As Levitin observes, these strategies exploit the assumption that financial products and services are always provided by a *single firm*: whether it be a "bank," "broker-dealer," "investment fund," or other species of financial institution.[82] Yet in reality, one of the defining features of modern finance is that these products and services are often provided through vertically disintegrated financial networks and intermediation chains.[83] And as the widespread use of rent-a-bank strategies highlights, the rationale for this vertical disintegration is often rooted in regulatory arbitrage.[84]

The key takeaway is that there are a range of reasons why firms may rationally decide to outsource the production of a given input. Some of these reasons—like contractability problems and comparative advantages—are driven by the desire to unlock firm-level efficiency gains. But others—and specifically regulatory arbitrage—highlight the potential tradeoffs between these private gains and the public policy objectives underpinning the relevant regulatory frameworks. Compounding matters, in a world where a firm's decisions may be driven by a combination of contractability problems, comparative advantages, *and* regulatory

---

[77] *See* Levitin, *supra* note __, at 359-360.

[78] *Id.*, at 360.

[79] *See* Elliehausen & Hannon, *supra* note __ (for empirical evidence suggesting that nonbank lenders are able to use rent-a-bank strategies to charge higher interest rates).

[80] *See* Michael A. Stegman, *Payday Lending*, 21 J. Econ. Persp. 169 (Winter 2007).

[81] *See* Levitin, *supra* note __, at 366-369 (describing the mixed and ultimately underwhelming regulatory response) and 369-370 (describing the subsequent expansion of rent-a-bank strategies).

[82] *Id.*, at 329.

[83] *See e.g.* Zoltan Pozsar, Tobias Adrian, Adam Ashcraft & Hayley Boesky, "Shadow Banking," Federal Reserve Bank of New York Economic Policy Review (Dec. 2013) (describing the lengthy and complex intermediation chains at the heart of the structured finance ecosystem); Dan Awrey, *Unbundling Banking, Money, and Payments*, 110 Georgetown L.J. 715 (2022) (describing the payment chains connecting the Federal Reserve System, banks, and nonbank payment platforms like PayPal); Levitin, *supra* note __ (describing disaggregation within consumer credit markets).

[84] *See e.g.* David Jones, *Emerging Problems with the Basel Capital Accord: Regulatory Capital Arbitrage and Related Issues*, 24 J. Banking & Fin. 35 (2000) (describing how structured finance was used to minimize the impact of bank capital rules); Awrey, *supra* note __ (describing how nonbank lenders avoid bank chartering, regulation, and supervision).

arbitrage, it can be extremely difficult to untangle and measure the broader social impact of firm outsourcing strategies and patterns. As we shall see, this is the core policy challenge stemming from the rise of BaaS.

II. THE RISE OF BANKING-AS-A-SERVICE

For most of human history, banking was a fundamentally analog experience. Want to deposit or withdraw your money? *Go to the bank*. Want to take out a mortgage, or a loan for your small business? *Go to the bank*. Want to convert U.S. dollars into pounds, yen, or pesos, or make an international wire transfer? *Go to the bank*. Have a question about your financial products or services, want to make a complaint, or even switch to another bank? You guessed it: *go to the bank*. While technology may have enabled your bank to perform many of these functions, it almost always remained out of sight—leaving customers with the impression that banking was an inherently "placed-based,"[85] bricks-and-mortar business. Especially in the United States, this impression was for decades reinforced by laws that restricted banks from operating multiple branches or across state lines.[86]

Today, the idea that banks are constrained by geography seems increasingly antiquated. Technological advances like the internet, modern web-based application programming interfaces (APIs), and smartphones have enabled banks to break free of their place-based roots, expand their geographic footprint, and offer their customers an ever-wider, more sophisticated, and more convenient range of digital products and services.[87] For the most part, bank customers have embraced this technological shift: with a recent survey finding that over three quarters of Americans prefer digital banking over visiting their local bank branch.[88] Importantly, as more and more banks have sought to harness the power of new technology, they have also become increasingly dependent on technology outsourcing. Section II.A describes conventional bank-IT outsourcing models and their emergence as a response to contractability problems, comparative advantages, and the desire to manage the risks stemming from long-term technological uncertainty.

Yet in both finance and technology, change is the only real constant. In a 2012 letter to potential Facebook investors, Mark Zuckerberg described one of the firm's core principles

---

[85] *SEE* SEAN VANATTA, *PLASTIC CAPITALISM: BANKS CREDIT CARDS, AND THE END OF FINANCIAL CONTROL* (2024) (describing the U.S. banking system and the regulatory frameworks that governed it until the 1970s as predominantly "place-based").

[86] *SEE E.G.* JACKSON & TAHYAR, *supra* note __, at 715-717 and 730-732 (2025) (describing historical constraints on bank branching and interstate banking and the roles of the McFadden Act and the Riegle-Neal Act in relaxing and, eventually, eliminating these constraints).

[87] *See e.g.* Acemoglu, Johnson & Mitton, *supra* note __, at 1 ("New technologies, especially information technology, are creating a shift from the old integrated firms towards more delayered organizations and outsourcing"). *See also* Holcomb & Hitt, *supra* note __, at 468 (also observing technology-driven vertical disintegration in banking and other industries).

[88] Mitch Strohm, *Digital Banking Survey: How Americans Prefer To Bank*, Forbes Advisor (Mar. 8, 2022), https://www.forbes.com/advisor/banking/digital-banking-survey-2022/.

as "Move Fast and Break Things."[89] This principle has since become a maxim for entrepreneurs, venture capitalists, and other agents of creative destruction across Silicon Valley, the once sleepy suburb of San Francisco that has in recent decades become the unofficial capital of the U.S. technology industry.[90] And one of the things that Silicon Valley has long wanted to break is finance—including conventional bank-IT outsourcing models. Section II.B describes "banking-as-a-service" or BaaS and explains how it effectively inverts these conventional outsourcing models. Specifically, rather than banks outsourcing their technology needs, the BaaS model envisions that technology-driven "fintech" platforms will take the wheel: providing financial products and services directly to consumers while outsourcing regulated activities like deposit-taking, debit and credit card issuance, and payments to their partner banks. Like conventional bank-IT outsourcing, the rationale for the BaaS model is grounded in contractability problems, comparative advantages, and the risks of long-term technological uncertainty. Yet unlike conventional bank-IT outsourcing, the rise of BaaS is also being driven by pervasive and potentially destabilizing regulatory arbitrage.

A. Conventional Bank-IT Outsourcing

Today, almost every aspect of the business of banking is heavily reliant on technology. Banks rely on technology to perform critical "back office" functions like creating, storing, and updating customer records, processing payments, loans, and other transactions, and ensuring compliance with their ongoing regulatory obligations. They also increasingly rely on technology for "front office" functions like websites that enable their customers to easily and securely access information about their accounts, pay their bills, update their personal details, and contact their bank with any questions or concerns. Yet just because banks rely on technology to perform these critical functions does not necessarily mean that they possess a comparative advantage in the design, implementation, or ongoing maintenance of this technology. In fact, as technology has become more critical to the business of banking, banks have increasingly turned to outsourcing as a strategy for meeting their growing technology needs.

Beyond banks, there are three key players in conventional bank-IT outsourcing (*see* Figure 1). The first are core service providers like FIS, Fiserv, and Jack Henry. These core service providers offer a suite of back office software packages designed to assist banks with functions like customer and account management, deposit and withdrawal processing, credit screening and monitoring, finance and accounting, fraud, risk management, and regulatory compliance.[91] They also help banks design their customer-facing websites, develop their

---

[89] *See* Mark Zuckerberg, "The Hacker Way," *WIRED* (Feb. 1, 2012), https://www.wired.com/2012/02/zuck-letter/.

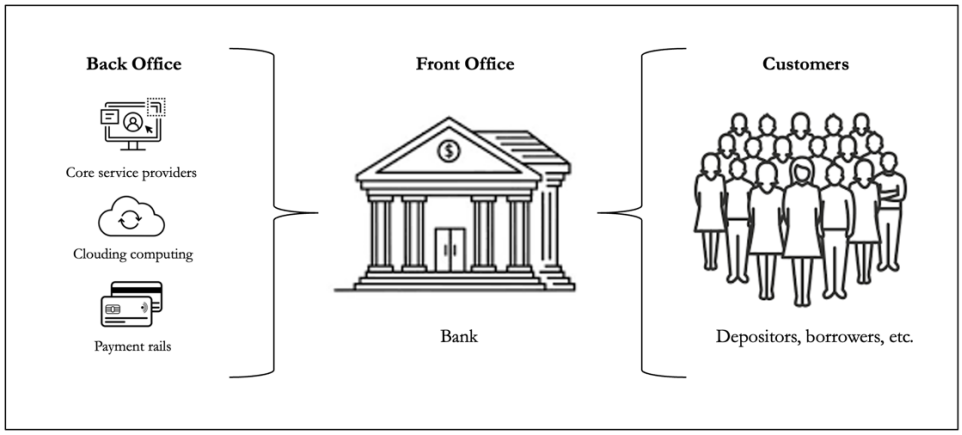
[90] *SEE* SEBASTIEN MALLABY, *THE POWER LAW: VENTURE CAPITAL AND THE MAKING OF THE NEW FUTURE* (2022) (describing the origins and evolution of Silicon Valley's ethos of creative destruction).

[91] *See* Julian Alcazar, Sam Baird, Emma Cronenweth, Fumiko Hayashi & Ken Isaacson, "Core Banking Systems and Options for Modernization," Federal Reserve Bank of Kansas City Payment System Research Briefing (Feb. 28, 2024).

mobile banking applications, and ensure that they can seamlessly connect to popular third-party finance apps like PayPal, Venmo, Robinhood, and Coinbase.[92] Accordingly, while these core service providers operate almost entirely behind the scenes, the technology platforms they design, build, maintain, and upgrade are the "backbone"[93] of the digital products and services that banks provide to their customers.

Figure 1

Conventional Bank-IT Outsourcing Relationships



For decades, these core service providers principally served smaller community banks that lacked the financial and human resources or economies of scale necessary to build their own in-house technology platforms.[94] Even today, over 66 percent of community banks in the United States rely exclusively on these core service providers to provide digital banking services.[95] Yet as customers have come to demand more and better digital banking experiences, even the largest banks have turned to firms like FIS, Fiserv, and Jack Henry.[96] This reversal of strategy in large part reflects the relentless pace of technological innovation over the past

[92] *Id.*

[93] *Id.*

[94] U.S. Department of the Treasury Report to the White House Competition Council, "Assessing the Impact of New Non-Bank Firms on Competition in Consumer Finance" 48 (Nov. 2022); Alcazar et al., *supra* note __.

[95] Thomas Siems, Jonathan Scott & Meredith Covington, "Adapting to the Digital Age: How are Core Service Providers Viewed?," Conference of State Bank Supervisors (Mar. 1, 2022), https://www.csbs.org/newsroom/adapting-digital-age-how-are-core-services-providers-viewed.

[96] *See* Jeremy Quittner, "FIS Sharpens Its Focus on Large Banks," *AMERICAN BANKER* (Feb. 15, 2012).

quarter century. As one long time industry analyst has observed: "Banks are realizing that the rate of change of technology is so fast that it really makes sense to outsource."[97]

Especially for these larger banks, these core service providers have also played an important role in navigating the transition from legacy information systems to modern web-based IT platforms that enable banks to provide the full suite of digital products and services like mobile banking, instant payments, and open finance.[98] Reflecting their growing importance, a 2020 survey conducted by the American Bankers Association (ABA) found that over 55 percent of respondent bank executives believed that their core service provider "keeps [their] bank competitive with innovative solutions."[99] As the ABA survey concluded: "Banks' relationships with their core providers are crucial to their ability to deploy the modern, innovative tools they need to compete in today's marketplace."[100]

The second group of key players in conventional bank-IT outsourcing are cloud computing platforms like Google Cloud Platform, Microsoft Azure, and Amazon Web Services (AWS).[101] Banking is a data-driven business. Banks need to screen and monitor the creditworthiness of borrowers, determine the value of pledged collateral, collect and analyze information about customers and their preferences, and accurately measure and continuously monitor their exposure to investment, operational, regulatory, and other risks. These activities require an enormous amount of data—data that holds little economic value to banks if they cannot cost-effectively store and process it. Before the advent of the internet, this data was typically stored and processed on large mainframe computers owned by individual banks. These mainframes were either physically co-located with the banks that owned them or directly connected to them by a closed network of fiber optic cables. Either way, a bank's data storage and processing capacity were constrained by its access to both the *physical space* needed to house these mainframes and network cables and the *human and investment capital* necessary to build, maintain, and upgrade this sophisticated and expensive technological infrastructure.

Once again, the internet changed everything. Rather than storing and processing data using their own dedicated mainframe computers, the internet enables banks to send their data for storage and processing virtually anywhere in the world. The term "cloud computing" refers to these types of outsourced, network-based data storage and processing arrangements.[102] While there are many variants of cloud computing, its essential feature is that ownership and

---

[97] *See* Daniel Wolfe, "Jack Henry Looks Ahead for Benefit from Outsourcing," *AMERICAN BANKER* (May 10, 2007).

[98] *See* McKinsey & Company, *Should US Banks be Moving to Next-Generation Core Banking Platforms?* (Jul. 26, 2022); Kate Fitzgerald, "Fiserv, Plaid Partner on Consumer Bank-Data Sharing," *AMERICAN BANKER* (Oct. 12, 2023); Kate Fitzgerald, "Fiserv Tests a Hub Approach to Embedded Finance," *AMERICAN BANKER* (Nov. 10, 2023).

[99] *See* American Bankers Association, *Core Processor Survey* 7 (2020).

[100] *Id.*, at 1.

[101] *See* U.S. Department of the Treasury, "The Financial Services Sector's Adoption of Cloud Services" (Feb. 2023) (describing the variants of cloud computing including public, private, and hybrid clouds).

[102] *Id.*, at 4.

control of the network infrastructure—including data centers, network servers, and software applications—resides not with individual banks but with highly specialized technology platforms like Google and AWS.[103] These technology platforms then contract with banks and other customers to provide data storage and processing capacity on their networks, and to meet agreed standards in terms of features like network security, performance, and resilience.

For banks, cloud computing holds out several significant advantages. First, unlike most banks, firms like Google and AWS have vast experience designing, building, and maintaining this type of sophisticated network infrastructure. This includes responding to the constantly evolving cybersecurity threats facing these networks.[104] Second, by spreading network infrastructure across a large number of geographically dispersed data centers, cloud computing platforms typically provide banks with a higher level of operational resilience and redundancy against natural disasters, cybersecurity incidents, and other potential network disruptions.[105] Third, and perhaps most importantly, cloud computing gives banks the ability to scale up their data storage and processing capacity rapidly and with minimal capital investment.[106]

Perhaps the clearest demonstration of this scalability was during the Covid-19 pandemic, where cloud computing enabled banks to quickly respond to the increased data processing demands associated with the simultaneous shift to a remote workplace and from branch-based to digital banking.[107] Critically, without cloud computing, the only way that banks could have managed this risk would have been to make investments before the pandemic in the additional people, physical space, mainframes, and other network infrastructure necessary to ensure that they always had a sufficient cushion of *excess* data storage and processing capacity. Viewed from this perspective, cloud computing enables banks to substitute these types of large, often unpredictable, and potentially redundant capital investments for lower and more predictable ongoing service costs that reflect the data storage and processing resources that banks actually use.[108]

The use of cloud computing by banks has taken off in recent years. According to a 2021 survey conducted by the ABA, more than 90 percent of respondent banks stated that

---

[103] Peter Mell & Timothy Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145 2 (Sept. 2011), https://doi.org/10.6028/NIST.SP.800-145.

[104] *See* U.S. Treasury Department, *supra* note __, at 21. ("From the perspective of the financial institutions interviewed for this report, the security capabilities for public cloud services generally match or exceed their on-premises capabilities.").

[105] *Id.*, at 20 ("Cloud services offer physical redundancy beyond what most financial institutions could develop independently").

[106] *Id.* ("The ability to rapidly procure and commit new resources may be the most attractive feature of cloud services to financial institutions.").

[107] *See* Lananh Nguyen, "Banks Tiptoe Toward Their Cloud-Based Future," *THE NEW YORK TIMES* (Jan. 3, 2022).

[108] *See* Depository Trust & Clearing Corporation, "Moving Financial Market Infrastructure to the Cloud" 5-6 (2017).

they used cloud computing for at least some their data, applications, or operations.[109] A survey by the U.S. Treasury Department published in 2023 similarly found that "the adoption of public cloud services has increased rapidly over the last decade."[110] Consistent with the advantages described above, respondents to the Treasury survey identified increased resilience, the ability to rapidly deploy new technology, and reduced costs as driving demand for cloud computing services.[111] Importantly, several respondents also identified the need to compete with the technology-enabled products and services offered by new fintech platforms as a significant catalyst for cloud adoption.[112]

The third and final group of key players are the twin behemoths of the global payments industry: Visa and Mastercard. In many ways, Visa and Mastercard occupy a unique position in the world of bank-IT outsourcing. First, both firms are technically offshoots of the banking industry itself, having originally been established by consortiums of banks as not-for-profit enterprises designed to pool their financial and human resources for the purpose of making long term investments in new payments technology and network infrastructure.[113] Second, unlike Fiserv, Jack Henry, or AWS, the names and logos of Visa and Mastercard are typically emblazoned on the products and services they enable banks to provide—giving them a level of visibility and brand recognition from the perspective of bank customers that sets them apart from other bank-IT outsourcing firms. Yet at their core, both Visa and Mastercard are fundamentally technology firms. Indeed, the list of technological innovations that have been developed and popularized by Visa or Mastercard reads like a history of the digital payments industry: everything from the magnetic stripe, to chip-and-pin cards, to modern tap-and-pay technology.[114] Looking ahead, Visa and Mastercard have also spearheaded investments in the development of blockchain-based payment platforms.[115]

In 2024, Visa and Mastercard together processed over $23 trillion in credit card, debit card, and online payments worldwide.[116] They were also responsible for more than 70 percent of all card payments made in the United States.[117] As a consequence, while your credit or debit

---

[109] *See* ABA, "Cloud Computing in the U.S. Banking Industry" (Jun. 2021).

[110] *See* U.S. Treasury Department, *supra* note __, at 4.

[111] *Id.*

[112] *Id.*, at 27.

[113] *See* David Sterns, *ELECTRONIC VALUE EXCHANGE: ORIGINS OF THE VISA ELECTRONIC PAYMENT SYSTEM* (2011).

[114] *Id.*

[115] *See* Emily Mason & Olga Kharif, "Visa, Mastercard Race to Tame a $253 Billion Crypto Threat," *BLOOMBERG* (Jul. 1, 2025).

[116] *See* Visa Inc., Form 10-K Annual Report 2 (2024), https://s29.q4cdn.com/385744025/files/doc_downloads/2024/Visa-Fiscal-2024-Annual-Report.pdf; Mastercard Incorporated, Form 10-K Annual Report 6 (2024), https://s25.q4cdn.com/479285134/files/doc_financials/2024/ar/MA-12-31-2024-10-K-as-filed-with-exhibits.pdf.

[117] *See* Nilson Report, *Visa and Mastercard Cards in the US—2024* (2025).

card will typically be issued by your bank, it will more often than not be Visa or Mastercard that developed, own, and control the technology that makes these cards such a convenient and widely accepted means of payment. Viewed through this wider lens, banks have effectively outsourced the research and development of new payment technologies to these ubiquitous and yet often poorly understood platforms.

Together, these conventional bank-IT outsourcing relationships share two important features. First, the economic rationales for outsourcing are grounded in the comparative technological and organizational advantages that core service providers, cloud computing providers, and Visa and Mastercard enjoy over traditional banks. FIS, Fiserv, and Jack Henry have decades of experience and expertise building software solutions and technology platforms specifically for the banking industry. They are also in a unique position to leverage this expertise: with their large and diverse customer bases enabling them to both aggregate information about customer demand and then amortize the high costs of developing new products and services designed to meet it. Similarly, Google, AWS, and other cloud service providers combine specialized technological expertise with highly resilient and scalable network infrastructure that would be prohibitively costly, if not impossible, for individual banks to replicate. And last but not least, Visa and Mastercard enjoy deep technological expertise, pronounced economies of scale, and network effects that position them at the heart of modern payments networks. This position gives them a comparative advantage not only in managing the risks of long term technological uncertainty, but in predicting—and in some ways dictating—the trajectory and pace of technological innovation.

Second, despite the critical importance of these technology outsourcing firms to the business of banking in the digital age, it is still banks themselves that remain the customer-facing institutions. Indeed, with the possible exception of Visa and Mastercard, most customers tend not to know what technology functions their bank outsources, or to whom they are being outsourced. As a consequence, when customers experience a problem with their bank's front or back office technology, they understandably expect the bank itself to resolve it. And as we shall see, the regulation of conventional bank-IT outsourcing relationships has long served to reinforce this expectation.

B. The Banking-as-a-Service Model

The evolution of conventional bank-IT outsourcing relationships has been driven by the emergence of new technologies and the corresponding growth in customer demand for a wide range of digital financial products and services. Yet as these new technologies have become more critical to the business of banking, technology firms have increasingly sought to flip this conventional outsourcing script. The result has been the rise of so-called "banking-as-a-service" or BaaS outsourcing models.[118] While there is no universally accepted definition of BaaS, the term is generally used to describe partnerships between technology firms and

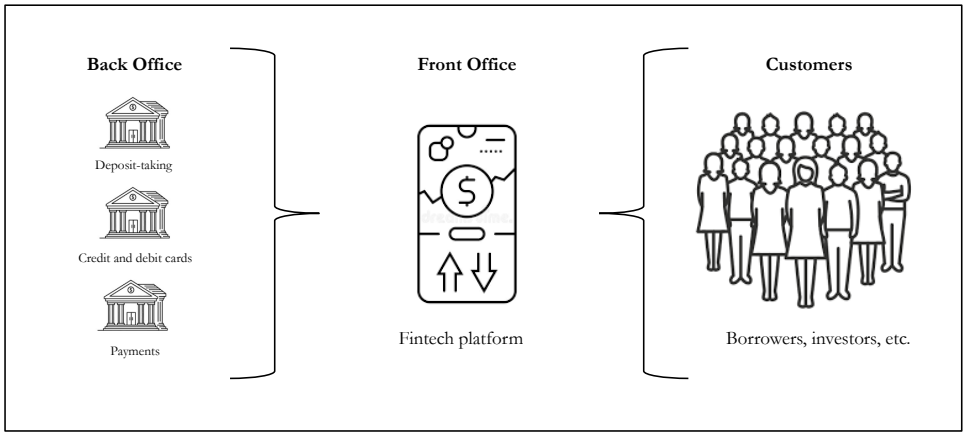
[118] The concept of "banking-as-a-service" is derived from the broader concept of "software-as-a-service" or SaaS, which describes a technology capability provided by a third party on a subscription or on-demand basis; *see* Mikula, *supra* note __, at 1.

chartered banks pursuant to which the customers of these technology firms are able to indirectly access core banking functions like deposit-taking, credit and debit card issuance, and payment processing.[119]

There are three key players in the BaaS ecosystem (*see* Figure 2). The first consists of a vast and rapidly expanding universe of fintech platforms. These fintech platforms include digital wallets like PayPal, Venmo, and Cash App; personal financial management tools like Credit Karma and Mint; online brokerages like Robinhood; "buy now, pay later" platforms like Klarna; cash advance and earned wage access products like EarnIn, and so-called "neobanks" like Chime.[120] In theory, the digitally native business models of these platforms give them a comparative advantage over traditional banks, broker-dealers, investment advisers, payday lenders, and other financial institutions in providing customers with cutting edge user experiences and data-driven financial products and services. While these platforms vary greatly in terms of the specific types of financial products and services they provide, they all share two important things in common. First, the business models of these platforms all revolve around technology-enabled—typically "mobile-first"—products and services that include one or a combination of the ability to hold customer funds, use debit or credit cards, or facilitate electronic payments. Second, and more importantly, these fintech platforms are not chartered banks.

Figure 2

The Banking-as-a-Service Model



[119] *Id.*

[120] *See e.g.* Dan Awrey, *Bad Money*, 106:2 Cornell Law Review 1 (2020) (describing digital wallets); James Fallow Tierney, *Investment Games*, 72 Duke L. J. 353 (2022) (describing online brokerages); Nakita Cuttino, *The Rise of FringeTech: Regulatory Risks in Early Wage Access*, 115 NW U. L. Rev. 1505 (2021) (describing earned wage access platforms); Tobias Berg, Andreas Fuster & Manju Puri, "Fintech Lending," Swiss Finance Institute Research Paper No 21-72 (2021) (describing fintech lending platforms), and Philippon, *supra* note __ (describing a variety of fintech business models).

This takes us to the second key player: the partner banks that provide fintech platforms with access to core banking functions. These partner banks play a number of indispensable roles within the BaaS ecosystem. As a starting point, these banks hold customer funds on behalf of fintech platforms. These funds are typically held in one of two ways. The first involves placing the funds in a direct deposit account (DDA). As the name implies, these DDAs create a direct legal relationship between each customer and the partner bank, with the result that customers are automatically covered by FDIC deposit insurance. The second, and often more popular, is what is known as a "For Benefit of" (FBO) account registered in the name of the fintech platform itself.[121] Thus, for example, if a customer transfers $100 to a fintech platform, the platform will transfer $100 to its FBO account with a partner bank, where it will then be credited to the platform's account and held alongside funds owed to the platform's other customers. Importantly, because customer funds are aggregated into FBO accounts registered in the name of the fintech platform, the platform will need to maintain a set of parallel subledgers recording the transactions and balances of individual customers.[122] In order to fulfill the legal requirements associated with FBO accounts, the platform and its partner banks will then need to periodically reconcile the two sets of records: confirming, amongst other things, that the total dollar value of the individual customer balances recorded on a platform's subledger equals the aggregate customer balances held with its partner banks.

These FBO accounts are the legal and institutional gateways that enable partner banks to then indirectly provide a wide range of other complementary products and services to the customers of fintech platforms. While these products and services vary from platform to platform, and from partner bank to partner bank, they often include debit and credit cards and electronic payment processing.[123] In many cases, they also include personal and small business loans and other credit products.[124] To take just one example, customers using the core checking and savings products offered by the neobank Chime through its partner banks-—currently The Bancorp Bank and Stride Bank-—are also able to access the platform's secured credit card, overdraft, and earned wage access products.[125] They can also take advantage of Chime's data-driven credit building tools and free tax filing service.[126] To take another example, one of the largest partner banks, Cross River Bank, provides fintech platforms with access to an API that supports loan underwriting and due diligence, disbursement, liquidity

[121] Fintech platforms typically prefer FBO accounts to DDAs because they give fintech platforms more flexibility in terms of the use of customer funds.

[122] *Id.*, at 47.

[123] *Id.*, at 19.

[124] *Id.*, at 80.

[125] *See* Chime's website homepage, https://www.chime.com/ (describing its products and services).

[126] *Id.*

management, regulatory compliance, and other critical functions and events in the lifecycle of a loan.[127]

The third key player in the BaaS ecosystem are so-called "middleware" providers. Predictably, the process of integrating the information systems of fintech platforms and traditional banks presents a host of challenges. These challenges include the technological challenges of integrating the modern web-based APIs used by fintech platforms with the older legacy information systems used by many partner banks. As explained by Jason Mikula, in the absence of a middleware provider, "[i]ntegrating with a bank partner often meant passing batch files back and forth-—anathema to technologists that were building their own applications with the latest API-first, microservices architecture."[128] They also include the challenges stemming from the very different business cultures of the banking and technology industries. As Mikula explains: "bank culture could also be a shock to those used to Silicon Valley's engineering driven culture, which emphasized building quickly, deploying minimal viable products to consumers, learning what worked and what did not, and iterating."[129]

Middleware providers like Synapse Financial Technologies and Treasury Prime emerged to address these technological and cultural challenges. These middleware providers specialize in engineering the technological bridges—known as "integrations"—between fintech platforms and their partner banks. In addition to capitalizing on their highly specialized technological expertise, fintech platforms and partner banks using middleware providers also collectively benefit from a reduction in both the number and complexity of integrations. Specifically, having engineered an integration for one platform and partner bank, a middleware provider can then often replicate that integration for other clients. Thus for example, if a middleware provider undertakes an integration for Fintech Platform A enabling it to connect to the information systems of Partner Bank 1, much of that work can then be used to connect Fintech Platforms B, C and D to the same partner bank. This enables fintech platforms to "[r]eplace the lengthy, expensive process of onboarding and integrating with a bank by working with a middleware [provider] who has already done the heavily lifting."[130] Inevitably, the extent of this heavy lifting will depend on the technological starting point of the relevant partner banks—with banks built on modern IT cores and using web-based APIs enjoying a distinct advantage. As a consequence, as more digitally native partner banks like Cross River, Piermont, and Column continue to emerge, one might expect the demand for these middleware providers to eventually decline.

---

[127] *See* Cross River Bank, "The Modern Full-Stack Approach to Banking | Cross River Operating System (COS)" (Oct. 16, 2023), https://www.crossriver.com/insights/the-modern-full-stack-approach-to-banking#:~:text=Example%20Use%20Cases,open%20an%20account%20in%20COS.

[128] Mikula, *supra* note __, at 12.

[129] *Id.*, at 13 [internal quotation marks omitted].

[130] *Id.*, at 48.

There are several factors driving the rise of BaaS. For many customers—and especially high risk, low income consumers[131]—the fintech platforms that rely on the BaaS model provide them with access to a wide range of high quality, inexpensive, and convenient digital financial products and services. For partner banks, the BaaS model holds out the prospect of new revenue streams, including minimum monthly revenue commitments from fintech platforms.[132] The customer funds that these fintech platforms channel to their partner banks also represent a source of low cost, relatively stable deposits.[133] But arguably the most significant benefits of the BaaS model flow to the fintech platforms themselves. As described above, the financial products and services that these platforms provide typically involve regulated functions like deposit-taking, debit and credit card issuance, and access to core payment infrastructure. Yet in the United States, only chartered banks and other depository institutions are legally permitted to perform these functions.[134] These vertical legal constraints leave fintech platforms with a stark and yet unavoidable choice: either obtain a bank charter or pursue the BaaS model. Given the significant initial and ongoing costs of obtaining a bank charter, the BaaS model often represents a far more straightforward and less costly path for fintech platforms looking to bring their technology-driven products and services to market.

Jason Mikula has described the BaaS model as representing the "disaggregation of the value chain of banking".[135] Yet it is arguably more accurate to say that BaaS is an *inversion* of the conventional bank-IT outsourcing model. Specifically, rather than banks outsourcing back office technology functions, the BaaS model is based on technology-driven fintech platforms outsourcing core elements of the banking franchise while simultaneously assuming a critical front office role. And while the factors driving the rise of BaaS include the comparative technological and organizational advantages enjoyed by these fintech platforms, they also include the desire on the part of these platforms to avoid the high costs of bank regulation and supervision. Section III explores these regulatory and supervisory frameworks in greater depth, the gaps in these frameworks into which the BaaS model currently falls, and how these

---

[131] While the reasons for this are complex, regulatory changes in the U.S. after the global financial crisis—including a cap on the interchange or "swipe" fees that banks could charge their customers each time they made a payment using their debit or credit cards—spurred these banks to find other strategies for monetizing their customer relationships. These strategies included minimum monthly fees for basic checking accounts and overdraft charges, both of which disproportionally impact high risk, low income customers. Importantly, because the interchange cap only applies to larger banks that are more likely to possess the human and financial capital necessary to invest in cutting edge technology, the effect was to make access to digital banking more expensive for high risk, low income customers.

[132] *Id.*, at 56-59.

[133] Although as described in Section IV.A, there are plausible states of the world where BaaS deposits could contribute to correlated liquidity demand on partner banks.

[134] *See e.g.* 12 U.S.C. §378(a)(1) (restricting the ability of firms other than banks from accepting deposits); 12 U.S.C. §342 (restricting the ability of firms other than banks from holding an account with the Federal Reserve System. These accounts are a legal and operational pre-condition for direct access to Fedwire and the clearinghouses at the heart of the U.S. payment system). For a more detailed description of these vertical legal constraints and how they limit access to the infrastructure necessary to perform core banking functions, see Awrey, *Unbundling*, *supra* note __.

[135] Mikula, *supra* note __, at 75.

gaps risk confounding the expectations that the customers of fintech platforms have about the scope of the financial safety net.

III. BANKING WITHOUT A NET

In a world where conventional bank-IT outsourcing and BaaS are subject to functionally equivalent regulatory treatment, the stark differences between these two outsourcing models might not matter. Most importantly, where the customers of fintech platforms that have deposited their hard-earned money with a partner bank enjoy the same legal protections as the bank's other depositors, there is arguably little reason for concern about the rise of BaaS—and perhaps much to celebrate. Yet too often, this is fundamentally not the case. This Section describes the conventional financial safety net that protects banks and their depositors, along with the regulatory frameworks that currently govern BaaS, and explores how the emerging gap between them risks confounding customer expectations about the availability of FDIC deposit insurance and other legal protections.

A. The Conventional Financial Safety Net

Banks have long played three important and intertwined roles in the modern financial system and economy. First, banks extend loans and other types of credit to individuals, households, businesses, and governments.[136] Second, banks accept deposits that serve as the dominant source of money.[137] Third, banks have historically been the owners, gatekeepers, and custodians of the clearinghouses and other financial market infrastructure through which the vast majority of payments currently flow.[138]

Reflecting these important economic roles, policymakers in the United States and around the world have granted banks a number of unique privileges. The oldest of these privileges is access to central bank emergency lending—or "lender-of-last-resort"—facilities.[139] Pursuant to §10B of the Federal Reserve Act (FRA), banks facing correlated liquidity demands from depositors and other short-term creditors can access the Federal Reserve's "discount window": enabling them to obtain loans from the Fed collateralized against their illiquid loans and other assets.[140] Pursuant to §14 of the FRA, banks can also sell

---

[136] *See* Federal Reserve Bank of St. Louis, "Loans and Leases in Bank Credit, All Commercial Banks" (TOTLL) (reporting aggregate loans by U.S. banks of $13.2 trillion as of Nov. 26, 2025).

[137] *See* Federal Reserve Board of Governors, Press Release, Money Stock Measures – H.6 Release (Nov. 25, 2025) (reporting M1 of $17.986 trillion, minus currency in circulation of $2.351 trillion, leaving $15.635 trillion in bank deposits—or roughly 87 percent of the total money supply excluding central bank reserves).

[138] *See* Awrey, *supra* note __, at 724-739 (describing the various roles U.S. banks play in connection with clearinghouses and other financial market infrastructure).

[139] *See* WALTER BAGEHOT, *LOMBARD STREET: A DESCRIPTION OF THE MONEY MARKET* (1873) (the seminal text underpinning the rationale for modern lender-of-last-resort facilities).

[140] *See e.g.* Federal Reserve Act, §10B (authorizing the Federal Reserve to undertake so-called "discount window" operations).

prescribed assets directly to the Fed in exchange for central bank reserves that can then be used to pay their obligations to depositors and other creditors.[141]

Banks are also eligible—and often required—to participate in government-backed deposit insurance programs. These programs obligate the government to step into the shoes of a failing bank, thereby honoring its contractual commitments to return depositor funds on demand. In the United States, the FDIC's deposit insurance program currently insures deposits up to $250,000 per depositor, per account type, per bank.[142] In order to make this commitment more credible, the FDIC compensates the depositors of failed banks from a dedicated deposit insurance fund that in the normal course of business is financed by *ex ante* contributions from banks and other insured depository institutions (IDIs).[143] The FDIC also commits to compensate depositors within an extremely short timeframe—typically one business day.[144]

These deposit insurance programs typically work in tandem with special bankruptcy or "resolution" frameworks. These resolution frameworks are designed to restructure or sell a failing bank's assets and liabilities on an expedited basis, thereby minimizing the potential disruption to the bank's customers, uninsured depositors, and other creditors.[145] In the United States, the FDIC administers this resolution framework for the chartered banks and other IDIs under its supervision.[146] Once a bank fails, the FDIC has a duty to maximize the value of its remaining assets, while simultaneously minimizing any compensation that must be paid from the deposit insurance fund.[147] To achieve these twin objectives, Congress has granted the FDIC a wide range of legal tools: including the ability to write down a bank's uninsured liabilities, convert its outstanding debt into equity, repudiate its contracts, and transfer its assets to either a private sector purchaser or a public sector bridge bank.[148] Armed with these tools,

---

[141] *See e.g.* Federal Reserve Act, §14 (authorizing the Federal Reserve to undertake so-called "open market" operations.

[142] *See* Dodd-Frank Act, § 335(a) (making permanent the increase of FDIC insurance coverage to $250,000).

[143] *See* Federal Deposit Insurance Act, 12 U.S.C. §§1817 and 1821.

[144] *See* FDIC, "Common Misconceptions about FDIC Insurance… and the Real Facts," *FDIC Consumer News* (Dec. 22, 2014), https://www.fdic.gov/consumers/consumer/news/cnfall14/misconceptions .html.

[145] *See* Federal Deposit Insurance Act, 12 U.S.C. §§1818, 1819, and 1821(c) (describing the FDIC's powers as receiver); FDIC, *Resolutions Handbook* (May 20, 2025), https://www.fdic.gov/bank-failures/resolutions-handbook. *See also* John Armour, "Making Bank Resolution Credible," in Niamh Moloney et al. (eds.), *THE OXFORD HANDBOOK OF FINANCIAL REGULATION* 453 (2015) (describing the evolution of bank resolution frameworks).

[146] *See* FDIC, "About FDIC: What We Do" (May 15, 2020), https://www.fdic.gov/about/whatwedo/index.html.

[147] *See* 12 U.S.C. §1821(d)(13)(E) (requiring the FDIC to maximize the net present value, or minimize any loss, from the sale of a failed bank's assets); 12 C.F.R. §360.1 (2021) (requiring the FDIC to pursue the resolution option that would impose the lowest costs on the deposit insurance fund).

[148] *See* 12 U.S.C. §§1818, 1819 and 1821(c) (describing in full the FDIC's powers under its resolution framework).

the expectation is that the FDIC will trigger the resolution process after the close of business on Friday afternoon, with the newly acquired or restructured bank able to open its doors for business first thing on Monday morning.

Last but not least, banks are eligible to open central bank reserve accounts. These reserve accounts enable accountholders to settle their obligations to one another using the central bank's own risk-free reserve balances as the means of final settlement. Yet in many jurisdictions—including the United States—only banks and a very limited range of other depository institutions are currently eligible to open these accounts.[149] Further compounding matters, access to a central bank reserve account is typically a legal and operational precondition to becoming a full participant in clearinghouses and other payment networks.[150] The practical effect of these access restrictions is to legally entrench banks at the heart of the conventional payment system.

In exchange for these unique privileges, banking is one of the most heavily regulated industries in the world.[151] In the United States, firms engaged in the business of banking are first required to obtain a state or federal bank charter.[152] Chartered banks are then subject to a highly sophisticated and costly framework of prudential regulation. This prudential regulatory framework includes detailed rulebooks governing how much banks can borrow, what type of investments they can make, and whether they are permitted to engage in activities other than the business of banking.[153] This framework also includes minimum capital requirements designed to ensure that banks can withstand a threshold level of losses before becoming balance sheet insolvent,[154] along with mandatory liquidity requirements designed to ensure that banks can pay their obligations to depositors and other creditors during periods of institutional stress.[155] These detailed rulebooks are then supplemented by intensive risk-based supervision

[149] *See* FRA, §13.1.

[150] *See* Awrey, *supra* note __, at 744-748.

[151] *See* Simon Levin & Andrew Lo, *Opinion: A New Approach to Financial Regulation*, 112:41 Proceedings of the National Academy of Sciences 12543 (Oct. 13, 2015) (reporting that Title 12 of the U.S. Code, governing banks and banking, was second only to the U.S. tax code in its complexity).

[152] *See e.g.* 12 U.S.C. §§21-27 (governing the establishment of a national bank) and §378(a)(2) (making it unlawful to engage in the business of "receiving deposits" unless authorized to do so).

[153] *See e.g.* Bank Holding Company Act, §4; Federal Reserve Act, §§23A and 23B.

[154] *See* JOHN ARMOUR, DAN AWREY, PAUL DAVIES, LUCA ENRIQUES, JEFF GORDON, COLIN MAYER, & JENNIFER PAYNE, *PRINCIPLES OF FINANCIAL REGULATION*, chapter 14 (2016) (describing the definition of capital, the basic requirements, and various mandatory and discretionary capital buffers). In the United States, these capital requirements are typically tailored to each bank on the basis of its size and other characteristics; see JACKSON & TAHYAR, *supra* note __, at 759-765.

[155] ARMOUR ET AL., *PRINCIPLES, supra* note __, chapter 15 (describing basic reserve ratios, the liquidity coverage ratio, and other liquidity requirements). Like capital requirements, in the United States many of these liquidity requirements are tailored on the basis of size and other characteristics; *id.*

by state and federal bank regulators.[156] While reliable data is scarce, it has been estimated that the largest banks can spend over $1 billion per year on compliance with these regulatory and supervisory frameworks.[157] At the other end of the spectrum, regulatory compliance costs are also significant for smaller community banks.[158]

One of the most important consequences of these unique regulatory privileges and protections is the insulation they provide depositors against the risk of bank failure. As a starting point, prudential regulation, risk-based supervision, and lender-of-last-resort facilities all reduce the *probability* that a bank will fail. If and when a bank does fail, the FDIC's deposit insurance program then makes sure that the vast majority of depositors are repaid rapidly and in full. The FDIC's bank resolution framework works in parallel to reduce the *impact* of failure: ensuring that failing banks are sold or wound down in a smooth and orderly fashion, thereby minimizing any risk to the bank's uninsured depositors and other creditors.[159] Together, these regulatory privileges and protections erect a comprehensive financial safety net that gives depositors a high level of confidence and trust in banks as both the dominant source of money and as the institutional gatekeepers of the modern payment system.

B. The Regulation of Bank Outsourcing Relationships

The regulation of bank outsourcing relationships—including BaaS—has historically been just one small piece of the wider regulatory and supervisory framework to which banks are subject. At present, the cornerstones of bank outsourcing regulation are two broad and, until recently, relatively obscure instruments: the Federal Reserve Board, OCC, and FDIC Interagency Guidance on Third-Party Relationships[160] and the Bank Service Company Act of 1962 (BSCA).[161]

---

[156] *See* PETER CONTI-BROWN & SEAN VANATTA, *PRIVATE FINANCE, PUBLIC POWER: A HISTORY OF BANK SUPERVISION IN AMERICA* (2025) (describing the rationale and evolution of bank supervision in the United States).

[157] *See* e.g. Peter Farley, "Spotlight on Compliance Costs as Banks Get Down to Business with AI", *INTERNATIONAL BANKER* (Jul. 4, 2017) (estimating compliance costs for tier one banks at well in excess of $1 billion per year).

[158] *See* Drew Dahl, Jim Fuchs, Andrew Meyer & Michelle Neely, "Compliance Costs, Economies of Scale, and Compliance Performance: Evidence from A Survey of Community Banks," Federal Reserve Bank of St. Louis (Apr. 2018) (reporting that, on average, compliance costs equaled 7 percent of respondent banks' non-interest expenses); Drew Dahl, Andrew Meyer & Michelle Clark Neeley, "Scale Matters: Community Banks and Compliance", Federal Reserve Bank of St. Louis (Jul. 14, 2016) (reporting that, on average, 8.7 percent of the non-interest expenses of banks with assets under $100 million go toward regulatory compliance).

[159] *See* Michael Ohlrogge, *Why Have Uninsured Depositors Become De Facto Insured?*, 100 NYU L. Rev. 345 (2025) (reporting empirical findings that even uninsured bank depositors are routinely insulated from bank failure).

[160] Federal Reserve Board, OCC, and FDIC, Interagency Guidance on Third-Party Relationships: Risk Management, 88:111 Fed. Reg. 37920 (Jun. 9, 2023) [hereinafter, the Interagency Guidance"].

[161] 12 U.S.C. 1861 *et seq.*

The Interagency Guidance on Third-Party Relationships articulates the collective view of the three primary federal banking agencies on sound risk management practices in connection with third-party outsourcing relationships. The Interagency Guidance casts an extremely broad net, encompassing any "business arrangement" between a banking organization and another entity.[162] The Interagency Guidance starts from the position that banks "routinely"[163] enter into these types of third-party outsourcing relationships, and that these relationships "can offer banking organizations significant benefits, such as quicker and more efficient access to technologies, human capital, delivery channels, products, services, and markets."[164] The Interagency Guidance also acknowledges the potential risks, explaining that "the use of third parties, especially those using new technology, may present elevated risks to banking organizations and their customers, including operational, compliance, and strategic risks."[165] The Guidance goes on to explain that "[i]ncreased risk often arises from greater operational or technological complexity, newer or different types of relationships, or potential inferior performance by the third party."[166]

Reflecting the diversity of outsourcing relationships and their tendency to evolve over time, the Interagency Guidance adopts a principles-based approach that requires banks to adopt sound risk management practices that are commensurate with the bank's size, complexity, and risk profile, together with the nature of each third-party relationship.[167] It then lays out a series of principles on specific topics that banks can apply "when developing and implementing risk management practices to assess and manage risks associated with third parties."[168] These topics include: planning and impact assessments, due diligence and third party selection, contract negotiation, ongoing monitoring, oversight and accountability, independent reviews, and documentation and reporting.[169]

While these principles are expressed in extremely broad terms, the one thing that the Interagency Guidance makes perfectly clear is that outsourcing to third parties "does not diminish or remove banking organizations' responsibility to ensure that activities are performed in a safe and sound manner and in compliance with applicable laws and regulations, including but not limited to those designed to protect customers."[170] As a consequence, even

---

[162] The Interagency Guidance also includes a generic and non-exhaustive list of these business arrangements, explaining that "Third-party relationships can include, but are not limited to, outsourced services, use of independent consultants, referral arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, and joint ventures."; Interagency Guidance, *supra* note __, at 37927.

[163] *Id.*, at 37920.

[164] *Id.*

[165] *Id.*

[166] *Id.*, at 37927.

[167] *Id.*

[168] *Id.*

[169] *Id.*, at 37928-37937.

[170] *Id.*, at 37920-37921.

where a third party is technically at fault for a problem, responsibility for resolving it ultimately resides with the bank itself.

Viewed against the backdrop of the rise of BaaS, the Interagency Guidance has two principal shortcomings. The first is that the Interagency Guidance is almost entirely written from the perspective of conventional bank outsourcing relationships. Thus, for example, the Interagency Guidance often implicitly assumes that the bank is the customer-facing institution: recommending, amongst other things, that third parties *receiving* personally identifiable information should be contractually required to maintain appropriate security measures[171] and "where customer interaction is an important aspect of the third-party relationship" that third parties should be *contractually required to receive and respond to customer complaints and inquiries* in a timely manner.[172] While these types of contractual protections obviously matter where a third-party is interacting with *the bank's* customers, they seem out of place where a fintech platform is the party with the direct customer-facing relationship. Indeed, even where the Interagency Guidance obliquely acknowledges the emergence and potential risks associated with the BaaS model,[173] its response is to simply say that "Longstanding principles of third-party risk management set forth in this guidance are applicable to all third-party relationships".[174] Especially given the implicit assumptions underpinning the Interagency Guidance about the structure of bank outsourcing relationships, this blunt and unhelpful statement gives banks remarkably little direction about how to manage the unique risks posed by BaaS. This in turn highlights the second shortcoming of the Interagency Guidance—the fact that is it only guidance and does not have the force and effect of law.[175]

The second, and increasingly central, cornerstone of bank outsourcing regulation is the BSCA. Enacted by Congress in 1962, the original purpose of the BSCA was to enable smaller community banks to compete with their larger rivals by permitting them to create and jointly-own "bank service companies" that provided authorized technology services to the banking industry.[176] The BSCA defines a bank service company as a corporation or limited liability company that is organized to perform authorized services and is wholly-owned by one or more banks or other IDIs.[177] The BSCA then authorizes these bank service companies to provide a list of services exclusively to these IDIs. This list—which, remarkably, has not been updated since 1962—specifically authorizes bank service companies to perform "check deposit sorting and posting, computation and posting of interest and other credits and charges,

---

[171] *Id.*, at 37933 [emphasis added].

[172] *Id.* [emphasis added].

[173] *Id.*, at 37923 ("the agencies recognize that some banking organizations are forming relationships with fintech companies, including under new or novel structures and arrangements. Depending on the specific circumstances… such relationships may introduce new or increase existing risks.").

[174] *Id.*

[175] *Id.*, at 37927.

[176] *See* Jacob Cunningham, *The Limits of the Bank Service Company Act*, 74 Duke L. J. 227, 233-237 (2024) (describing the legislative history and intend behind the BSCA).

[177] BSCA, §1861(b).

preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution."[178]

The BSCA states that a bank service company shall be subject to examination and regulation by the federal banking agency that oversees the bank with the largest equity investment in the company.[179] Importantly, the BSCA also appears to expand the scope of federal regulation and examination beyond bank service companies themselves. Specifically, pursuant to §1867(c) of the BSCA, whenever a depository institution, its subsidiaries, or affiliates "causes to be performed for itself, by contract or otherwise, any services authorized under this chapter… such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the depository institution itself."[180] Over six decades later, the Federal Reserve Board, OCC, and FDIC would rely on this language to extend the scope of prudential supervision to encompass a wide range of technology service providers: including core service providers like Jack Henry[181] and cloud service providers like AWS.[182]

The use of the BSCA to extend the reach of federal bank regulation and supervision to technology platforms like Jack Henry and AWS has not been without controversy.[183] Perhaps the most frequent criticism leveled against this expanded use of the BSCA is the lack transparency.[184] There is currently no publicly available list of the technology platforms that are subject to examination by federal banking agencies. Nor is there a publicly available framework governing when, why, or how these examinations should be conducted.

One of the reasons for this lack of transparency may be the fact that federal bank agencies have adopted an interpretation of the BSCA that is not entirely supported by the statutory text. First, §1863 of the BSCA only authorizes bank service companies to perform listed services. Insofar as §1867 then stipulates that the outsourcing of services "authorized by this chapter" is subject to regulation and examination "as if such services were being performed by the depository institution," one might reasonably interpret the scope of this provision as being limited to services performed by bank-owned service companies and not third-party technology platforms.[185] Indeed, this interpretation makes perfect sense when

[178] *Id.*, §1863.

[179] *Id.*, §1867(a).

[180] *Id.*, §1867(c).

[181] *See* Jack Henry & Assocs., Inc., Annual Report (Form 10-K) 12 (Aug. 26, 2024) (disclosing that the firm is subject to examination by federal banking agencies under the BSCA).

[182] *See* Liz Hoffman, Dana Mattioli & Ryan Trace, "Fed Examined Amazon's Cloud in New Scrutiny for Tech," *THE WALL STREET JOURNAL* (Aug. 1, 2019).

[183] *See e.g.* Heidi Richards, "Time to Admit the Limits of the Bank Service Company Act," *OPEN BANKER* (Feb.18, 2025).

[184] *See e.g.* Cunningham, *supra* note __.

[185] Put differently, unlike bank service companies, the ability of independent firms like AWS and Jack Henry to provide outsourcing services to banks is not in any way contingent on authorization under the BSCA.

viewed as a means of ensuring that depository institutions cannot evade their regulatory obligations simply by outsourcing functions to their bank service companies. Second, and along the same vein, the language of §1867 makes it clear that the authority to bring technology firms within the scope of bank regulation and supervision is limited to those cases where a depository institution, its affiliate, or subsidiary "causes to be performed *for itself*" one or more authorized services. Yet while this may adequately describe conventional bank outsourcing arrangements in which the bank is outsourcing services to technology firms, it does not capture BaaS arrangements in which a partner bank is performing services *for others*. Lastly, the antiquated list of authorized services in many cases bears little or no relation to the critical technology functions that banks outsource today.

Where does this leave us? Together, the Interagency Guidance and BSCA provide federal banking agencies with a foundation—if not always a solid one—for regulating and supervising conventional-IT bank outsourcing relationships. And importantly, even when these outsourcing relationships go wrong, there is still a high degree of legal certainty that banks themselves will be held responsible and that bank depositors will be protected by the conventional financial safety net. Yet it is equally certain that by treating the relationships between fintech platforms and their partner banks as just another type of conventional outsourcing, the Interagency Guidance fails to address the unique risks posed by the rise of BaaS. Section III.C examines the implications of this growing regulatory gap and how it risks fundamentally destabilizing consumer expectations about who should be responsible when these relationships break down and, ultimately, the scope of the financial safety net.

C. BaaS and the Financial Safety Net

The BaaS model exploits gaps within both the third-party outsourcing framework and the conventional financial safety net. As a threshold matter, the Fed, OCC, and FDIC Interagency Guidance only provides direction to *banks* regarding their legal obligations in connection with any third-party outsourcing arrangements. As a consequence, even if the Interagency Guidance technically applies to BaaS, it does not provide any guidance, let alone reflect any legally binding regulatory obligations, for the *fintech platforms* driving the rise of this new outsourcing model. Similarly, BaaS does not appear to fall within the scope of the BSCA given that banks are not receiving any of the narrow and increasingly antiquated range of authorized services currently enumerated under the Act. This arguably leaves federal banking agencies with a relatively limited range of legal tools that might be used to more fully integrate BaaS into the scope of prudential regulation and supervision.

Far more importantly, the BaaS model exposes a critical weakness in the design of the financial safety net—and specifically FDIC deposit insurance. From the perspective of fintech platforms, the most attractive feature of banks is their ability to legally accept customer funds and hold them as deposits. Yet as we have seen, banks can hold these deposits using one of

Since these services are not "authorized by" the BSCA as expressly envisioned by §1867, §1867 arguably should not apply to these firms.

two basic account structures.[186] The first—which includes direct deposit accounts or DDAs—envisions that the customers of a fintech platform will have a direct legal relationship with a partner bank. Since each customer is technically the legal owner of an account in this model, these customers are automatically protected by FDIC deposit insurance. The second—FBO accounts—permit fintech platforms to open omnibus bank accounts in their own name and then pool and hold funds on behalf of their customers. Importantly, because fintech platforms are the registered owners of these omnibus FBO accounts, and because these accounts will typically hold far in excess of $250,000, the customers of these platforms are not automatically protected by FDIC deposit insurance.

At least in theory, the solution to this problem is something known as "pass-through" deposit insurance. As the name implies, pass-through deposit insurance looks past *legal* ownership to identify and protect the *beneficial* owners of the funds deposited in an FBO account—in this case the customers of a fintech platform. Provided that certain ownership, disclosure, and recordkeeping requirements have been satisfied, these beneficial owners will then be entitled to deposit insurance coverage in the event that the partner bank holding these funds fails.[187] Yet pass-through deposit insurance is subject to two important and poorly understood limits. First, reflecting the trust law principles upon which FBO accounts are based, eligibility for pass-through deposit insurance is contingent on the partner bank keeping accurate and up-to-date records of both the identity of each beneficial owner and the precise amount they are owed. Second, pass-through deposit insurance only provides compensation to these beneficial owners in the event of the failure of a partner bank—not the bankruptcy of a customer-facing fintech platform.

Despite these important limitations, eligibility for pass-through deposit insurance figures prominently in the marketing strategies of many fintech platforms that take advantage of the BaaS model. An illustrative example is a statement extracted from the online marketing materials produced by the "prize-linked" savings app, Yotta. After stating in all-caps "FDIC INSURED," the statement goes on to read:

> "Yotta does not hold any customer funds. Deposits are held with Evolve Bank & Trust, *member FDIC*. Funds held with Evolve Bank & Trust, *member FDIC are eligible for FDIC insurance* up to $250,000."[188]

While somewhat less transparent, the website homepage for the neobank Chime—which also offers pass-through deposit insurance—includes similar language:

> "Chime is a financial technology company, not a bank. Banking services are provided by The Bancorp Bank, N.A. and Stride Bank, N.A.; *Members FDIC*"[189]

---

[186] Although in reality there are a variety of different types of DDAs and FBO accounts.

[187] 12 C.F.R. §§330.5 and 330.7.

[188] *See* Anonymous Letter to FDIC, "Bank Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses," Response to Request for Comment (Jul. 1, 2024) [emphasis added].

[189] *See* Chime website homepage, https://www.chime.com/ [emphasis added].

On the one hand, one might reasonably view the fact that fintech platforms choose to deposit customer funds with an FDIC-insured partner bank as a sign of prudence—a reassuring signal that these platforms will do what they must to safeguard customer funds. Indeed, from a marketing perspective, this is almost certainly the point. On the other hand, these statements and others like them typically do little to signal to these customers that there is an enormous difference between holding an FDIC-insured bank deposit and merely being "eligible" for pass-through deposit insurance. Nor in most cases do these statements clearly set out the extremely narrow and highly contingent range of circumstances in which the FDIC will step in to protect the customers of fintech platforms.[190]

It is the contingent nature of pass-through deposit insurance, together with the fact that it does not protect against the failure of the fintech platforms with which customers actually have a direct legal relationship, that ultimately risks confounding customer expectations regarding the scope and protections of the financial safety net. The recent bankruptcy of Synapse Financial Technologies offers an illustrative real world example. Synapse was a middleware provider connecting an impressive client roster of over 100 customer-facing fintech platforms including Mercury, Juno, and Yotta with a stable of FDIC-insured partner banks. Synapse abruptly filed for bankruptcy in April 2024, with subsequent filings revealing poor recordkeeping practices and somewhere between $65 million and $95 million in missing customer funds.[191]

Reflecting these catastrophic bookkeeping problems, many of Synapse's banking partners, including Evolve Bank & Trust, found themselves unable to verify the outstanding balances of both fintech platforms and their individual customers in Synapse's DDA and FBO accounts.[192] Being unable to verify these balances, these partner banks were also unable to process payments to or on behalf of these platforms or customers. This in turn left the fintech platforms that relied on Synapse to maintain these records out of pocket and, in many cases, unable to return customer funds.[193] Amidst this stalemate, the Synapse bankruptcy was unceremoniously dismissed in November 2025.[194] Almost two years after Synapse filed for

[190] For a notable—if still not entirely transparent—counterexample, see Revolut Technologies Inc., "How does Revolut keep my money safe?" (December 2025), https://help.revolut.com/en-US/help/security-logging-in/how-does-revolut-keep-my-money-safe/ (explaining that customer funds are insured "as long as specific deposit insurance requirements are met" and that "FDIC insurance doesn't protect your funds in the event of Revolut's failure").

[191] *See* Synapse Financial Technologies, Inc. Northern District of California, Bankruptcy Court, Progress Reports of Trustee, Jelena McWilliams (Apr. 2025-Jul. 2025).

[192] *Id.*

[193] *Id.*

[194] Synapse Financial Technologies, Inc. Northern District of California, Bankruptcy Court, Notice of Dismissal (Nov. 12, 2025).

bankruptcy, it is therefore still unclear whether and how much of their money the customers of these fintech platforms will ultimately get paid back.[195]

The details of why Synapse filed for bankruptcy are less relevant for our purposes than what the bankruptcy process revealed about the bargain that the customers of these fintech platforms thought they had struck. As part of this process, the bankruptcy court received 108 victim impact statements—the majority from customers of the prize-linked savings app Yotta.[196] Collectively, these statements paint a vivid picture and foreground three important themes. The first theme reflects the reasons why customers were using the fintech platforms caught up in the Synapse bankruptcy. Dozens of customers reported that they were using platforms like Yotta, Juno, and Yieldstreet as savings vehicles: whether to buy a home,[197] pay for college,[198] or meet other anticipated future expenses.[199] When describing the impact of the Synapse bankruptcy on their personal finances, many customers also reported an inability to pay their mortgage or rent, medical bills, and other household expenses.[200] Broadly speaking, these statements reveal that customers were not using these fintech platforms to gamble on crypto or other highly speculative assets. Instead, they were using them to grow their savings, put money aside for a rainy day, and pay for the everyday necessities of life. Accordingly, while there is no question that these platforms are not *banks*, it is hard to argue that they are not performing core *banking* functions.

Build on this first theme, the second theme cutting across the Synapse victim impact statements is the expectation on the part of customers that they would be protected by the conventional financial safety net. No less than 35 of the 108 statements make explicit reference to the fact that they believed their deposits were covered by FDIC deposit insurance. As one customer, who used Yotta to accumulate over $11,000 for use as an emergency fund, explained: "Yotta was marketed as a fun, interactive high yield savings account that was FDIC insured."[201] Another customer, who held $25,000 through Yotta, echoed a similar sentiment: "Yotta advertised heavily that funds were housed in FDIC insured banks, leading me and

---

[195] While the Consumer Financial Protection Board (CFPB) had previously intervened in the bankruptcy case in order to make affected customers eligible for compensation from the CFPB Civil Penalty Fund, as of writing the status of this compensation and the timing of any payouts is still unclear; see Penny Crosman, "Synapse Bankruptcy Dismissed, CFPB May Start Payment Victims," *AMERICAN BANKER* (Nov. 14, 2025).

[196] *See* Synapse Bankruptcy, Collection of Victim Impact Statements [on file with author]. To preserve the anonymity of customers, the author has replaced identifying information with a unique victim impact statement number.

[197] *Id.*, victim impact statements 1, 24, 37, 39, 52, 53, 71, 77, 84, and 99.

[198] *Id.*, victim impact statements 2, 13, 57, 63, 79, 86, 87, and 100.

[199] *Id.*, victim impact statements 7 (saving to buy a car), 8 (for the birth of a child), 21 (for hurricane impact windows), 22 (moving into a nursing home), 23 (leaving a toxic relationship), 31 (moving costs), (wedding costs), 51 (starting a business), 54 (paying off credit card debt), 61 (wedding costs), 72 (tax payments), 89 (birth of a child), 92 (starting a family), and 94 (retirement).

[200] *Id.*, victim impact statements 3, 5, 6, 10, 16, 17, 18, 25, 29, 44, 67, 69, 71, 80, 90, 98, and 104.

[201] *Id.*, victim impact statement 37.

others to believe our money was at no more risk than at a brick and mortar bank."[202] And a third, who had saved $282,000 for a down payment on a house, wrote: "We were reassured our money was safe and FDIC insured. If we knew our money wasn't safe, we would never have done this."[203] Crucially, none of these 35 customers acknowledged that neither the bankruptcy of Synapse itself, nor the failure of Yotta to return their money, were events covered by FDIC deposit insurance. Although, as if to drive this point home, one customer rightly observed: "We need regulations in place to ensure that Americans are NEVER mislead about FDIC insurance".[204]

In the end, platforms like Yotta, Juno, and Yieldstreet are just a small sample of the dozens of popular fintech platforms that relied on Synapse to channel customer funds to partner banks and then keep track of how much money was held, by whom, and on whose behalf. Nevertheless, the victim impact statements also illuminate a third theme: how these types of seemingly idiosyncratic failures can chip away at public confidence and trust in financial institutions and the wider financial system. Upon learning that their funds were not protected by FDIC deposit insurance, one Yotta customer stated that it "shakes my faith in the financial institutions in this country."[205] Another said that their "trust in the financial system was completely shattered."[206] Importantly, this loss of public trust was not confined to financial institutions themselves. Several victim impact statements reflected frustration with the lack of government accountability in the wake of the Synapse bankruptcy. One customer stated: "I reached out to the Federal Reserve, FDIC, my representatives, senators, and the White House. Nobody took responsibility."[207] Other customers reported that their complaints were passed from regulator to regulator, with one ultimately observing "The idea that I trusted the government… to protect me, only for them to point fingers, is grotesque."[208] Still others said they "have lost all faith in our regulators,"[209] "Everyone is failing us,"[210] and "it seems like the banks and the government don't care."[211] These statements shine a powerful spotlight on the regulatory gaps into which the BaaS model currently falls. They also offer us valuable insights into how new technology is changing public perceptions about the distinction between

---

[202] *Id.*, victim impact statement 1.

[203] *Id.*, victim impact statement 77.

[204] *Id.*, victim impact statement 74.

[205] *Id.*, victim impact statement 41.

[206] *Id.*, victim impact statement 106. *See also* victim impact statement 56 ("The fact that this "FDIC" backed bank just took our money is ridiculous… How should we trust banking institutions when you let this happen?").

[207] *Id.*, victim impact statement 57.

[208] *Id.*, victim impact statement 30. *See also* victim impact statements 1, 14, 21, 23, 35, 57, 62, 65, 71, 73, 76, 78, 82, and 101.

[209] *Id.*, victim impact statement 71.

[210] *Id.*, victim impact statement 91.

[211] *Id.*, victim impact statement 108. *See also* victim impact statement 16 ("The federal government has absolutely failed us").

bank*s* and bank*ing*—and thus how crises, scandals, and failures at what we might today view as the periphery of the financial system can shake confidence and trust in institutions much closer to its core.

It is tempting to view the Synapse debacle as an isolated incident—an idiosyncratic case of bad management coupled with lax regulatory oversight. Terrible for customers, great for newspaper headlines, but ultimately of little consequence beyond the still evolving BaaS ecosystem. Yet in reality, both Synapse and the chaos unleashed by its collapse reflect a far deeper, more systemic, and potentially more troubling evolution in the relationship between banking, technology, and financial stability. Section IV explores how the instability in customer expectations highlighted by the failure of Synapse, combined with the opaque and interconnected structure of the BaaS model, could trigger or amplify bank runs and, perhaps one day, even more widespread banking panics.

IV. OUTSOURCING INSTABILITY

The ongoing fallout from the Synapse bankruptcy illuminates how the business model instability triggered by the shift from conventional bank-IT outsourcing to the BaaS model can confound customer expectations. This Section explores how this instability in customer expectations, combined with the continued growth of BaaS, along with its opaque and interconnection structure, could create or amplify channels for institutional or broader financial instability. These channels include correlated liquidity demands on partner banks, breakdowns in the shadow intermediation chains at the heart of the BaaS model, and information contagion both within the fintech ecosystem and, more importantly, between this ecosystem and the conventional banking system.

A. Correlated Liquidity Demands

The first and perhaps most straightforward way that the continued growth of the BaaS model could contribute to institutional or broader financial instability stems from the risk that fintech platforms might make large and highly correlated withdrawals of customer funds from their partner banks. In theory, fintech platforms and other wholesale depositors are often viewed as a cheap source of "sticky" deposits and, accordingly, a relatively stable source of short-term funding.[212] Yet while this may be true in most states of the world, both logic and experience suggest that there are several plausible scenarios in which fintech platforms might be forced to make these type of highly correlated liquidity demands.

First, correlated withdrawals could be the product of competition amongst BaaS partner banks. Thus, for example, as fintech platforms learn which partner banks offer the best technology platforms, pricing, or other features, we would expect them to rationally migrate toward the most competitive banks. Almost inevitably, however, this migration toward

[212] *See e.g.* Mikula, *supra* note __, at 56-57 ("Historically, retail and corporate deposits have been some of the most desirable for banks to hold, as they tend to be "sticky," meaning customers are less likely to move funds elsewhere, and they are often less expensive… than other forms of funding.").

the most competitive partner banks will be accompanied by a migration *away* from the least competitive banks. Especially if this migration were to take place in a relatively short timeframe, involve fintech platforms shifting large balances on behalf of their customers, and target banks that rely heavily on these BaaS deposits, the practical effect would be correlated withdrawals that resembled a conventional bank run.

Second, and perhaps more realistically, correlated liquidity demands could be the product of perceived instability within the fintech ecosystem. In response to the revelation of negative information about the creditworthiness of specific fintech platforms, or the broader fintech ecosystem, customers may rationally decide to withdraw their money in order to avoid the high costs of bankruptcy so vividly illustrated by the failure of Synapse.[213] This incentive to withdraw will be particularly powerful where customers use a platform to make recurring payments, pay their bills, or fund other expenses and, thus, need immediate and ongoing access to their money. Further compounding these dynamics, even where the revelation of negative information itself is not a catalyst, customers may still withdraw their money in anticipation that a critical mass of *other* customers might withdraw their money first, thereby draining the platform of liquidity.[214] Where enough depositors display this type of decision-making, the resulting "first come, first served" dynamic can create a self-fulfilling prophecy in which even otherwise creditworthy platforms are forced into bankruptcy.[215] Most importantly, where fintech platforms experience these types of correlated liquidity demands, they will inevitably be forced to withdraw customer funds from their partner banks. Where the number and aggregate amount of these withdrawals reaches a critical threshold, the practical result will be a potentially destabilizing bank run.

Instability within the fintech ecosystem could also trigger correlated liquidity demands by a partner bank's *non-BaaS* depositors. Specifically, observing instability within the fintech ecosystem, and then anticipating—as described above—that this instability could trigger correlated withdrawals by fintech platforms, these depositors may rationally decide to withdraw their money. In theory, this incentive will be particularly powerful for uninsured wholesale depositors that face the highest risk of not being repaid in full in the event that these correlated withdrawals precipitate a liquidity crisis that forces the bank into the FDIC resolution process.

Last but not least, correlated liquidity demands could be triggered by concerns about the safety and soundness of a partner bank. As reflected in many of the Synapse victim impact statements, customers of fintech platforms are often aware that their money is deposited with one or more partner banks. Yet as these statements also clearly demonstrate, there is often considerable confusion amongst these customers—i.e. expectations instability—about whether their money is protected by FDIC deposit insurance. Where negative information is

---

[213] *See e.g.* Charles Jackin & Sudipto Bhattacharya, *Distinguishing Panics from Information-Based Bank Runs: Welfare and Policy Implications*, 96:3 J. Pol. Econ. 568 (1998) (describing these types of *information*-based runs).

[214] *See e.g.* Diamond & Dybvig, *Bank Runs, Deposit Insurance, and Liquidity*, 91 J. Pol. Econ. 401 (1983) (describing these types of *coordination*-based runs).

[215] *Id.*

revealed about the safety and soundness of a fintech platform's partner bank, these customers thus face a stark choice. First, they can undertake the time-consuming and costly due diligence necessary to verify whether they are in fact covered by pass-through deposit insurance. Second, they can simply withdraw their money from the fintech platform. Once again, where a critical mass of customers rationally decide to withdraw first and ask questions later, the cumulative effect will be functionally equivalent to a run on the fintech platform.[216] Just as importantly, the run on the fintech platform will then in all likelihood further compound the safety and soundness concerns in relation to its partner bank.

To understand how quickly these types of correlated liquidity demands can escalate into full-blown bank runs, one need look no further than the spectacular collapse of Silicon Valley Bank (SVB) in March 2023.[217] As its name implied, SVB was a highly specialized bank that provided financial products and services to technology firms operating in and around Silicon Valley. On Wednesday, March 8th, SVB announced that had sold approximately $21 billion in U.S. treasury securities, that it was taking a $1.8 billion after-tax loss on these sales, and that it planned to raise $15 billion in new term debt and $2.25 billion in equity.[218] The announcement of SVB's "strategic" restructuring sparked panic amongst Silicon Valley venture capitalists, many of whom not only quickly withdrew their own personal and business deposits, but also recommended that their portfolio companies do so as well.[219] News of this embryonic run quickly spread via social media, triggering a massive withdrawal of over $40 billion dollars in deposits over the next 24 hours.[220] By the close of business on Friday, March 10th, SVB—which only days earlier had been one of the largest banks in the United States—was in FDIC receivership.[221]

Against this backdrop, the partner banks at the heart of the BaaS model share two important features with SVB. First, they typically rely on relatively large—and often uninsured—deposits as a source of short-term funding. Second, these large deposits are sourced from a relatively narrow cross-section of technology firms, many of which interact frequently with in the same geographic, business, and professional communities. This combination of features has a critical bearing on the exposure of partner banks to potential

---

[216] In an effort to stem these customer withdrawals, the fintech platform itself may also attempt to move customer funds to a different partner bank—ultimately with the same result.

[217] For detailed postmortems on SVB's collapse, see Federal Reserve Board, "Review of the Federal Reserve's Supervision and Regulation of Silicon Valley Bank" (Apr. 2023) and California Department of Financial Protection & Innovation, "Review of DPFI's Oversight and Regulation of Silicon Valley Bank" (May 8, 2025).

[218] *See* SVB, "Message to Stakeholders Regarding Recent Strategic Actions Taken by SVB" (Mar. 8, 2025), https://s201.q4cdn.com/589201576/files/doc_downloads/2023/03/r/Q1-2023-Investor-Letter.FINAL-030823.pdf.

[219] *See* Andrew Ross Sorkin, Ravi Mattu, Bernhard Warner, Sarah Kessler, Michael J. de la Mecred, Lauren Hirsch & Ephrat Livni, "Why Did Silicon Valley Bank Collapse?" *NEW YORK TIMES DEALBOOK NEWSLETTER* (Mar. 11, 2023).

[220] Federal Reserve Board, SVB Review, *supra* note __, at 4.

[221] *See* FDIC, Press Release, "FDIC Acts to Protect All Depositors of the former Silicon Valley Bank, Santa Clara, California," (Mar. 13, 2023), https://www.fdic.gov/news/press-releases/2023/pr23019.html.

correlated liquidity demands. Specifically, while the *size* of these deposits means that relative few depositors by number need to withdraw their money before these withdrawals snowball into a run, their *industry concentration* makes it easier to disseminate information about any deterioration in a partner bank's creditworthiness and, crucially, the decisions of other depositors about whether or not to withdraw their money. Together, these features arguably make BaaS partner banks inherently more vulnerable to destabilizing runs.

B. The New Shadow Intermediation Chains

The second potential risk to institutional and financial stability posed by the rise of BaaS stems from the emergence of new shadow intermediation chains. The concept of a shadow intermediation chain gained prominence in the thick of the global financial crisis, where it was used to describe the process by which mortgages and loans originated by banks and other commercial lenders were sold to structured finance vehicles, which then repackaged the underlying cash flow rights into marketable debt securities that were themselves then sold to money market funds and other institutional investors.[222] These shadow intermediation chains were viewed as contributing to financial instability in three distinct and yet interconnected ways. First, by enabling banks and other originating creditors to shift the credit and market risks associated with these loans off their balance sheets, these shadow intermediation chains diluted their incentives to engage in rigorous *ex ante* screening and *ex post* monitoring of both borrowers and their collateral.[223] Second, these intermediation chains made it more difficult to identify and monitor the location, nature, and extent of potential risks—thereby undermining both effective market discipline and prudential regulatory oversight.[224] Third, once the crisis struck, the links in these chains became the channels through which financial instability spread from the mortgage market, to structured finance and wholesale money markets, to money market funds, and ultimately to the balance sheets of banks, central banks, and governments around the world.

Like the shadow intermediation chains at the epicenter of the global financial crisis, the key players within the BaaS ecosystem are connected through a series of bilateral contractual and credit relationships: between customers and fintech platforms, between fintech platforms and middleware providers, and between fintech platforms and middleware providers and their partner banks. The complexity of these intermediation chains is then compounded by the fact that fintech platforms often deposit customer funds with multiple partner banks. As highlighted by the fallout from the Synapse bankruptcy, the failure of just one link in this chain—even a seemingly secondary one—can have an enormous impact on

---

[222] *See* Zoltan Pozsar, Tobias Adrian, Adam Ashcraft & Hayley Boesky, "Shadow Banking," Federal Reserve Bank of New York Staff Report No. 458 (Jul. 2010).

[223] *See* Benjamin Keys, Tanmoy Mukherjee, Amit Seru & Vikrant Vig, *Did Securitization Lead to Lax Screening? Evidence from Subprime Loans*, 125(1) Q. J. Econ. 307 (2010); but see also Ryan Bubb & Alex Kaufman, *Securitization and Moral Hazard: Evidence from Credit Score Cutoff Rules*, 63 J. Mon. Econ. 1 (Apr. 2014).

[224] *See* Robert Bartlett, *Inefficiencies in the Information Thicket: A Case Study of Derivatives Disclosures During the Financial Crisis*, 36 J. Corp. L. 1 (2010).

the stability of the wider network. Indeed, not only did the failure of Synapse expose customers to potentially devastating losses, it also undermined the stability and solvency of several fintech platforms and partner banks.[225] In the event, this fallout was only contained because of the relatively small size of this ecosystem and its key players. Yet as this ecosystem continues to grow and evolve, there is no guarantee that it will not become even more complex and interconnected, and hence that the next failure will not have far more serious consequences for financial stability.

In addition to these new shadow intermediation chains, the BaaS model introduces the prospect of lengthy and nebulous *customer data* chains. These customer data chains are forged every time a customer-facing fintech platform onboards a new customer. The data collected as part of this onboarding process will then typically be provided to the fintech platform's partner banks for the purposes of administering the platform's FBO accounts and ensuring compliance with the recordkeeping requirements necessary to make the customer eligible for pass-through deposit insurance in the event of a bank's failure. Where applicable, this data will also be provided to any middleware provider managing the connectivity between the fintech platform and its partner banks. Thereafter, every time the customer transfers money to or from the fintech platform, information about these transfers needs to be provided to the other links in these customer data chains.

Yet as once again illustrated by the fallout from the Synapse bankruptcy, we should not simply assume that information will flow smoothly through these customer data chains. In fact, the mere existence of middleware providers speaks to the technical challenges of building APIs that seamlessly connect the information systems of otherwise independent financial institutions. As a consequence, at any given moment in time, the different links in these data chains may possess different information about customers, transactions, and outstanding balances. Where these differences persist for any length of time, they can put enormous pressure on fintech platforms, middleware providers, and their partner banks to reconcile them—especially where representations have been made that customers are eligible for pass-through deposit insurance. Yet this reconciliation process itself takes significant time, investment, and ongoing coordination amongst these key players. And as demonstrated by the multiple failed attempts at reconciliation during the Synapse bankruptcy, there is still no guarantee that this process will yield an agreement about who owes what to whom. Looking ahead, where questions arise about the timeliness and accuracy of this reconciliation process, customers may rationally respond to this uncertainty by withdrawing their money—potentially triggering large, correlated, and destabilizing outflows of customer funds from both fintech platforms and their partner banks. Viewed from this perspective, the fragility of these customer data chains is very much connected to the fragility of the wider BaaS ecosystem.

[225] *See e.g.* Alexander Saeedy, "The Bank Behind the Fintech Revolution Stumbles After Customer Funds Go Missing," *THE WALL STREET JOURNAL* (Dec. 25, 2024).

C. The Threat of Information Contagion

The third and final risk posed by the rise of BaaS stems from the behavior of fintech platform customers and bank depositors in the face of uncertainty about whether or not they are protected by FDIC deposit insurance. In theory, the objective of deposit insurance and other elements of the financial safety net is to create a credible commitment—an *expectation*—that depositors will not lose money in the event that their bank fails. This expectation is ultimately what incentivizes depositors to deposit their money in FDIC-insured banks and, conversely, disincentivizes them from withdrawing their money at the first sign of trouble.[226] Importantly, the logical implication of this expectation is that people and businesses that hand over their money to firms that are *not* FDIC-insured banks should expect to lose some or all of this money when these firms fail.

Yet as painfully illustrated by the Synapse victim impact statements, the rise of BaaS can make it difficult for customers to successfully determine whether and under what circumstances they are protected by this financial safety net. To a lay person, the statement that a bank is "FDIC-insured" may seem very similar to the statements published by fintech platforms like Yotta that customer funds are deposited with an FDIC-insured bank and "eligible for deposit insurance." A lay person might also reasonably assume that statements made by neobanks like Chime that customer funds are held with an FDIC member bank means that their money is automatically covered by FDIC deposit insurance. Yet in reality, these and other similar statements can obscure important differences in the legal protections that these customers are entitled to receive in the event of the failure of either a fintech platform or its partner banks. These protections run the gamut from receiving a check from the FDIC for the full amount of their bank balance the next business day to having to wait months, if not years, for the conclusion of a costly and uncertain bankruptcy process that may ultimately only return pennies on the dollar. These critically important and yet potentially difficult to understand differences in legal protections are the causal link between the business model instability and expectations instability at the heart of the BaaS model.

Importantly, this combination of business model and expectations instability is also a source of potential "information contagion".[227] Specifically, having witnessed customer expectations about the protections of the financial safety confounded by the failure of one fintech platform, the customers of *other*, otherwise *unconnected*, fintech platforms may rationally decide to withdraw their money. This decision may stem from the perception that these other fintech platforms pursue similar business models, or are exposed to similar risks, as the platform that failed. It may also stem from the realization that these customers do not know

---

[226] *See e.g.* Bengt Holmstrom, "Understanding the Role of Debt in the Financial System," Bank for International Settlements Working Paper No. 479 (Jan. 2015) (describing how this expectation increases the "moneyness" of bank deposits, thereby reducing substitution effects that might trigger bank runs) and Diamond & Dybvig, *supra* note __ (describing how this expectation reduces coordination problems that might trigger bank runs).

[227] *See* Viral Acharya & Tanju Yorulmazer, *Information Contagion and Bank Herding*, 40:1 J. Money, Credit and Banking 215 (Feb. 2008); Toni Ahnert & Co-Pierre Georg, *Information Contagion and Systemic Risk*, 35 J. Fin. Stab. 159 (2018).

anything about their platform's business model or risks, or the legal protections to which they are entitled. Whatever the reason, these customers may decide that the best course of action is simply to withdraw first and ask questions later. Where this type of information contagion takes hold, the failure of one or just a small number of fintech platforms could thus quickly spread to the entire BaaS ecosystem including, importantly, their partner banks. And where this contagion engulfs partner banks, there is also the risk that depositors—unaware of the differences between conventional bank-IT and BaaS outsourcing—would withdraw their money from other banks with little or no connection to the BaaS ecosystem. In this way, the combination of business model and expectations instability could one day sow the seeds of more widespread banking panics.

Today, the threat of information contagion might not loom large on the horizon. Indeed, by most conventional metrics, fintech platforms, their partner banks, and the wider BaaS ecosystem are still nowhere near large or interconnected enough to be considered likely vectors of contagion. Yet almost by definition, the threat of information contagion is highest when we least expect it. The failure of SVB is an illustrative case in point. SVB's failure in March 2023 sent shock waves through the U.S. banking system: disrupting short-term money markets and triggering destabilizing and ultimately fatal runs on two otherwise unconnected banks—Signature Bank and First Republic—that, importantly, were perceived as pursuing similar business models.[228] The fact that these interconnected failures were nowhere on the horizon at the beginning of 2023 serves as a powerful reminder that it is extremely difficult to predict the confluence of financial and psychological factors that can trigger information contagion or, once triggered, how far the contagion will spread. Given the spectacular growth of the BaaS model, together with the expectations instability highlighted by the failure of Synapse, it would seem imprudent to simply dismiss this potential threat.

The possibility that this expectations instability might trigger or amplify broader financial instability creates a potentially acute moral hazard problem. Specifically, where policymakers stand fast and refuse to protect the customers of fintech platforms from instability within the BaaS ecosystem, they risk invoking the political wrath of those customers whose expectations are thereby confounded. The desire to avoid this wrath would then create powerful incentives for policymakers to respond to this instability by resorting to improvised and *ex post* expansions of the financial safety net, including the type of taxpayer-funded bailouts that characterized the policy response to the global financial crisis. Reducing this moral hazard problem demands that we identify and evaluate the potential *ex ante* regulatory strategies that sever the causal links between business model, expectations, and financial stability.

V. OPTIONS FOR POLICY REFORM

The risks posed by the triple cocktail of business model, expectations, and financial instability are very real. So too are the gaps in the regulatory perimeter into which the BaaS

[228] *See e.g.* FDIC, "FDIC's Supervision of First Republic Bank" 2-3 (Sep. 8, 2023) (identifying similarities between the business models of First Republic and SVB, including rapid growth, an overreliance on uninsured deposits, and exposure to interest rate risk, as causes of the bank's failure).

model currently falls. This Section concludes by identifying and evaluating potential options for policy reform. These options include relatively incremental changes to bank recordkeeping and liability rules that reflect the specific risks highlighted by the fallout from the Synapse bankruptcy. They also include more radical reforms to the perimeter of bank regulation and the scope of the financial safety net that reflect the far broader challenges stemming from both ongoing technological disruption in the banking industry and the corrosive effects of regulatory arbitrage.

A. Recordkeeping Reform

Let's start with what is arguably the most straightforward, if decidedly modest, option for policy reform. As described in Section III.C, the problem at the root of the Synapse scandal was not the middleware provider's bankruptcy per se, but rather that Synapse, its fintech platform customers, and their partner banks were unable to reconcile their customer account and balance information. The resulting dispute over who owed what to whom meant that several fintech platforms and partner banks were understandably hesitant to return customer funds. Crucially, the failure of partner banks to keep accurate records also meant that these customers were ineligible for FDIC pass-through deposit insurance.

One obvious solution to this problem is to impose an affirmative obligation on fintech platforms, middleware providers, and partner banks to establish, maintain, and test electronic interfaces—APIs—that enable the continuous, real-time transfer and reconciliation of customer account, balance, and transaction information. In the wake of the Synapse scandal, the FDIC actually proposed a new rule broadly along these lines.[229] Published in September 2024, the proposed rule would have required banks administering "custodial deposit accounts with transactional features"—including BaaS partner banks—to maintain records identifying the beneficial owners of these accounts, the balance attributed to each beneficial owner, and the ownership category of deposited funds for the purposes of FDIC deposit insurance.[230] Where certain additional requirements were satisfied, partner banks would have also been permitted to maintain the required records through middleware providers and other designated third parties,[231] provided that the bank retained unrestricted access to these records in the event of "business interruption, insolvency, or the third party's bankruptcy".[232] To ensure seamless access, the proposed rule required that these records be maintained using a specified electronic file format.[233] Importantly, the rule also contemplated extensive internal controls, including a requirement that partner banks conduct reconciliations against their

[229] FDIC, Proposed Rule, "Recordkeeping for Custodial Accounts," Fed. Reg. 89:191, 80135 (Oct. 2, 2024).

[230] *Id.*, §375.1.

[231] *Id.*, §375.3(c).

[232] *Id.*, §375.3(c)(1).

[233] *Id.*, Appendix A.

beneficial ownership records at least once every business day.[234] Collectively, these requirements were designed to promote the FDIC's ability to make timely and accurate determinations about whether the customers of fintech platforms were eligible for pass-through deposit insurance in the event of the failure of a partner bank.[235]

It is unclear whether the Trump Administration will move ahead with the FDIC's proposed recordkeeping rule, seek to amend it, or simply abandon it altogether. More importantly for the present purposes, the proposed rule was extremely limited in its scope and, ultimately, fundamentally flawed. As a preliminary matter, the rule started from the premise that partner banks were the customer-facing institutions within the BaaS ecosystem: and thus the entry point for customer account, balance, and transaction information. Yet as we have seen, it is often fintech platforms or middleware providers that perform these critical front office roles before passing this information on to their partner banks. Viewed from this perspective, what is missing from the proposed rule is an affirmative obligation on these fintech platforms and middleware providers to provide this information to their partner banks on a timely and accurate basis.

Second, and along the same vein, despite acknowledging the critical role of third party technology firms within the BaaS ecosystem, the proposed rule placed responsibly for designing, building, and maintaining the technological infrastructure necessary to comply with the rule squarely on partner banks. Yet once again, given their comparative technological and organizational advantages, we should expect fintech platforms and middleware providers to often be in a far better position to perform these critical functions. And importantly, while the proposed rule would have required partners banks to enter into contracts with these third party technology firms that clearly defined each party's roles and responsibilities,[236] it also explicitly prohibited banks from contractually shifting their recordkeeping obgliations under the proposed rule.[237] By placing the responsibility for compliance exclusively on partner banks, the proposed rule would thus have failed to apply regulatory pressure on the fintech platforms and middleware providers that have and continue to play an extremely influential role in the development of the BaaS ecosystem.

Last but certainly not least, the FDIC's proposed recordkeeping rule would have done very little to address the expectations instability revealed by the Synapse bankruptcy. While greater certainty around the availability of pass-through deposit insurance would clearly be a welcome improvement, the reality is that this protection only applies in the event of the failure of an FDIC-insured *partner bank*. Yet if the deeper problem is ultimately that customers expect this protection to extend to the bankruptcy of a *fintech platform*, it is hard to see how imposing more rigorous recordkeeping obligations on partner banks would serve to recalibrate these expectations. Even more problematic, given that the FDIC explicitly framed the proposed rule

[234] *Id.*, §375.3(b)(2) and (c)(3)(ii).

[235] *Id.*, 80135 and §375.1.

[236] *Id.*, §375.3(4)(i).

[237] *Id.*, §375.3(4)(iv).

as a response to the fallout from the Synapse bankruptcy,[238] the customers of fintech platforms might have been left with the false impression that they would henceforth been protected in the event of future fintech bankruptcies.

B. Liability Rules for Bank-Fintech Partnerships

Enhanced bank recordkeeping requirements are undoubtedly an important step in the right direction. Yet their impact may ultimately be relatively limited insofar as these and other requirements fail to sufficiently incentivize fintech platforms and middleware providers to make the investments in technological infrastructure necessary to protect customers and ensure regulatory compliance. As we have already seen, both the existing Interagency Guidance on Third-Party Relationships and the FDIC's proposed recordkeeping rule envision that partner banks will be responsible for any conduct by fintech platforms, middleware providers, and other third party technology firms that harms customers or violates federal banking law. The practical effect is to insulate these important players from any direct regulatory obligations or liability stemming from the performance of their critical roles within the BaaS ecosystem. And while in theory policymakers might seek to use the BSCA to impose such obligations, its antiquated framing and list of authorized services bear little resemblance to the BaaS model and, hence, leave its potential application vulnerable to administrative law and other legal challenges.[239]

One way to address this incentive problem is for the FDIC, OCC, and Federal Reserve to establish special liability rules for bank-fintech partnerships. These liability rules could take a number of different forms and allocate liability in a variety of ways. To take just one example, in the event of the failure of a partner bank, where non-compliance with bank recordkeeping requirements rendered the customers of a fintech platform ineligible for pass-through deposit insurance, the partner bank, fintech platform, and any middleware provider could be held jointly and severally liable for any resulting customer losses.[240] This rule could then be combined with a second rule giving the customers of the fintech platform, as beneficial owners, the same priority and legal entitlements as a failed bank's other uninsured depositors. More broadly, given the critical customer-facing role that these fintech platforms and, in some cases, middleware providers play within the BaaS ecosystem, it makes sense to impose liability

[238] *Id.*, 80135, 80138, 80139, 80146, 80147, and 80149 ("the recent events surrounding the bankruptcy of Synapse [have] raised questions about the completeness, accuracy, and integrity of custodial deposit account records underlying arrangements with third parties at certain IDI[s]. These events highlight substantial risks with respect to the prompt access to customers funds held in custodial deposit accounts. These issues create uncertainty that undermines the public confidence that underpins banks and our nation's broader financial system.").

[239] Especially in the wake of the Supreme Court's decision in *Loper Bright* v. *Raimondo*, 603 U.S. 369 (2024) (curtailing the level of deference that courts are required to give an agency's interpretation of legislation granting it delegated authority).

[240] In theory, this liability rule could be combined with a parallel whistleblower rule exculpating a partner bank, middleware provider, or fintech platform from liability where they reported material noncompliance with recordkeeping or other rules in advance of any harm to customers.

on them for harms caused by financial, technological, or other failures the avoidance of which was reasonably foreseeable and within their control.

The imposition of new liability rules for bank-fintech partnerships would hold out two potentially significant benefits. First, the prospect of liability would generate more powerful incentives for the fintech platforms and middleware providers that in many cases possess a comparative technological advantage in the design and implementation of the APIs and other technological infrastructure that drive the BaaS ecosystem. Viewed in this light, these technology firms will in many cases be what Professor Guido Calabresi has described as the "cheapest cost avoider": the party in the best position to avoid potential harms, and hence the party to which liability should generally be allocated.[241] Second, these liability rules would help minimize expectations instability by reducing the difference in outcomes between FDIC-insured depositors and fintech platform customers in the event of bank failure. To help strengthen this connection between expectations and outcomes, these liability rules could even by made contingent on whether a fintech platform advertised the availability of deposit insurance to its customers. If properly designed, these liability rules would thus better align the incentives of these platforms with both public policy objectives and their partner banks, while simultaneously providing their customers with a higher level of protection against the unique risks posed by the rise of BaaS.

C. Tighten the Financial Safety Net

Policy reforms like enhanced recordkeeping requirements and new liability rules for bank-fintech partnerships would represent a meaningful improvement over the status quo. Yet these incremental reforms would not address the deeper policy challenges that ongoing technological disruption and regulatory arbitrage pose to the integrity of the perimeter of banking regulation. As a consequence, they cannot completely eliminate the business model, expectations, and financial instability generated by the rise of BaaS—let alone future waves of technological and financial innovation. This take us in search of more radical policy options. One, perhaps intuitively appealing, option is to tighten the existing regulatory perimeter with the objective of extinguishing the expectation that the customers of fintech platforms will enjoy the protections of the conventional financial safety net.

In theory, federal banking agencies already have several legal tools at their disposal to achieve this objective. One of these tools is the power to enforce the prohibition against unfair and deceptive acts or practices pursuant to both §5 of the Federal Trade Commission Act[242] and Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act.[243] Under both of these statutory frameworks, an act or practice is "unfair" if it causes or is likely to

---

[241] *SEE* GUIDO CALABRESI, *THE COST OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS* (1970).

[242] 28 U.S.C. §§2671-2680.

[243] Pub. L. No. 111-203, 124 Stat. 1376 (2010). *See also* FDIC Consumer Compliance Examination Manual, Unfair, "Deceptive and Abusive Practices - Federal Trade Commission Act/Dodd-Frank Act," (Aug. 2025), https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/7/vii-1-1.pdf.

cause substantial injury to customers, the injury is not reasonably avoidable by these customers, and the injury is not outweighed by countervailing benefits to consumers or to competition.[244] Meanwhile, a representation, omission, or practice is "deceptive" if it is likely to mislead a customer, the consumer's interpretation of the representation is reasonable under the circumstances, and the misleading representation is material to the customer's decision-making.[245] Under the Dodd-Frank Act, the Consumer Financial Protection Bureau (CFPB) also has the authority to bring enforcement actions in connection with "abusive" acts or practices.[246] For these purposes, an act or practice is "abusive" if it materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service.[247] Importantly, an act or practice will also be abusive if it takes unreasonable advantage of a lack of understanding on the part of a consumer about the material risks, costs, or conditions of a product or service, the inability of a consumer to protect their interests in selecting or using a product or service, or the reasonable reliance by a consumer on a covered financial institution to act in their best interests.[248]

The FDIC has occasionally issued warnings to fintech platforms not to make misrepresentations about whether their customers are protected by deposit insurance.[249] However, the FDIC, CFPB, and other federal banking agencies have never launched a more sustained market-wide campaign seeking to leverage the prohibitions against unfair, deceptive and abusive acts and practices (UDAAP) to root out and deter potential misconduct. Yet as demonstrated by Synapse victim impact statements, there is a strong *prima facie* case that many of the marketing practices within the BaaS ecosystem fall squarely within the scope of the UDAAP prohibition. This is especially the case for statements like "eligible for FDIC deposit insurance" and "customer funds are deposited with Bank X. Member FDIC" which, even when technically accurate, would qualify as abusive insofar as they take "unreasonable advantage of a lack of understanding on the part of a consumer about the material risks, costs, or conditions of a product or service."[250] Accordingly, more vigorous, targeted, and sustained UDAAP enforcement could play a constructive role in eliminating acts and practices that contribute to expectations instability.

---

[244] 15 U.S.C. §45(n); 12 U.S.C. §5531(c)(1).

[245] *See* Federal Trade Commission Policy Statement on Deception (Oct. 14, 1983), appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984); CFPB, Examination Manual v.3, UDAAP-5 (March 2022) (citing FTC Policy Statement on Deception). The CFPB has previously indicated that it will look to authorities under the FTC Act for guidance in defining the scope of deception under Title X of the Dodd-Frank Act. *See id.* at 5 n.10.

[246] 12 U.S.C. §5531(d).

[247] *Id.*, §5531(d)(1).

[248] *Id.*, §5531(d)(2).

[249] *See e.g.* FDIC, Press Release, "FDIC Demands Five Entities Cease Making False or Misleading Representations about Deposit Insurance" (Jan. 19, 2024), https://www.fdic.gov/news/press-releases/2024/pr24003.html.

[250] 12 U.S.C. §5531(d)(2).

More targeted and sustained UDAAP enforcement by federal banking agencies is dependent on both the dedication of significant financial, human, and other resources and, crucially, the political will to pursue this costly strategy. The effectiveness of this strategy in reducing expectations instability may also be somewhat limited to the extent that some fintech platforms will inevitably escape enforcement, that questionable acts and practices will therefore not be completely eliminated, and that regulatory enforcement actions may not be highly salient events for the vast majority of fintech customers.

In light of these potential limitations, a second, complementary, and in some ways more radical policy option resides in the illegal deposit-taking provisions under §21(a)(2) of the Glass-Steagall Act of 1933.[251] In theory, §21(a)(2) makes it unlawful for a person, firm, corporation, association, business trust, or other similar organization "to engage, to any extent whatever... in the business of receiving deposits subject to check or to repayment upon presentation of a pass book, certificate of deposit, or other evidence of debt, or upon request of the depositor."[252] This blanket prohibition is then subject to three enumerated exemptions, the most important of which has long been interpreted as covering national and state-chartered banks and other IDIs. For organizations that do not fall within one of these exceptions, violations of §21(a)(2) are subject to criminal sanctions, including fines and imprisonment of up to five years.

The version of §21(a)(2) passed by Congress in 1933 has never been entirely fit for purpose. The provision is riddled with ambiguous language and carveouts. For example, while the prohibition explicitly applies only to illegal *deposit* taking, federal banking law generally defines a "deposit" as a balance of money received or held by a "depository institution,"[253] a category that includes commercial banks, credit unions, savings and loan associations, and other institutions that are exempt from the application of the prohibition.[254] As a consequence, federal law enforcement agencies have rarely even contemplated enforcing the prohibition, let alone actually wielding it to effectively police the perimeter of bank regulation and protect the core deposit franchise.

Reforming §21(a)(2) is thus long overdue. What is more, the emergence and rapid growth of the BaaS ecosystem arguably provides the most powerful justification yet for why policymakers should update this prohibition for the twenty-first century. These reforms could be implemented in a variety of ways. For example, Professor Morgan Ricks has proposed an "unauthorized banking statute"—essentially a beefed up §21(a)(2)—that by adopting a more functional definition of money would capture, amongst a wide range of other

[251] 12 U.S.C §378(a)(2).

[252] *Id.*

[253] *See e.g.* 12 U.S.C. §1813(l)(1); 12 C.F.R. §204.2(a)(1)(i)-(ii).

[254] *See e.g.* 12 U.S.C §1813(c)(1). Although courts have theld that successful enforcement of §21(a)(2) does not require the government to prove the existence of a bank; *see United States* v. *Jenkins*, 945 F.2d 167 (2nd Cir. 1991). *See also* Letter from Assistant Attorney General Philip Heymann, Criminal Division, to Martin Lybecker, Associated Director, SEC Division of Marketing Management (Dec. 18, 1979) (deemphasizing the use of the word "deposit" in determining whether SEC-regulated money market funds ran afoul of the §21(a)(1), the sister provision of §21(a)(2)).

instruments, the contractual obligations of fintech platforms accepting customer funds to return these funds on demand.[255] Congress could also amend the current §21(a)(2) to grant federal banking agencies delegated authority to define the scope of the prohibition on a dynamic basis in response to emergence of new business models. Rather than simply banning BaaS as illegal deposit-taking, federal banking agencies could then use this rulemaking authority to articulate the conditions—like recordkeeping requirements, liability rules, advertising restrictions, and the availability of pass-through deposit insurance—under which fintech platforms could operate without violating the prohibition.

The threat of criminal sanctions under a reformed §21(a)(2) would serve as a powerful deterrent for those fintech platforms seeking to exploit the BaaS model to avoid obtaining a bank charter while simultaneously creating the expectation that their customers will enjoy the protections of the conventional financial safety net. Yet as with all powerful deterrents, there is the risk that this will effectively kill the BaaS ecosystem—and with it the benefits stemming from the comparative technological and organizational advantages possessed by many fintech platforms. To the extent that policymakers value these benefits, it may therefore be desirable to combine the stick represented by the UDAAP and §21(a)(2) prohibitions with a carrot in the form of a new federal chartering framework better tailored to the unique business models of these platforms.

D. Expand the Regulatory Perimeter

Policy reforms like enhanced recordkeeping requirements and new liability rules for bank-fintech partnerships can together minimize the risk and uncertainty that the customers of fintech platforms face when their partner banks fail. The credible threat of more targeted and sustained enforcement of the UDAAP and illegal deposit-taking prohibitions can then help prevent the emergence of business models, acts, and practices that risk creating or reinforcing the expectation that the conventional financial safety will also protect these customers if their fintech platform meets a similar fate. At present, these fintech platforms are regulated under a complex patchwork of state and federal laws that can vary greatly depending on a platform's geographic footprint, its business model, and the types of financial products and services it provides.[256] This raises an important question about whether policymakers should carve out space for these platforms within the perimeter of federal banking regulation.

A constructive starting point for answering this question is our earlier observation that the economic rationale for the BaaS model is rooted in the desire of fintech platforms to access core elements of the banking franchise like deposit-taking, credit and debit card issuance, and payments. This introduces the possibility that Congress could create a bespoke chartering framework designed specifically for platforms engaged in this relatively narrow range of

[255] *SEE* RICKS, *supra* note __, 243-245.

[256] *See e.g.* Congressional Research Service, "Fintech: Overview of Financial Regulators and Recent Policy Approaches," CRS Report R46333 (Apr. 28, 2020), https://www.congress.gov/crs-product/R46333 (providing an overview of the wide range of crosscutting regulatory frameworks and initiatives targeting the U.S. fintech ecosystem).

activities. While the details are beyond the scope of this Article, this new chartering framework could include two core features. First, in order to maintain a sharp distinction between this new charter type and traditional banks, chartered fintech platforms could be prohibited from using customer funds to finance their ongoing operations, make loans or other investments, or otherwise engage in financial intermediation. Instead, platforms could be required to open a central bank reserve account and then hold all customer funds, for their exclusive benefit, in this account. Second, these platforms could be made subject to a streamlined resolution process designed to ensure that, in the event of a platform's bankruptcy, the customer funds held in this account would be returned to them rapidly and in full.

Compliance with this new chartering framework would inevitably require ongoing regulation and supervision by a federal banking agency: most likely either the Federal Reserve Board or OCC. Yet given the relatively narrow scope of the proposed charter, together with the prohibition against financial intermediation, this regulatory and supervisory framework would not need to be anywhere near as costly or intrusive as the equivalent frameworks to which banks are currently subject. For example, rather than focusing on the design and implementation of highly technical policy levers like capital adequacy, asset quality, earnings, and liquidity management, the responsible banking agency could instead focus on relatively straightforward tasks like ensuring that chartered platforms maintain accurate customer records, ongoing verification of the identity of customers and their outstanding reserve account balances, and designing and testing the processes for ensuring that customer funds are returned in the event of a platform's bankruptcy.

In recent years, scholars, policymakers, and even the OCC have advanced a range of possible blueprints for a fintech charter.[257] Most recently, Professor David Zaring has proposed a menu of "skinny" charters that reflect the wide variety of different activities and functions performed by fintech platforms.[258] Without commenting on the promise and perils of these other blueprints, a new federal charter that included these two core features—mandatory placement of customer funds in a ringfenced central bank reserve account and an expedited process for returning these funds following a fintech platform's bankruptcy—would yield several important benefits.

First, from the perspective of customers, requiring fintech platforms operating under this new chartering framework to place customer funds in a risk-free central bank reserve account would fully insulate them from the type of uncertainty, stress, and negative financial outcomes associated with the Synapse bankruptcy. At the same time, by credibly committing to return customer funds rapidly and in full, the expedited resolution process would effectively replicate the outcomes long delivered by FDIC deposit insurance. By replicating these outcomes, the new chartering framework would thus leave these customers in essentially the

---

[257] *SEE E.G.* AWREY, *BEYOND BANKS*, *supra* note __, chapter 7 (advocating for the creation of a federal payments charter); OCC, Comptroller's Licensing Manual Supplement: Considering Applications From Financial Technology Companies (Jul. 2018), https://www.occ.treas.gov (the OCC's fintech chartering program was abandoned following the 2020 presidential election and a subsequent change in agency leadership).

[258] David Zaring, *Skinny Charters: Rebuilding the Banking Regulatory Perimeter*, 50:3 J. Corp. L. 700 (2025).

same position as they would have been had they simply deposited their money directly into a traditional bank.

Second, for fintech platforms, access to central bank reserve accounts would eliminate a critical legal obstacle to direct participation in the clearinghouses and payment networks at the heart of the conventional payment system.[259] As a consequence, it would greatly reduce the reliance of these platforms on banks and, ultimately, on the BaaS model. Importantly, fintech platforms would also benefit from a chartering framework that, especially in comparison with a conventional bank charter, was more specifically tailored to their relatively narrow business models. In theory, this reduced compliance burden would then enable these platforms to better structure their business models and strategies around capitalizing on their comparative technological and organizational advantages. Accordingly, while there is a strong policy argument for making this new charter mandatory for nonbank fintech platforms engaging in deposit-taking, credit and debit card issuance, or payments, one might therefore expect to observe significant levels of voluntary adoption.[260]

This new chartering framework would also hold out potentially significant benefits for the integrity of the regulatory perimeter and, ultimately, for financial stability. With the addition of this framework, fintech platforms would have a relatively limited and clearly defined range of chartering options. The first option would be to obtain a traditional bank charter, thereby gaining access to the unique benefits of the conventional financial safety net, but also subjecting themselves to the unique compliance burdens of bank regulation and supervision. For platforms that found that these burdens outweighed the benefits, the second option would then be to obtain a new fintech charter. And importantly, for any remaining platforms that found neither of these first two options attractive, targeted and sustained enforcement of §21(a)(2) would ensure that their business models did not run afoul of the prohibition against illegal deposit-taking.

By giving fintech platforms a viable option that avoided the costly and sometimes unnecessary burdens associated with bank regulation and supervision, the introduction of a fintech charter would relieve the pressure created by hydraulic effects of regulatory arbitrage that have in part driven the rise of the BaaS model.[261] Even more importantly, while the choice

---

[259] *See* discussion in Section III.A *supra*.

[260] The primary policy argument for mandatory adoption flows from the observation that, assuming voluntary adoption was incomplete, some fintech platforms would remain outside the perimeter of federal bank regulation. In addition to leaving the regulatory perimeter vulnerable to the hydraulic effects of regulatory arbitrage, this would open the door to some level of residual expectations instability.

[261] The importance of clear and limited optionality in reducing the corrosive impact of regulatory arbitrage exposes some of the potential drawbacks of trying to shoehorn new business models into old chartering frameworks. This was the strategy pursued by the OCC in connection with both its 2018 proposal for a fintech charter and, more recently, its push for fintech platforms to adopt its existing trust charter; see OCC, "OCC Announces Conditional Approvals for Five National Trust Charter Applications," OCC News Release 2025-125 (Dec. 12, 2025), https://occ.gov/news-issuances/news-releases/2025/nr-occ-2025-125.html. The principal drawback is that making these types of opaque and often *ad hoc* changes to existing chartering models can both blur the regulatory perimeter, thus opening the door to regulatory arbitrage, and provide cover for a broader deregulatory agenda.

between obtain a traditional bank charter or a new fintech charter might be incredibly important from the perspective of fintech platforms, we would expect the vast majority of their customers to be almost completely indifferent—safe in the knowledge, or ignorance, that their funds were protected regardless of which chartering option a platform decided to pursue. This legally engineered indifference would reflect the complete elimination of expectations instability and, with it, the prospect that this instability could metastasize into correlated liquidity demands, the breakdown of BaaS intermediation chains, or broader information contagion.

CONCLUSION

Time and technology eventually change everything—even a business as old as banking. The inevitability of technological disruption demands that policymakers seek to better understand how bank regulation and supervision, the design of the regulatory perimeter, and the scope of the financial safety net can and should evolve in response to the emergence of new business models, new patterns of customer behavior, and new challenges. The rise of BaaS represents a significant new test of the ability of policymakers to respond to these demands. And whether they ultimately decide to adopt incremental changes to existing regulatory and supervisory frameworks or more fundamental reforms to the perimeter of bank regulation and the scope of the financial safety net, the surest way to fail this test is by continuing to ignore the complex and evolving relationship between banking, technology, and instability.

european corporate governance institute

about ECGI

The European Corporate Governance Institute has been established to improve *corporate governance through fostering independent scientific research and related activities.*

The ECGI will produce and disseminate high quality research while remaining close to the concerns and interests of corporate, financial and public policy makers. It will draw on the expertise of scholars from numerous countries and bring together a critical mass of expertise and interest to bear on this important subject.

The views expressed in this working paper are those of the authors, not those of the ECGI or its members.

www.ecgi.global

european corporate governance institute

ECGI Working Paper Series in Law

Editorial Board

Editor	Amir Licht, Professor of Law, Harry Radzyner Law School, Reichman University
Consulting Editors	Hse-Yu Iris Chiu, Professor of Corporate Law and Financial Regulation, University College London
	Martin Gelter, Professor of Law, Fordham University School of Law
	Geneviève Helleringer, Professor of Law, ESSEC Business School and Oxford Law Faculty
	Kathryn Judge, Professor of Law, Coumbia Law School
	Wolf-Georg Ringe, Professor of Law & Finance, University of Hamburg
Editorial Assistant	Asif Malik, ECGI Working Paper Series Manager

https://ecgi.global/content/working-papers