



Technology Providers and Financial Stability: Overview of Risks and Regulatory Frameworks

Gene Amromin, Cindy Hull, Emma Weiss,
Rebecca Chmielewski, Patty Cowperthwait,
Brett Solimine, Kenekchukwu Anadu,
Falk Braeuning, Siobhan Sanders,
Lorenzo Garza, Sam Schulhofer-Wohl,
Amy Chapel, and Meeoak Cho


June 23, 2025

WP 2025-08

<https://doi.org/10.21033/wp-2025-08>

FEDERAL RESERVE BANK *of* CHICAGO

*Working papers are not edited, and all opinions are the responsibility of the author(s). The views expressed do not necessarily reflect the views of the Federal Reserve Bank of Chicago or the Federal Reserve System.



Technology Providers and Financial Stability: Overview of Risks and Regulatory Frameworks

Gene Amromin, Rebecca Chmielewski, Patty Cowperthwait, Cindy Hull, Brett Solimine, Emma Weiss (FRB Chicago); Kenechukwu Anadu, Falk Braeuning, Siobhan Sanders (FRB Boston); Amy Chapel, Meeoak Cho, Lorenzo Garza, Sam Schulhofer-Wohl (FRB Dallas)¹

June 23, 2025

Abstract

Technology-focused Third-Party Service Providers (TPSPs) have become important players in the operations of financial institutions and the financial markets. This paper summarizes micro- and macro-prudential regulatory frameworks in place to address risks that TPSPs pose to the financial system. The key takeaways are as follows: First, in the U.S., TPSPs operate under limited comprehensive prudential regulatory oversight, aimed primarily at ensuring that their products are safe and resilient on an ongoing basis. Second, while banks rely on multiple TPSPs and hundreds of their services daily for their core banking businesses, U.S. banking supervisors have limited direct visibility into these activities and risks they may pose. Third, although the existing U.S. regulatory framework has some systemic risk considerations, there is no macroprudential structure in place for TPSP risks. Official bodies in other jurisdictions have developed macroprudential frameworks or high-level guidance to address TPSP risks, but their implementation in major economies is nascent at best. Finally, TPSPs are likely an important source of systemic vulnerability for financial institutions and financial markets, although vulnerabilities may be difficult to discern due to a need to assess the criticality of each activity performed by TPSPs and the concentration of TPSPs within that activity.

JEL classification: G10, G23, G28

Keywords: financial stability, third-party service providers, cyber risks

¹ We thank Rachel Grundmeier, Ken Lewis, Fernanda Nechio, and Ned Prescott for helpful comments and suggestions. The views expressed in this paper are those of the authors and do not necessarily reflect the position of the Federal Reserve Banks of Boston, Chicago, and Dallas or the Federal Reserve System.

Introduction

Providers of sophisticated technology have become crucial actors in the operations of financial institutions and financial markets. These technology-based third-party service providers (or TPSPs) offer business solutions to other companies, and their services are embedded across the full range of activities conducted by financial institutions. TPSPs are increasingly a source of interconnectedness as they often provide services to many, sometimes even hundreds, of financial institutions and these services often enable interactions with other financial institutions. TPSPs may also be single points of failure for many financial-sector firms. Both characteristics could create systemic vulnerabilities to the U.S. financial system. The types of TPSPs most in focus for U.S. financial sector regulators have been firms that perform core bank processing functions, facilitate large-value payments, provide information technology infrastructure such as cloud services, and process information about their clients' assets.

In this study, we examine existing regulatory frameworks, both in the United States and internationally, to assess their potential for addressing macro-prudential financial stability risks. This study also includes an overview of the technology-based TPSP sector as well as a case study showcasing one example of financial stability risks that could arise from TPSPs. Our four key takeaways regarding TPSP risks and regulatory frameworks are as follows.

- **First, in the U.S., TPSPs currently operate under limited comprehensive prudential regulatory oversight, aimed primarily at ensuring that their products are safe and resilient on an ongoing basis.** U.S. bank regulators have established programs to supervise TPSPs. However, their authority is limited to requiring that TPSPs address identified risks to their depository institution customers.
- **Second, while banks rely on multiple TPSPs and hundreds of their services daily for their core banking businesses, U.S. banking supervisors have limited direct visibility into these activities and risks they may pose.** The Federal Banking Agencies (FBAs) issued guidance placing direct accountability on the banks for managing risks from their universe of TPSPs.² They also maintain a supervisory program on a small subset of TPSPs utilizing the limited authority provided by the Bank Service Company Act (BSCA) passed in 1962.
- **Third, although the existing U.S. regulatory framework has some systemic risk considerations, there is no macroprudential structure in place for TPSP risks.** International official bodies, including the Financial Stability Board (FSB), the Bank for International Settlements (BIS), and the Group of Seven (G7), have developed macroprudential frameworks or high-level guidance that encourage adoption of approaches to identify, monitor, manage and respond to systemic risks from TPSPs. However, their implementation in major economies is nascent at best.³ Moreover, the

² The Federal Banking Agencies refers to the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation.

³ In the EU, the Digital Operational Resilience Act (DORA) entered into force in January 2023 and became applicable in January 2025. See: The European Parliament and the Council of the European Union, 2022, Regulation on Digital Operational Resilience for the Financial Sector, Brussels, Belgium, December, available online, <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>. In the U.K., the Critical Third Party oversight regime became law in the Financial Services and Markets Act 2023 and a supervisory statement was issued jointly by UK regulators in November 2024. See: the National Archives, 2023, Financial Services and Markets Act 2023, London, UK, available

tradeoffs between fostering technological innovation and mitigating potential financial stability risks arising from such innovation remain an open question.

- **Finally, TPSPs are likely an important source of systemic vulnerability for financial institutions and financial markets.** However, vulnerabilities that TPSPs pose to the broader financial system are especially difficult to discern, as one must assess the criticality of each activity performed by TPSPs and the concentration of TPSPs within that activity. Focusing on TPSP size alone could miss important interconnections arising from, for example, a small TPSP that provides critical services that enable many systemically important financial institutions to interact with other financial institutions, payment systems, or the central bank. Foreign entities could also exploit these vulnerabilities by attacking TPSPs to damage the U.S. financial system.

The remainder of this paper is structured as follows. Section 2 provides an overview of TPSPs and ways they interact with financial institutions. Section 3 summarizes the current U.S. supervisory framework and highlights its key limitations. Section 4 summarizes recommended TPSP regulatory frameworks from the FSB, BIS, and G7. It also compares those recommendations to existing regimes in the U.S., U.K., and European Union (EU). Section 5 highlights a case study that examined the impact of an operational interruption from a cyber event at a TPSP on depository institutions' demand for same-day liquidity at the Federal Reserve's discount window. A conclusion follows, in Section 6.

Section 2. Technology Third-Party Service Providers to Banks: Landscape Overview

Companies have been innovating and offering new technologies to financial services firms for decades. For example, computer loan machines or cash machines (early ATMs) were introduced to banks in the 1960s. Point of sale terminals allowing credit and debit card payments were introduced in the 1970s, providing a big improvement on the carbon paper card imprinters that banks previously used to record card payments.⁴ In the 1980s, core banking platforms – considered the fintech firms of their time – helped banks automate and replace handwritten journals and ledgers.⁵ Computerized financial information systems (e.g., Bloomberg terminals and other market data providers) were introduced in the 1980s to provide financial firms with 24/7 information and data. Today, many firms are focused on transitioning their core infrastructure to cloud service providers.⁶

Today, banks and other financial institutions use thousands of technology-focused TPSPs to execute their routine business activities. Services range from traditional banking activities,

online, <https://www.legislation.gov.uk/ukpga/2023/29/contents>; Bank of England, 2024, Critical Third Parties to the UK Financial Sector, London, UK, November, available online, <https://www.bankofengland.co.uk/prudential-regulation/publication/2024/november/operational-resilience-critical-third-parties-to-the-uk-financial-sector-supervisory-statement>.

⁴ Federal Reserve History. "Electronic Point-of-Sale Payments." September 25, 2024. Available online, <https://www.federalreservehistory.org/essays/electronic-point-of-sale-payments>.

⁵ Sengupta, Niloy, 2023, "The Evolution of Core Banking Platforms: How we got here. What's next?" Kindryl Perspectives on Progress, available online, <https://www.kindryl.com/us/en/perspectives/articles/2023/08/the-evolution-of-core-banking-systems>.

⁶ U.S. Department of the Treasury, 2023. The Financial Services Sector's Adoption of Cloud Services, Washington, DC, February, available online, <https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf>.

such as lending and payments and billing, to money transfers, mortgage servicing, and blockchain activities.

Within this universe of technology service providers, technology firms engage with financial institutions using two primary approaches: traditional and fintech partnerships. The distinction can be thought of as third parties providing services *to* banks, versus third parties providing services *through* banks.

With the traditional approach, technology firms provide products and services that enable banks to deliver banking services to the banks' customers. Examples include core system banking and document imaging and archival services. The landscape has evolved so that today a wide array of TPSPs permeates every business line that banks run, along multiple dimensions. Banks rely on TPSPs to be able to conduct their core business activities. At the same time, there is now a concentration of a small number of TPSPs for several core banking business functions. Any disruption of services from one such TPSP could impact a large number of banks simultaneously, potentially making this provider a "single point of failure" for the banking system more broadly.⁷

Although many parts of the TPSP space may be competitive, transitioning from one service provider to another may be challenging given binding contractual obligations and operational integration with the TPSP. Moreover, the lack of interoperability across TPSPs makes switching or diversifying very costly and nearly impossible to complete in the short-term.⁸ Thus, financial sector firms may have limited bargaining power with their existing TPSPs to demand better services or higher resilience standards.

In a second approach, the fintech partnership, a technology firm engages with a financial institution as a consumer of banking services, most often so that the technology firm can obtain access to financial rails and money movement. In this model, fintech firms provide services directly to customers.⁹ Banking-as-a-service and peer-to-peer lending are examples of this approach.

Section 3. The Current U.S. Third-Party Service Provider Supervisory Framework

Risk management of banks' TPSPs has been an area of supervisory attention for decades. Indeed, interagency regulatory guidance stresses that banks should not outsource risks: banks remain responsible for operating in a safe and sound manner and implementing effective risk management programs even when they engage the services of TPSPs.¹⁰ The Federal Reserve System supervises only a subset of the vast number of TPSPs serving the banking

⁷ Financial Stability Oversight Council, 2024, Annual Report, Washington, DC, December, available online, <https://home.treasury.gov/system/files/261/FSOC2024AnnualReport.pdf>.

⁸ Basel Committee on Banking Supervision, 2024, "Consultative Document: Principles for the sound management of third-party risk," Basel, Switzerland, July, available online, <https://www.bis.org/bcbs/publ/d577.pdf>.

⁹ Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, 2024, "Joint Statement on Banks' Arrangements with Third Parties to Deliver Bank Deposit Products and Services," Washington, DC, July, available online, <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20240725c1.pdf>

¹⁰ Board of Governors of the Federal Reserve System, Division of Supervision and Regulation, 2023, SR 23-4, "Interagency Guidance on Third-Party Relationships: Risk Management," Washington, DC, June, available online, <https://www.federalreserve.gov/supervisionreg/srletters/SR2304.htm>.

industry, which may limit the Federal Reserve’s supervisory visibility into the full range of TPSP activities at a single firm or a single TPSP’s footprint across the banking system.¹¹

Bank Service Company Act

In the U.S., the Federal Reserve, the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, Federal Banking Agencies or FBAs), through the Bank Service Company Act (BSCA) enacted in 1962, have limited authority to regulate and examine TPSPs. Specifically, the BSCA provides statutory authority to the FBAs to regulate and examine activities of third parties that provide services to an insured depository institution and its affiliates to the same extent as if such services were being performed by the depository institution itself. In response to technological challenges faced by banks during the 1960s, the BSCA was enacted to allow banks to purchase and use certain service providers, including those that provided record keeping services.¹² Of the thousands of TPSPs used by banks, only a subset is directly supervised under BSCA authority.¹³

Importantly, the BSCA limits the FBAs to supervising the services performed for the depository institution by the TPSP, *not the TPSP itself*. Additionally, the BSCA also limits the scope of services mainly to those related to traditional banking activities such as check processing, back-office services, and accounting,. Given the speed with which technological innovation occurs, and the heightened concentration and interconnectedness risks noted above, the supervisory authority over third party service providers may be dated and limited in scope.

Service Provider Program

The FBAs’ Service Provider Program (SPP) was established in 1978 to implement the authorities defined in the BSCA. The FBAs adopted interagency guidelines to operationalize the supervision of TPSPs covered by the BSCA; these guidelines were last updated in 2012.¹⁴ According to these administrative guidelines, the FBAs jointly conduct direct supervision, which means that they must come to consensus on the list of TPSPs in the supervision program, supervisory conclusions, and ratings. Within the Federal Reserve, governance for the supervision

¹¹ An interagency technology service provider supervision program incorporates a risk-based process for selecting service providers for inclusion in the program. See Federal Reserve Board of Governors, 2024, “Report to Congress: Cybersecurity and Financial System Resilience Report,” Washington, DC, July, available online, <https://www.federalreserve.gov/publications/files/cybersecurity-report-202407.pdf>. .

¹² Jacob Cunningham, The Limits of the Bank Service Company Act, 74 *Duke Law Journal* 227-268 (2024), available online <https://scholarship.law.duke.edu/dlj/vol74/iss1/4>.

¹³ The FBAs use risk-based factors, such as the number of financial institutions regulated by each agency, to supervise a subset under BSCA authority. See: Federal Financial Institutions Examination Council (FFIEC), IT booklets, Supervision of Technology Service Providers Booklet, Multi-regional data processing servicers (MDPS) Program IT booklet, available online, <https://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers/supervisory-programs/mdps-program/>.

¹⁴ Federal Financial Institutions Examination Council, 2012, IT Examination Handbook, Supervision of Technology Service Providers, October, available online, https://ithandbook.ffiec.gov/media/su0fpuni/ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf.

of the largest, systemically important technology service providers falls under the Division of Supervision and Regulation at the Board of Governors of the Federal Reserve System.¹⁵

FBA enforcement powers

The BSCA provides authority to the FBAs to issue orders as necessary to enable them to administer and carry out the requirements of the statute. The FBAs have entered into consent orders (a form of a binding legal order) with TPSPs. The FBAs appear to cite two types of authority in their consent orders, both the BSCA and a statutory enforcement authority provided by the Federal Deposit Insurance Act (through also naming the TPSPs as “institution affiliated parties.”)¹⁶ As discussed above, the FBAs’ authority under the BSCA, and thus any reliance on the BSCA in the consent orders, would be limited in scope to the *services* performed for the depository institution by the TPS.

In terms of ways in which BSCA oversight has been effective, BSCA examination reports and ratings are made available to their customer depository institutions upon request or automatically if the BSCA rating is below supervisory expectations.¹⁷ Furthermore, the FBAs have recently issued rulemakings for TPSPs to hold them accountable, including the Computer Security Incident Notification final rule from November 2021.¹⁸ This rule sets an expectation for TPSPs to promptly notify their insured depository institution clients of a computer security incident impacting services provided to them. Of note, since the rule does not require the TPSP to notify the FBAs directly, this could lead to delays in FBAs identifying material outages impacting a broad group of institutions.

Section 4. Existing Macro- and Micro-Prudential Approaches to Risks Associated with TPSPs

This section provides an initial scan of the existing approaches to managing the risks associated with TPSPs in the U.S., U.K. and EU, and their alignment with recommended frameworks from international standard-setting bodies (Financial Stability Board (FSB), G7, and Bank of International Settlements).

¹⁵ Specifically, the Federal Reserve's Service Provider Oversight section at the Board conducts direct supervision of Significant Service Providers (SSP) and oversees the supervision of Regional Service Providers (RSP) at Reserve Banks. See Ibid., Federal Financial Institutions Examination Council, 2012, IT Examination Handbook, Supervision of Technology Service Providers, October, available online, https://ithandbook.ffiec.gov/media/su0fpunj/ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf.

¹⁶ Bergin, James P. and Paul Lim, 2024, “The Bank Service Company Act: The Curious Late Life of an Old Law,” July, available online, <https://www.lexisnexis.com/community/insights/legal/b/practical-guidance/posts/the-bank-service-company-act-the-curious-late-life-of-an-old-law>.

¹⁷ See: Federal Financial Institutions Examination Council, 2012, IT Examination Handbook, Supervision of Technology Service Providers, October, available online, https://ithandbook.ffiec.gov/media/su0fpunj/ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf.

¹⁸ See Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Joint Press Release, 2021, “Agencies approve final rule requiring computer-security incident notification,” November, available online, <https://www.federalreserve.gov/newsevents/pressreleases/bcreg20211118a.htm>.

Guidance from international organizations

In the last two years, various international bodies have produced recommendations on how to identify, monitor, manage, and respond to risks from TPSPs, both at the firm level and the financial system level. These recommendations aim to help financial institutions identify and manage critical services and risks and seek to highlight what can be done by financial authorities regarding systemic third-party dependencies and systemic risks.

On the macroprudential side, all frameworks consistently say that financial authorities should have the ability to obtain data to identify third-party dependencies and review financial institutions' registers of critical service providers to understand the landscape and potential risks from criticality or concentration of TPSPs. They also recommend cross-border supervisory cooperation and information sharing. The FSB goes a step further to also recommend designation criteria and designation powers for critical TPSPs, as well as tabletop exercises.

Micro-prudential frameworks are also largely aligned across the FSB, the G7 and the BIS. They include guidance for financial institutions on identifying and monitoring risks from TPSPs, such as establishing a framework for identifying those risks; having clear onboarding and monitoring standards; keeping a register of TPSPs by financial institutions; identifying concentration risks; and monitoring supply chain and concentration-related risks. Frameworks also include guidance on managing and responding to risks by having business continuity plans, managing concentration risks, and laying out clear exit strategies and incident reporting procedures. The FSB has a unique recommendation on having clear regulations for contracts with TPSPs.

Existing approaches in the EU, U.K., and U.S.

Both U.K. and EU financial regulators are close to finalizing the process for designating and overseeing critical TPSPs to the financial sector. They are expected to formally designate some TPSPs as critical beginning in 2025.

- As proposed, the U.K. regime will focus on qualitative designation criteria including materiality of services, concentration of services, and other drivers of systemic impact. The government gained this new authority with the passage of legislation in 2023.¹⁹ The new law gives the U.K. government the ability to designate a TPSP to the U.K. financial services sector as “critical” and gives the financial regulators (the Bank of England, the Prudential Regulatory Authority, and the Financial Conduct Authority) authority to make and enforce rules and to gather information and conduct investigations on designated critical TPSPs. The approach has two main elements. First, a set of six fundamental rules that apply to all services provided to financial sector clients, aimed at managing financial stability risks posed by critical third parties. Second, a set of detailed rules aimed at bolstering the operational resilience of a critical third party’s material services.

¹⁹ HM Treasury, 2024, “Critical Third Parties: Approach to Designation,” March, available online, https://assets.publishing.service.gov.uk/media/65fbf692703c42001a58f10d/HM_Treasury_Approach_to_Designating_Critical_Third_Parties_2024.pdf.

- The EU’s Digital Operational Resilience Act (DORA) regime, on the other hand, lays out six quantitative criteria and five qualitative criteria, all of which must be met to trigger a designation.²⁰ In DORA, detailed requirements with respect to expectations for critical TPSPs have not yet been set out, with the focus instead being on the European Supervisory Authorities’ new powers to launch investigations. Major cloud service providers and market data providers are expected to be in scope for both the U.K. and EU regimes. DORA also contains a requirement that critical TPSPs establish a specific subsidiary in the EU, though it may provide services from outside the EU.

In contrast to the U.K. and EU, there is currently no U.S. framework for macroprudential oversight of TPSPs. Applicable federal regulatory requirements place responsibility for effective management of technology operations and related risks on financial institutions, regardless of whether services are outsourced to third parties.²¹ The U.S. FBAs have limited authority to supervise TPSPs of insured depository institutions at the micro-prudential level, and the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) have implemented regulations and safeguarding requirements for certain entities under their jurisdictions for systems that directly support some trading and market-related systems.

The Financial Stability Oversight Council (FSOC) has broad responsibilities to assess, monitor, and mitigate risks to U.S. financial stability.²² Included in this is the authority to designate nonbank financial companies as requiring consolidated supervision and enhanced prudential standards under section 113 of the Dodd-Frank Act (and financial market utilities under Title VIII and certain bank holding companies under section 117) as well as the authority to designate certain payment, clearing, and settlement activities for additional regulation.²³

Some public-private partnerships and interagency groups exist to enable cooperation around TPSP issues, but these groups lack authority to set and enforce rules. Financial and Banking Information Infrastructure Committee (FBIIC) member agencies coordinate on operational issues related to critical infrastructure and cybersecurity matters within the financial services sector.²⁴ Similarly, the Treasury Department’s Office of Cybersecurity and Critical Infrastructure Protection works closely with financial sector companies, industry groups, and government partners to share information about threats and vulnerabilities, encourage the use of baseline protections and best practices, and respond to and recover from significant incidents. In a 2023 report on cloud services, however, the Treasury Department noted that a lack of

²⁰ See: The European Parliament and the Council of the European Union, 2022, Regulation on Digital Operational Resilience for the Financial Sector, Brussels, Belgium, December, available online, <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>.

²¹ U.S. Department of the Treasury, 2023. The Financial Services Sector’s Adoption of Cloud Services, Washington, DC, February, available online, <https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf> p. 31.

²² Financial Stability Oversight Council, “Council Work,” available online, <https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/financial-stability-oversight-council/council-work>.

²³ Financial Stability Oversight Council, “Designations,” available online, <https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/designations>.

²⁴ FBIIC (Financial and Banking Information Infrastructure Committee) is composed of 18 federal and state financial regulatory agencies and is chaired by Treasury. More information available online at <https://www.fbiic.gov/>.

aggregated data to assess concentration is a barrier to understanding the potential impact of an operational incident on a cloud services provider on the financial sector.²⁵

Figures 3 and 4 below present cross-jurisdictional comparisons of macroprudential and micro-prudential frameworks and existing approaches, respectively.

Figure 3: Financial system-level guidance and regulatory powers and capabilities²⁶

		Guidance / recommendations			Regulatory powers/capabilities			
		FSB	G7	BIS/BCBS	UK	EU DORA	US Interagency Guidance (2023)	US: BSCA (1962)
Identify	Designating some providers as critical from a financial stability perspective	Yes	No	No	Yes	Yes	No	Yes
	Criteria for identifying TPSPs and their risks	Yes	No	Yes	Yes	Yes	No	No
Monitor	Obtain data to identify third-party dependencies	Yes	Yes	Yes	Yes	Yes	No	Yes
	Review financial institutions' registers	Yes	Yes	Yes	Yes	Yes	No	No
	Oversee risks associated with TPSPs		Yes	Yes	Yes	Yes	Yes	Yes
Manage (ex-ante)	Dialogue between authorities, institutions, and service providers	Yes	Yes	Yes	Yes	Yes	No	Yes
	Sector-wide tabletop exercises - joint assurance activities (tabletop exercises)	Yes	No	No	Yes	Yes	No	No
	Incident response coordination frameworks	Yes	Yes	No	Yes	Yes	No	Yes
	Incident reporting	Yes	NA	No	Yes	Yes	No	Yes
Respond (ex-post)	Cross-border supervisory cooperation and information sharing	Yes	NA	Yes	Yes	Yes	No	No

²⁵ U.S. Department of the Treasury, 2023. The Financial Services Sector's Adoption of Cloud Services, Washington, DC, February, available online, <https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf>.

²⁶ Sources for Figures 3 and 4: authors based on public documents including the following: Financial Stability Board, 2023, "Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities," December, available online: <https://www.fsb.org/uploads/P041223-1.pdf>; G7, 2022: G7 FUNDAMENTAL ELEMENTS FOR THIRD PARTY CYBER RISK MANAGEMENT IN THE FINANCIAL SECTOR, October, available online: https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2022-G7-fundamental-elements-for-third-party-cyber-risk-management-in-the-financial-sector.en.pdf; Basel Committee on Banking Supervision, 2024, "Consultative Document: Principles for the sound management of third-party risk," Basel, Switzerland, July, available online, <https://www.bis.org/bcbs/publ/d577.pdf>; Bank of England, 2024, Critical Third Parties to the UK Financial Sector, London, UK, November, available online, <https://www.bankofengland.co.uk/prudential-regulation/publication/2024/november/operational-resilience-critical-third-parties-to-the-uk-financial-sector-supervisory-statement>; The European Parliament and the Council of the European Union, 2022, Regulation on Digital Operational Resilience for the Financial Sector, Brussels, Belgium, December, available online, <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>; Board of Governors of the Federal Reserve System, Division of Supervision and Regulation, 2023, SR 23-4, "Interagency Guidance on Third-Party Relationships: Risk Management," Washington, DC, June, available online, <https://www.federalreserve.gov/supervisionreg/srletters/SR2304.htm>; and 12 USC Ch. 18: BANK SERVICE COMPANIES available online, <https://uscode.house.gov/view.xhtml?path=/prelim@title12/chapter18&edition=prelim>.

Figure 4: Financial institution-level guidance and regulatory powers and capabilities

		Guidance / recommendations			Regulatory powers/capabilities			
		FSB	G7	BIS/BCBS	UK	EU DORA	US Interagency Guidance (2023)	US: BSCA (1962)
Identify	Establish a framework	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Onboarding and monitoring standards	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Register of TPSPs by financial institution	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Identify concentration risks	Yes	Yes	Yes	Yes	Yes	No	Yes
Monitor	Service providers' supply chains	Yes	Yes	Yes	Yes		Yes	Yes
	Concentration-related risks	Yes	Yes	Yes	Yes	Yes	No	Yes
Manage (ex-ante)	Business continuity plans	Yes	Yes	Yes	Yes	Yes	Yes	No
	Clear regulations regarding contracts with critical TPSPs	Yes	No	No	No	Yes	No	No
	Manage concentration risks	Yes	Yes	Yes	Yes	Yes	No	Yes
	Exit strategies	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Supervisory powers to directly oversee provision of services by financial institutions to critical TPSPs	Yes	NA	No	Yes	Yes	N/A	N/A
Respond (ex-post)	Incident reporting	Yes	Yes	No	Yes	Yes	Yes	Yes

Section 5. Case study: Cyber and Operational Risks Originating from TPSPs

The paper “Cyberattacks and Financial Stability: Evidence from a Natural Experiment”, is one of few existing empirical evaluations of spillovers from a TPSP-centered cyberattack to the banking sector.²⁷ This study is unique in highlighting the linkages between risk events from TPSPs, risk management tools available to depository institutions, and Federal Reserve operations. During this event, the Federal Reserve was both an impacted party and a source of liquidity and operational support. Many firms were not able to process payments in Fedwire,²⁸ and banks obtained liquidity by borrowing from the discount window²⁹ during the event. The study also revealed heterogeneity in bank responses, as small banks were the most frequent users of the discount window while larger banks relied on market-based funding. The date of the event and other details were withheld to protect the confidentiality of the affected parties.

²⁷ “Cyberattacks and Financial Stability: Evidence from a Natural Experiment”, FEDS Notes, May 2022, Antonis Kotidis and Stacey L. Schreft., available online, <https://doi.org/10.17016/FEDS.2022.025>.

²⁸ Fedwire is a real-time, gross settlement payment system owned and operated by the Federal Reserve Banks and used by financial institutions, businesses, and government agencies to make large-value payments. For more information, see: The Federal Reserve, “Fedwire Funds Service,” available online, <https://www.frb services.org/financial-services/wires>.

²⁹ The “discount window” refers to Federal Reserve lending to depository institutions to support the liquidity and stability of the banking system and the effective implementation of monetary policy. For more information, see: The Federal Reserve, Discount Window | Payment System Risk, available online, <https://www.frbdiscountwindow.org/>.

Description of event

A TPSP involved with providing payment services to banks was hit with a cyberattack. Once discovered, this TPSP took its computer systems offline to limit the damage. In consequence, some bank customers of the TPSP lost the ability to send payments over Fedwire using their usual processes. The affected banks had backup processes available for accessing Fedwire, but those processes were more time-consuming to use, and the banks generally did not switch over to them quickly. The TPSP outage lasted several days.

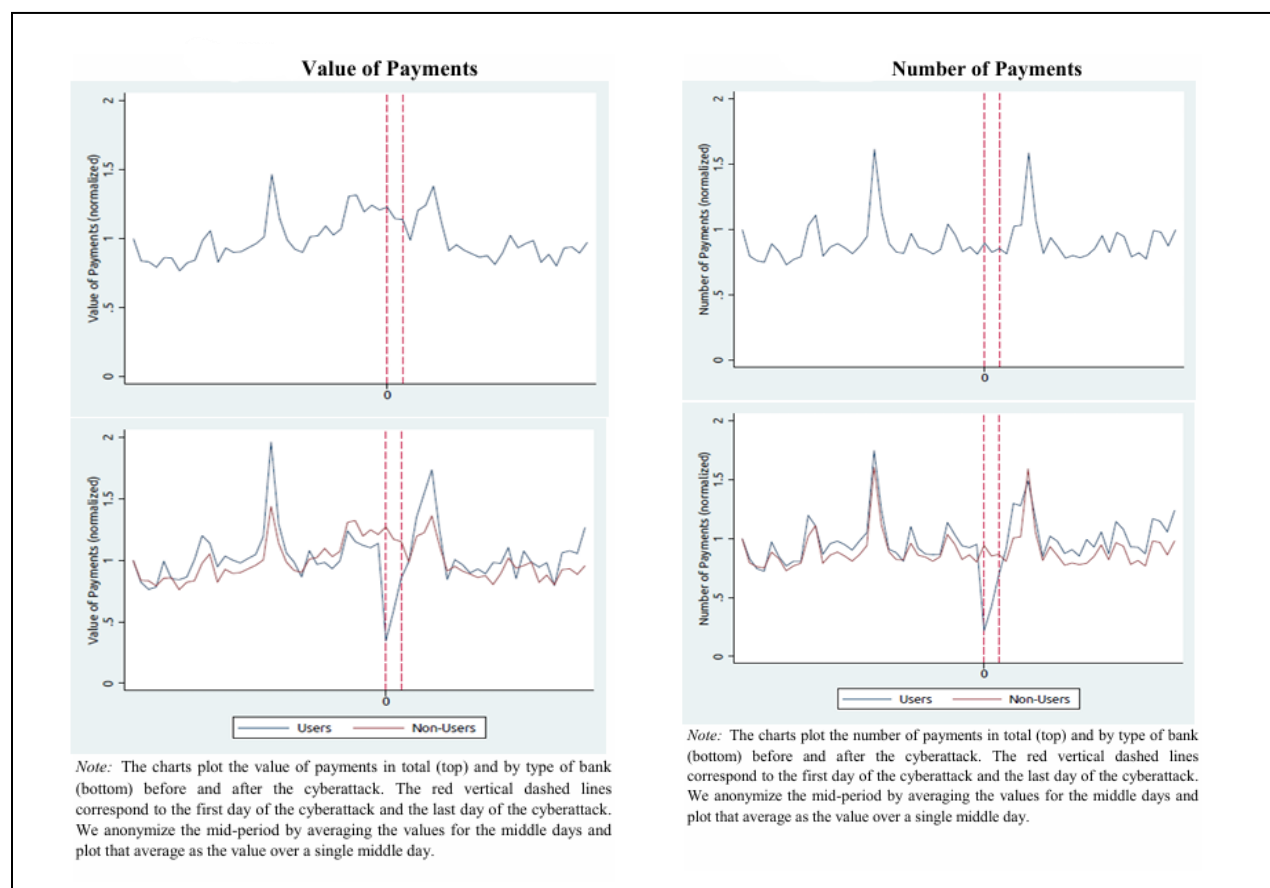
How banks responded

The directly affected banks sent fewer payments; other banks that expected to receive these payments had fewer incoming payments during the cyberattack. The receiver-banks, however, were able to make *their* outgoing payments either because the Federal Reserve provided liquidity via the discount window, they found other sources of liquidity in the open market, or they had sufficient excess reserves when the event occurred.

- Relatively smaller banks were more likely to tap the discount window for funding; this was especially true for those with relatively fewer reserves as a share of their assets.
- In contrast, relatively larger banks borrowed from the fed funds market, with the exception of a few very large banks that had a high share of reserves relative to total assets. The authors found that those very large banks were more likely to draw down their own reserves on the first and subsequent days of the cyberattack.

Data comparing TPSP users vs. non-users shows that the cyberattack had a material impact on the number and volume of payments made on users, but little to no impact on non-users (see Figure 5). It appears that interventions by the Federal Reserve – both as a provider of contingent liquidity and an operator of Fedwire – and actions by user and non-user banks to shore up liquidity prevented the cyberattack from becoming a financial stability event.

Figure 5: Value and number of payments made via Fedwire during cyberattack event³⁰



This case study highlights three key themes of cyber and operational risk events that originate at TPSPs.

- First, interconnectedness of TPSPs is a key source of vulnerability across the financial system, including the banking sector, financial markets, and payment systems. More data and analysis on interconnectedness and concentration risk will be helpful in monitoring these types of vulnerabilities in the financial system.
- Second, a financial firm's TPSP-related operational risk events can quickly create liquidity risks, which can have cascading effects to the financial system more broadly. Financial institutions have varying capabilities and tools to address sudden liquid demands from these types of events.
- Finally, routine maintenance and tests of business continuity plans by both TPSPs and financial institutions reliant on TPSPs for critical services are key for improving individual firm resilience and response capabilities and for preventing spillovers to the financial system more broadly.

³⁰ "Cyberattacks and Financial Stability: Evidence from a Natural Experiment", FEDS Notes, May 2022, Antonis Kotidis and Stacey L. Schreft, available online <https://doi.org/10.17016/FEDS.2022.025>.

Section 6. Conclusion and next steps

Financial institutions and financial markets increasingly rely on TPSPs for their operations. Regulatory frameworks are evolving in some major jurisdictions, but the lack of visibility surrounding TPSP relationships with financial institutions makes it difficult to discern the extent to which TPSPs can present systemic risks. In the U.S., the regulatory regime for TPSPs relies more on industry working groups and public-private partnerships, a contrast to more formal oversight regimes recently introduced in the EU and U.K. Compared with international guidance to the financial system on the supervision of TPSPs, the U.S. approach is more focused on micro-prudential oversight. The case study presented above highlights financial stability risks from a payments-related disruption that originated at a TPSP. Rapid technology adoption forcing changes in the financial sector landscape could further increase financial system vulnerabilities to TPSPs from concentration and interconnectedness. Further research is needed to better understand financial system vulnerabilities arising from TPSPs and potential implications for oversight of these firms.

Appendix 1: List of Acronyms

ATM	Automated Teller Machine
BCBS	Basel Commission on Banking Supervision
BIS	Bank for International Settlements
BSCA	Bank Service Company Act
CFTC	Commodity Futures Trading Commission
DORA	Digital Operational Resilience Act
EU	European Union
FBA	Federal Banking Agencies
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FRB	Federal Reserve Board
FSB	Financial Stability Board
FSOC	Financial Stability Oversight Council
G7	Group of Seven
OCC	Office of the Comptroller of the Currency
RSP	Regional Service Providers
SEC	Securities and Exchange Commission
SPP	Significant Service Providers
TPSPs	Third-party service providers
U.K.	United Kingdom
U.S.	United States