THE PROPAGATION OF CYBERATTACKS THROUGH THE FINANCIAL SYSTEM: EVIDENCE FROM AN ACTUAL EVENT*

Antonis Kotidis[†] and Stacey L. Schreft[‡]

March 19, 2023

Abstract

This article uses confidential datasets to quantify the effects of a multiday cyberattack on a shared technology service provider (TSP) to the banking sector. The TSP went offline—a common shock that disrupted its customers' ability to send payments (the first-round effect). Banks and the TSP reduced this effect by more than half with their business continuity plans. Nevertheless, through contagion, other banks experienced a material shortfall of liquidity, causing them to borrow, including from the Federal Reserve, or tap their reserves (second-round effect). By also sending payments after business hours, they avoided further contagion (third-round effect).

JEL Classification Codes: E42, E58, G21

Keywords: cybersecurity, payments, financial network, automation, digitization, outsourcing

For correspondence: Federal Reserve Board of Governors, Attn: Antonis Kotidis, 20th & Constitution, N.W., Washington, DC 20551, <u>antonis.kotidis@frb.gov</u>

^{*} This paper was previously distributed as "Cyberattacks and Financial Stability: Evidence from a Natural Experiment." We are deeply grateful to Andreas Lehnert, Beth Klee, and Jill Cetina for their support and comments at various stages of this project. We also thank Gara Afonso; Filippo Curti; Adam Copeland; Thomas Eisenbach (discussant); Jeff Gerlach; Laura Kodres (discussant); Anna Kovner; Pete Kyle (discussant); Michael Lee; Kris Natoli; Margaux MacDonald; Francesco Vallascas (discussant); Baozhong Yang (discussant); Peter Zimmerman (discussant); and participants at the Columbia SIPA/Federal Reserve Bank of New York seminar series; European Systemic Risk Board's 2022 Cyber Workshop; Federal Reserve Bank of Chicago seminar series; Federal Reserve Bank of Atlanta and Georgia State University 2022 Financial Stability Conference; MIT Golub Center for Finance and Policy 9th Annual Conference; European Banking Association Policy Research Workshop; Office of the Comptroller of the Currency 2022 EconFINTECH Symposium; Federal Reserve Bank of Cleveland and Office of Financial Research 2022 Financial Stability Conference; and Federal Reserve Bank of Philadelphia, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency 2022 Interagency Risk Quantification Forum for helpful discussions. Tristan D'Orsaneo provided outstanding research assistance. The views expressed in this paper are those of the authors and do not necessarily reflect the position of the Board of Governors of the Federal Reserve System, the Office of Financial Research, or the U.S. Treasury Department.

[†] Board of Governors of the Federal Reserve System

[‡] Board of Governors of the Federal Reserve System and U.S. Treasury Office of Financial Research

I. Introduction

The disruption of communications infrastructure has long been a risk for the financial system, as has financial institutions' reliance on outsourced service providers (FBIIC, 2003). Digitization dramatically increases the volume and speed of information flows, allowing the modern financial system to better achieve its potential (Petralia et al., 2019; Pierri and Timmer, 2022). To take full advantage of digitization, financial institutions are increasingly outsourcing core banking functions to third-party technology service providers (TSPs) that offer software, platforms, and infrastructure as a service.

The unprecedented digital transformation in the financial system brings benefits in scalability, flexibility, and cybersecurity because TSPs can invest more heavily in security than individual financial institutions. At the same time, it brings new risks (Vives, 2019). A TSP may be a more attractive target for a cyberattack, and operational outages at the TSP can be a common shock that disrupts operations directly at many financial institutions and indirectly at others through contagion (Financial Stability Board, 2019; Asensio, Bouveret, and Harris, 2022). Cyberattacks are of special concern because, unlike other operational risks, they can be timed and targeted for maximum effect, and traditional mitigants like capital and liquidity may not prevent them from being disruptive and forcing firms to conduct business manually (Brando et al., 2022).¹ Financial institutions invest in cybersecurity and business continuity plans (BCPs) to provide resilience in the wake of a cyberattack (U.S. Congress House Committee on Financial Services, 2015). Nevertheless, 63% of financial institutions reported destructive cyberattacks in 2021, up 17% from 2020. Moreover, 60% reported an increase in island hopping, where an attacker targets a TSP and uses that intrusion to hop to the TSP's customers (Kellermann, 2022). Consequently, cyberattacks have emerged as a new threat to financial stability that concerns policymakers (Lagarde, 2018;

¹ For example, the January 2023 attack on ION Trading UK "forced several European and U.S. banks and brokers to process trades manually." StoneX Financial Ltd. Reported being "unable to perform due diligence on payments and transfer requests," which delayed its provision of clearing and execution services (Almeida, Burton, and Doherty, 2023). Operational risk is often thought of as being idiosyncratic, but evidence from bank holding companies has found it to increase systemic risk (Berger et al., 2022), and cyberattacks on TSPs certainly bring that risk.

Powell, 2019; Powell, 2021), as well as academics (Duffie and Younger, 2019; Kashyap and Wetherilt, 2019).

Against this background, this article analyzes a unique multiday cyberattack that disrupted the operations of a major TSP on which some banks relied for core banking services.² When the TSP discovered the cyberattack, it took its computer systems offline to limit the damage, thereby creating a common shock to its customers.³ Some bank customers of the TSP ("users") lost the ability to send payments to the Fedwire payment system in their usual way, which was through the TSP. Fedwire offers several other methods, all more manual and time-consuming, for sending payments, and users had to switch to them.⁴ In contrast, other banks that were not reliant on the TSP and affected by the service outage ("non-users") remained able to send payments through Fedwire with their usual processes.

Although the cyberattack did not disrupt the functioning of the overall financial system, it had a material impact on individual financial institutions. The common shock from the TSP's service outage disrupted users' ability to send payments (*the first-round effect*), which in turn disrupted payments received by non-users of the TSP, leaving them with fewer reserves available for sending their own payments. The drop in non-users' reserves was sufficiently material for them to seek other sources of funds (*the second-round effect*). In addition, non-users sent payments after normal business hours to avoid sending materially fewer payments themselves, which could have disrupted yet other non-users' ability to send payments (*the third-round effect*). This article quantifies significant first- and second-round effects, as well as how various BCPs and Federal Reserve operational support and liquidity provision dramatically mitigated those effects and muted the third-round effect to avoid broader financial instability.

² The confidentiality of the cyberattack is maintained by not referring to the TSP's name or locations; not specifying the dates, weekdays, or duration of the cyberattack; and not describing the nature of the attack.

³ Cybersecurity requires defending against, discovering, responding to, and recovering from cyberattacks. Here, "cyberattack" refers to the active intrusion and the disruption of the TSP's systems. This captures the fact that the TSP's taking its systems offline can be more disruptive than the period when the attacker is inside the TSP's systems. ⁴ Cyberattacks commonly result in victims taking their computer systems offline and switching to manual processes to avert a complete shutdown in operations (for example, Copper Mountain Mining Corporation, 2022).

The empirical analysis exploits a number of daily confidential, transactions-level datasets that allow analysis of users' and non-users' behavior as senders of payments (senders initiate payments) and receivers of payments, whichever is appropriate for the round being studied. The analysis starts with a difference-in-differences model to study the first-round effect of the common shock on the ability of users (the treatment group) to send payments relative to non-users (the control group). On the first day of the cyberattack, which was the worst day, users as senders of Fedwire payments sent 33% (46%) fewer payments in number (value) compared with non-users. Over the subsequent days of the cyberattack, the drop in payments sent by users gradually decreased but remained statistically significant.

Despite this sizable first-round effect for users, the cyberattack did not disrupt the functioning of the payments system. Overall, it disrupted just 0.32% of all Fedwire payments on the first day. Two factors contributed to this outcome. First, although the TSP was a major firm (and a potential bottleneck for users (Carvalho, Elliott, and Spray, 2022), Fedwire payments are concentrated in the U.S. global systemically important banks (G-SIBs), who usually send payments directly to Fedwire. Consequently, although users on average were fairly large, they did not account for a large share of Fedwire payments.⁵ Second, and more important for capturing the lessons of this cyberattack, the muted effect results from numerous mitigating actions taken by the private (the TSP and the banks) and official (the Federal Reserve) sectors.

Starting with the TSP, once it went offline, its priorities were ensuring that its computer systems were free from malware and, once that was done, restoring customers' access to its systems. Although the TSP did not restore service to a sizable number of users until the last day of the attack, that restoration resulted in 62% fewer Fedwire payments being disrupted that day. This result highlights an important conclusion: that while a shared TSP can be the single point of failure, its prompt response to restore services can substantially reduce fragility and contagion.

Users' mitigating actions began with their switching to other ways to send payments. Had users not switched, they would not have sent any payments (the drop in payments sent would have been

⁵ In particular, ten banks are responsible for 60% of all Fedwire payments.

100%), and the overall share of Fedwire payments disrupted on the first day of the attack would have been 0.7%, more than twice the 0.32% attributed to the attack. However, users did not switch quickly or smoothly to other processes, which are low cost but more manual, requiring users to be pre-authorized for access and able to verify their identity. Each day of the event, although users did not face a shortage of funds, they got a slow start sending payments and sent far fewer payments throughout the business day. The Federal Reserve granted requests to extend Fedwire's operating hours into the evening, which gave users more time to send payments. On the first day of the cyberattack, for example, users sent 6% more payments by value because of Fedwire's extended hours, but not a larger number of payments. This implies that users prioritized sending larger payments later in the business day, which is another BCP from a systemic perspective because it keeps more funds flowing through the payment system.⁶ The empirical analysis confirms that on the first day, the average payment sent by users was larger in the afternoon and evening. On later days, the average payment size remained significantly larger in the afternoon but not the evening. Taken together, these results highlight that resilience to supply-chain shocks can emerge from having low-cost BCPs associated with granular steps in production processes. Multisourcing TSPs was not among those BCPs (for reasons described in Section III) and contrary to the focus of the theoretical literature on optimal supply chain resilience, which abstracts from details of production processes (Elliott and Golub, 2022; Elliott, Golub, and Leduc, 2022).

After establishing the first-round effect of the common shock on users and the importance of their BCPs, this article turns to quantifying the second-round effect—whether non-user banks, those not reliant on the TSP to send payments, received fewer payments than they otherwise would have, and if so, whether their liquidity was impaired enough for them to tap other sources of funds to compensate. Because banks rely heavily on incoming payments to send their own payments (Afonso et al., 2022), but vary in their normal reliance on incoming payments from users, the second-round analysis uses an exposure variable that measures a non-user's share of incoming

⁶ A similar situation arose on September 11, 2001, from the terrorist attacks in New York: banks sent larger, but not more, payments in the evening, which helped payments flow through the system (McAndrews and Potter, 2002).

payments from users in the weeks before the cyberattack and focuses on exposed receiver-banks, those non-users with positive exposures in their role as receivers of payments from users. In other words, the exposure variable is constructed to capture the scope for contagion through the payments network. The analysis finds that a 1% increase in a receiver-bank's exposure is associated with a 0.7% decrease in incoming payments from users on the first day of the cyberattack. The effect is about half as large and still statistically significant in the mid-period of the cyberattack, but not on the last day.

How exposed receivers responded to the disruption in their incoming payments depended on their size and reserves, reflecting the role of liquidity buffers and consistent with the literature on which banks borrow in the federal funds market and at the discount window.⁷ Relatively smaller banks, especially those with less available liquidity as measured by their reserves relative to total assets, were more likely to tap the discount window, taking advantage of the Federal Reserve's role as a lender of last resort. In contrast, relatively larger banks borrowed from the interbank market, with the exception of the largest of the large banks, which are required to hold additional liquidity buffers. Those very large banks saw their reserves decrease during the cyberattack and significantly on the first day, suggesting that they were able to tap those buffers to address any shortfall in incoming payments. All of these actions have costs, either the cost of borrowing funds or the opportunity cost of using liquidity buffers. The fact that exposed receivers incurred those costs supports the conclusion that the shortfall in liquidity they experienced was material.

Finally, this article considers whether the cyberattack propagated further, creating a thirdround effect and broader contagion. Payments sent by exposed receivers were relatively low and almost statistically significant. In contrast to normal days, these banks sent more payments each evening during the attack, using Fedwire's extended hours to make up for the delays during the business day. This helped them avoid a significant drop in their payments sent and further disruptive contagion.

⁷ Ashcraft, McAndrews, and Skeie (2011) shows that smaller banks are less likely to access the fed funds market for funding and more likely to borrow from the discount window. Ennis and Klee (2021) shows that discount window borrowing is larger for banks with relatively fewer reserves.

II. Related Literature

This article contributes to several literatures. Most directly, it contributes to the relatively new literature on cybersecurity and financial stability. Most cyberattacks on the financial system have been contained, hours-long events, precluding the identification of the effect and any policy response, even in cases where data on the event are available. As such, the existing literature has largely described, without quantifying, the transmission channels through which cybersecurity events might impair the financial system (Boer and Vasquez, 2017; ESRB, 2020; Healey et al., 2018; Kopp, Kaffenberger, and Wilson, 2017; Office of Financial Research, 2017; Ros, 2020; Schreft and Zhang, 2018; Warren, Kaivanto, and Prince, 2018).⁸ The exceptions have quantified hypothetical cyberattacks (Duffie and Younger, 2019; Eisenbach, Kovner, and Lee, 2022). These exercises quantify how cyberattacks might be transmitted through the financial system, but beyond the effect of the assumed initial shock, the contagion studied hinges on the assumptions made about how banks react during the attack and in the absence of any BCPs. More recently, BCPs have been central in models of optimal cybersecurity investment when digital infrastructure is shared (Ahnert et al., 2022; Anand, Duley, and Gai, 2022). This article contributes to the literature by being the first to study an actual multiday cyberattack, which allows quantification of the effect of the common shock and the subsequent contagion.⁹ The analysis captures how banks' use of their BCPs and official sector assistance mitigated the cyberattack's effect. The applicable BCPs were low cost, and their use dramatically mitigated the disruption from the cyberattack. However, they were not sufficient to fully prevent contagion from users to non-users. Although the focus of the article is on the financial sector, its lessons apply to other sectors of the economy, as disruptive cyberattacks have become commonplace.

⁸ Other papers estimate the cost of cyberattacks (Aldasoro et al., 2020; Bouveret, 2019; Council of Economic Advisors, 2018; Gogolin, Lim, and Vallascas, 2021; Wellburn and Strong, 2019) and whether stock prices reflect the potential losses (Jamilov, Rey, and Tahoun, 2021; Florackis et al., 2023; Kamiya et al., 2021).

⁹ Another paper quantifying the effect of a cyber event is Crosignani, Macchiavelli, and Silva (2023), which studies the NotPetya attack. NotPetya did not affect financial firms directly, but the paper finds that access to bank credit lines and the use of trade credit mitigated the damage done.

This article also contributes to the long and largely theoretical lines of literature on externalities in the financial system. The modern financial system is a complex network that allows for the diversification of risk but also creates channels for contagion that can threaten financial stability (Allen and Gale, 2000; Lagunoff and Schreft, 2001; Eisenberg and Noe, 2001; de Vries, 2005; Gai and Kapadia, 2010; Gai, Haldane, and Kapadia, 2011; Caballero and Simsek, 2013; Brunnermeier and Oehmke, 2013; Elliott, Golub, and Jackson, 2014; Acemoglu, Ozdaglar, and Tahbaz-Salehi, 2015; and Erol and Vohra, 2022). This literature has considered systematic risk from common shocks to financial networks and from bad shocks propagating through the financial system. It has explored how various contagion channels, network structures, and shocks contribute to the fragility of the system. Another line of the literature has found that core-periphery network structures can arise in equilibrium but bring systemic risk because the core can propagate stress throughout the network. The payment system has a complex core-periphery structure with Fedwire at its core (Ashcraft and Duffie, 2007; Soramäki et al., 2007; Afonso and Lagos, 2015; Denbee et al., 2021; Bianchi and Bigio, 2022). Any disruption to the ability of banks to send payments is a potential financial stability risk (McAndrews and Rajan, 2000; Armentier, Arnold, McAndrews, 2008; Klee, 2010; Afonso and Shin, 2011; Afonso, Kovner, and Schoar, 2011; Afonso et al., 2022).¹⁰ This article brings this literature to life by quantifying the effect of an actual common shock (from a cyberattack) to the banking system and the associated amplification and contagion through the Fedwire payment system. It takes a step beyond the existing literature by quantifying these effects with and without banks' BCPs and official-sector support that mitigated some of the externalities.¹¹

Finally, the structure of financial networks is made more complex by financial institutions'

¹⁰ This network has been disrupted in the past by events that affected access to Fedwire and required Federal Reserve intervention (for example, the September 11, 2001, terrorist attacks; the software failure at Bank of New York in 1985) (McAndrews and Potter, 2002; Lacker, 2003; Ennis and Price, 2015). The payment system's relevance for bank lending, inflation, and the transmission of monetary policy means that such disruptions can affect the macroeconomy more generally (Parlour, Rajan, and Walden, 2022; Piazzesi and Schneider, 2021).

¹¹ Despite the rich theoretical literature, identification of the propagation of actual shocks through financial networks remains largely unexplored because of a lack of data. A related empirical literature emphasizes the role of production networks as a mechanism for shocks' propagation and amplification (for example, Barrot and Sauvagnat (2016); Boehm, Flaaen, and Pandalai-Nayar (2019); and Carvalho et al. (2021)).

outsourcing parts of their operations to TSPs (Duffie et al., 2022). This compounds risks to financial stability in three related ways covered in the literature.¹² First, financial institutions are susceptible to additional common shocks through their shared TSPs and to new channels of contagion through their digital technology supply chain and its interactions with their traditional supply chains (Elliott, Golub, and Leduc, 2022). Second, financial institutions' decision to invest in cybersecurity is subject to a classic principal-agent problem (Shleifer and Vishny, 1997; Goyal and Vigier, 2014; Acemoglu, Malekian, and Ozdaglar, 2016; Kashyap and Wetherilt, 2019; Aldasoro et al., 2020; Ahnert et al., 2022; Anand, Duley, Gai, 2022; Asensio, Bouveret, and Harris, 2022). With some core bank technology services outsourced, cybersecurity becomes a shared responsibility between banks and their service providers. The TSP may provide better cybersecurity than any individual bank and can serve as a gatekeeper through which cyber attackers have to pass to penetrate banks' systems.¹³ At the same time, banks have an incentive to free ride and underinvest in monitoring the TSP and investing in their own cybersecurity. This problem is amplified when the TSP's cybersecurity is unobservable. Third, when firms face considerable switching costs in replacing a TSP, they are likely to continue outsourcing from the same vendor, which can make markets less competitive (Farrell and Klemperer, 2004; Lewis and Yildirim, 2005; Whitten, Chakrabarty, and Wakefield, 2010). Financial institutions' efforts to get better terms from vendors, given that banks recognize the switching costs, can discourage standardization across vendors, resulting in a lack of interoperability that further raises switching costs. When switching is unlikely, TSPs' incentives to provide better cybersecurity to retain customers and financial institutions' incentives to monitor TSPs are lessened.

This article adds to these strands of the literature on outsourcing risk by quantifying the effect of a cyberattack on the digital technology supply chain that had ramifications for the financial

¹² Cybersecurity risk in supply chains, regardless of industry, remains a fairly new area of research (Ghadge et al., 2020). Policymakers, however, recognize these risks and encourage the monitoring of outsourced vendors (Financial Stability Board, 2020; BoG, FDIC, and OCC, 2020; BoG, 2021).

¹³ Banks' use of TSPs to provide core bank services is commonly viewed as essential for banks to remain current with changing technology and cybersecurity needs and to avoid the complexity of legacy computer systems that require maintenance and updating to interact with new technologies and remain competitive (EY 2019).

system. The attack served as a common shock on the banks using the TSP, and through those banks' reactions, disrupted liquidity at other banks that did not use the TSP. A lack of interoperability in TSPs' systems and the high cost of those systems meant that it was not cost-effective or even feasible for the banks to be customers of multiple TSPs and treat them as backups for each other, although much literature focuses on multisourcing as a BCP (Sheffi and Rice, 2005; Elliott and Golub, 2022).¹⁴ While the literature focuses on the cybersecurity investment decision, this study highlights how the use of many low-cost BCPs can dramatically increase network resiliency.

III. Description of the Cyberattack

The cyberattack effectively started when the TSP discovered the attack on its computer network and disconnected affected servers from the internet. It effectively ended when the TSP was back online and enough of its customers could access its services.¹⁵ The TSP's taking its servers offline served as a common shock to user banks that prevented them from sending Fedwire payments in their usual and preferred way.¹⁶ Non-users faced no similar operational disruption.

There were more than 50 users, which is important for the clustering of standard errors in the empirical analysis. For simplicity, this article refers to users as banks, although some credit unions and other financial institutions, all sending Fedwire payments, are included in the group. The average user was a top decile U.S. bank by assets and larger than the average non-user (Figure I), even though the U.S. G-SIBs, which send the vast majority of Fedwire payments, were non-users.

Faced with the TSP's service outage, users' BCPs would have had them switch to using one

¹⁴ King (2021) illustrates the costs and obstacles faced by a depository institution in switching TSPs.

¹⁵ The cyberattack may have occurred earlier and had a hidden phase (Kashyap and Wetherilt, 2019) during which it was either not discovered or not realized to require a response. The empirical analysis checks for this possibility. Likewise, remediation and recovery from the cyberattack (such as making improvements to cybersecurity and dealing with related litigation) may have occurred later than the end date used in this article.

¹⁶ Appendix Figure I illustrates the propagation of a cyberattack, like the one studied, through the payment system. Bank 3 (a user of the TSP) loses its connection to Fedwire and cannot send \$100 payment, which leaves Bank 4 (a non-user of the TSP) with fewer funds (\$50 in reserves plus \$100 due from Bank 2) to send its own payment (\$200) to Bank 1 (a non-user of the TSP). Unless Bank 4 replenishes the funding loss (\$50), the shock will propagate further to the payment system.

or more of the available alternatives for sending Fedwire payments. Fedwire offers organizations a range of solutions for sending payments (FRBServices.org, 2021a and 2021b). These solutions vary in their cost and degree of automation. TSPs and banks that send a large volume of payments would use an unattended and secure computer-to-computer interface to Fedwire. This solution is costly because of its security requirements. Users instead bought access to this solution as part of a bundle of services purchased from the TSP. The expense of such a bundle, the lack of interoperability between competing TSPs' services, and the complexity of converting a bank's operations from one TSP to another mean that users would not have multisourced the bundle before the attack or had the option of switching TSPs during the service outage. Instead, users would have switched to semi- or non-automated solutions offered by Fedwire. Those include web-based, attended solutions that generate payment instructions that can be sent to Fedwire, as well as an offline option of calling Fedwire Services with transaction information (usually limited to three transactions per call). These alternatives require users to be pre-authorized for access and informed about the identity verification processes, which include the use of tokens and keywords.

Although Fedwire payments data do not indicate how each payment was sent, conversations with the Federal Reserve's response team for the event revealed that users executed their BCPs and switched to the other ways to send payments. As a result, the data show that users sent significantly fewer payments by number and value over Fedwire during the cyberattack (Figure II), but not zero payments, which would have been the case if users had not found ways to send payments.¹⁷ On the first day of the attack, when the effect was most severe, users sent 81% fewer payments compared with the same day the week before, corresponding to a 72% drop in the value of payments sent. The decrease in the number and value of payments sent by users on the first day is similar quantitatively whether compared with the same day two weeks, one month, and even one year before the cyberattack.¹⁸ The fact that the drop in payments during the attack was not 0% is itself informative, indicating that users had difficulty switching to the alternative ways to send

¹⁷ To protect the confidentiality of the event, the number and value of payments are normalized to one in Figure II.

¹⁸ Appendix Figure II shows no divergence in payments sent by users and non-users one year before the cyberattack.

payments. Section V presents empirical evidence attributing most of the decrease in payments sent each day to the cyberattack. Once users switched to other ways to send payments, they implemented additional BCPs to further mitigate the effect; this, too, is analyzed in Section V.

An alternative way to visualize the disruption and use of BCPs is shown in Figures III and IV, which display payments sent by users and by what fraction of users by half-hour over the first day (left panel), mid-period (middle panel), and last day (last panel) of the cyberattack. For the midperiod, the values for the middle days are averaged, and that average is plotted as a single middle day to mask the length of the event. In each chart, the red line denotes payments sent on the relevant day of the cyberattack, and the neutral lines denote payments sent on the same weekday in earlier and later weeks within a three-month window around the cyberattack (from the first day of the month before to the last day of the month after the attack). The dotted red line denotes 6:30 p.m. The normal deadline for a bank to send a payment request to Fedwire is 6:00 p.m. eastern time, with settlement occurring by 6:30 p.m. A recommended BCP for banks and TSPs dealing with an operational disruption is to ask Fedwire to extend its operating hours into the evening.¹⁹

Compared with payments sent on the same weekday in other weeks, on the first day of the cyberattack (Figure III, top and bottom left charts), users started sending payments later in the day and sent substantially fewer payments by number and value.²⁰ As the day progressed, users sent payments at an improving pace, reflecting that more users had implemented their BCPs and switched to alternative ways to access Fedwire (Figure IV, bottom left chart). The difficulty making that switch is evident: typically, 93% of users would have sent at least one payment by the end of the day, but on the first day of the cyberattack, only 74% did so. Users sent 9.7% of their payments (13% of the value of their payments) after 6:30 p.m., indicating that they requested and made use of extended Fedwire operating hours, but the extra time did not make up for the drop in payments during normal business hours (Figure III, top and bottom left).²¹

¹⁹ The latest a bank or TSP can ask for an extension is 15 minutes before the close of Fedwire. Extensions are typically for 15 minutes at a time, and multiple extensions can be requested. If an extension is granted, Fedwire remains open for all banks, and another extension can be requested before the new closing time.

²⁰ The time stamp on Fedwire payments is the settlement time, which is what the figures show.

²¹ Armantier, Arnold, and McAndrews (2008) analyzes the normal timing distribution of Fedwire payments.

These patterns imply that users sent larger payments in the afternoon and evening of the first day compared with other weeks (Figure IV, top left chart). This is another BCP, consistent with the Federal Reserve's recommendations that banks "prioritize their offline transactions to those that the institution has identified as the most critical transactions, particularly later in the business day" (FRBservices.org, 2021b). This practice keeps more funds flowing through Fedwire, even when a smaller number of payments are sent, mitigating contagious disruptions in reserves (Afonso et al., 2022). It has been used during other operational disruptions as well, such as the September 11, 2001, terrorist attacks in New York (McAndrews and Potter, 2002).

As the cyberattack wore on, users' sending of payments gradually improved (Figures III and IV, middle and right panels). The improvement in the mid-period and on the last day is from more users switching to other ways to send payments, getting better at using the other methods, prioritizing larger payments, having their service restored by the TPS, and, to a lesser extent than on the first day, sending payments in the evening. However, users that did send payments continued to start later in the day (Figure IV, bottom, middle, and right panels).²² A spike in the average payment size occurs at the start of those days (Figure IV, top, middle, and right panels), which likely reflects users prioritizing sending payments left over from the previous day.

Non-users were not directly affected by the cyberattack and continued to send Fedwire payments by their usual means. However, contagion through payment flows reduced the reserves they had available to send payments, at least for the non-users that normally were on the receiving end of payments from users (they will later be defined as *exposed receiver-banks*). That is, exposed receiver-banks saw a drop in incoming payments during the cyberattack and responded by seeking alternative sources of funds to send their payments. The empirical analysis in <u>Section VI</u> confirms the contagion and exposed receivers' responses, which were successful at preventing a disruption in non-users' ability to send payments and thus further contagion. Exposed receivers started sending payments at the usual time, and throughout the first day their payments sent were at the lower end of the distribution of payments sent on the same weekday in other weeks (Figure V).

²² More than 6% of users did not start sending payments again until after the cyberattack was over.

<u>Section VI</u> shows that the difference in their payments sent is just shy of being statistically significant thanks to their sending payments during Fedwire's extended operating hours, perhaps to compensate for delays they incurred in sending payments earlier while borrowing funds.

IV. Data

This article brings together several confidential datasets, described below.

List of Users of the TSP: Key to the analysis is a confidential list of user banks. These data cannot be obtained by other proprietary or commercial datasets. The data allow tracing payments sent by users (the treatment group) relative to non-users (the control group).

Fedwire Funds Service: Fedwire is a real-time gross settlement system, where requests to send payments are processed and settled by the Federal Reserve after they are initiated by a bank. The dataset provides daily, transaction-level data on payment flows between a diverse set of financial institutions. Although banks are identified by their 9-digit ABA (American Bankers Association-assigned) routing number, the analysis is at the depository-institution level using the RSSD number. This is because regulations, including reserve requirements, are at the depository-institution level.²³ Settlement institutions, such as CHIPS, are excluded from the analysis.

Federal Funds: The federal funds market is an over-the-counter market where depository institutions negotiate directly with each other for uncollateralized interbank loans of reserves they hold at the Federal Reserve. The Furfine algorithm (Furfine, 1999) is used to identify fed funds loans, with attention restricted to loans extended by Federal Home Loan Banks (FHLBs). The FHLBs account for almost 100% of all fed funds loans to eligible depository institutions (Appendix Figure III).²⁴ The validity of the fed funds data is cross-checked against two sources: the universe of fed funds transactions as reported in confidential FR 2420 forms, as well as the

²³ A similar aggregation at the depository-institution level can be found in Eisenbach, Kovner, and Lee (2022) and Copeland, Duffie, and Yang (2021).

²⁴ In a thorough analysis of the increased role of FHLBs in funding markets, Gissler and Narajabad (2017) show that FHLBs often account for almost the entire supply of federal funds.

10K filings of FHLBs.²⁵ Thus, the sample does not suffer from the known type I and type II errors of the Furfine algorithm identified by Armantier and Copeland (2015).

Discount Window Borrowing: Eligible depository institutions can post collateral and borrow funds from the Federal Reserve's discount window. These depository institutions can borrow from the discount window if they are illiquid but solvent and have set up the systems and collateral-pledging processes to access the window. The dataset provides information on depository institutions' daily borrowing from the discount window.

Other Datasets: Confidential Federal Reserve accounting records are used for end-of-day reserves that banks hold with the Federal Reserve. Reserve balances from these records are matched with balance sheet data from bank Call Reports.

V. First-round Effect of the Cyberattack

V.A. Disruption of payments sent by users

As described above, the first-round effect of the cyberattack would be through the common shock to user banks' ability to send payments. The empirical analysis thus starts with a differencein-differences model to study that effect.

For the purpose of the analysis, a *sender-bank* is defined as a bank that sends a payment over Fedwire, and a *receiver-bank* is defined as a bank that receives a payment.²⁶ The variables of interest after aggregating Fedwire's transaction-level data are the change in the number and in the total value of Fedwire payments sent by each sender-bank *s* - receiver-bank *r* pair on a specific day *t* compared with the same day a week before to account for seasonality in payment flows (for example, Treasury settlement days, which occur Thursdays, mid-month, and end of month). Appendix Table I presents summary statistics. The empirical model is thus:

²⁵ The Federal Reserve Bank of New York uses FR 2420 data to publish the daily fed funds market volume.

²⁶ For this analysis, the U.S. G-SIBs are excluded from the group of senders. <u>Section V.C.</u> reports the results of several robustness tests, including the case where the G-SIBs are included as senders.

 $\Delta log(Payments)_{srt}$

 $= \beta_1 \times Users_s \times First Day of Cyberattack_t$ $+ \beta_2 \times Users_s \times Mid - Period of Cyberattack_t$ $+ \beta_3 \times Users_s \times Last Day of Cyberattack_t + FE + \varepsilon_{srt},$ (1)

which is run two ways, with *Payments* measured as the number of payments and also as the dollar value of payments.²⁷ Users is a dummy variable that takes value one if a sender-bank was a user and zero otherwise. *First Day of Cyberattack* is a dummy variable that is one on the first day of the cyberattack and zero otherwise. *Mid-Period of Cyberattack* is a dummy variable that is one between the first and last days of the event and zero otherwise. *Last Day of Cyberattack* is a dummy variable that is one on the last day of the event and zero otherwise.²⁸ Each of these day variables is then interacted with the dummy variable *Users* to capture the effect that the cyberattack had on the number and value of payments sent by users on each day during the multiday event as users adapted and the TSP gradually restored their service. A set of fixed effects is added progressively to isolate the effect of the cyberattack on payment flows. Standard errors are conservative and two-way clustered at the sender-bank and day level.²⁹

Table I (columns 1 through 3 and 5 through 7) reports the effect of the cyberattack by day on payments sent by users relative to non-users, including all mitigating efforts; the contribution of mitigants is covered in <u>Section V.B</u>. These columns show the results for all users versus non-users, even though some users may have had service restored and been able to use the TSP on some days

²⁷ The upper 99th percentile of transactions in Fedwire is winsorized to avoid having a few abnormally large payments shape the findings. The article's conclusions do not change if the data are not winsorized.

²⁸ To maintain the confidentiality of the cyberattack's length, the first and last days of the attack are simply referred to as such. For the "mid-period," the dependent variables for each middle day are the log difference in payments (number or value) between a given day during the cyberattack and the same weekday one week earlier. The average is then taken over all the days of the mid-period. That is, the average of the log difference is used, not the difference of the log average; the latter would not properly adjust for the seasonality in payment flows. A similar point has been made in the context of bilateral trade flows in the international trade literature (Baldwin and Taglioni, 2006).

²⁹ The number of clusters (sender-banks) is confidential information. However, there are at least 50 clusters in both clustering dimensions (sender-bank and time), which means that the standard errors are not biased downwards (Bertrand, Duflo, and Mullainathan, 2004). The results are robust when standard errors are triple-clustered at the sender-bank, receiver-bank, and day level.

of the event. Columns 1, 2, and 3 (5, 6, and 7) consider the number (value) of payments sent. Columns 3 and 7 present the preferred specification, with a set of receiver-bank*day fixed effects to compare payments sent by users and non-users to the same receiver-bank on the same day, as well as a set of sender-bank*receiver-bank fixed effects to control for the flow of payments between each pair. Economic conditions and monetary policy can affect the value of payments sent, but users and non-users operated in the same economic and policy environments before and after the cyberattack. Thus, although many factors can drive variation in payments sent, the model identifies the fraction attributable to the cyberattack.

The model estimates a 33% (46%) drop (after de-logging) in the number (value) of payments sent by users, regardless of whether their service was restored, relative to non-users on the first day (Table I, row 1, columns 3 and 7).³⁰ Over the subsequent days (rows 2 and 3), the effect of the cyberattack on payments sent gradually decreased as users gained experience with the alternative means of sending Fedwire payments and the TSP made progress restoring service. On average during the mid-period of the event, the estimated drop in the number (value) of payments sent falls to 13% (20%), less than half the first-day effect. On the last day of the event, the estimate shows little additional improvement, with an 11% (18%) drop in the number (value) of payments sent by users. These estimates are all statistically significant.³¹

V.B. Economic magnitude of the first-round effect and the role of mitigants

Ultimately what matters is the economic magnitude of the first-round effect on payment flows. Because payment flows are highly concentrated among the U.S. G-SIBs, even though the average user is in the top decile of banks by assets, users' share of the total value of payments sent over Fedwire on the same day one week before the first day of the cyberattack, when the disruption was

³⁰ Here and as needed, estimated coefficients on dummy variables are de-logged (Halvorsen and Palmquist, 1980).

³¹ A shortfall in users' liquidity can be ruled out as a cause of the drop in their payments sent. In fact, the opposite should have occurred. With users hindered in their ability to send payments, reserves should have passively accumulated in their accounts at the Federal Reserve because non-user banks, in fulfilling their obligation to process customer payments, continued to send them payments. Reserves of users rose 16% relative to non-users' reserves over the cyberattack (not shown).

most severe, is 0.7%. This means that the 46% drop in the value of payments sent by users relative to non-users (from Table I, column 7) resulted in only 0.32% (0.46*0.7%) of the value of all Fedwire payments being disrupted from the cyberattack. This effect is small, despite the disruption being statistically significant. However, it includes the effect of all mitigants, including users' BCPs and the Federal Reserve support provided. The rest of this section quantifies the effects of these mitigants collectively and individually.

1. *The TSP restores service to users*. Business continuity planning for a TSP concerns ensuring that its own operations are resilient to cyberattacks and that its customers remain able to use its services throughout an attack. The first-round effect of a cyberattack for users would be expected to fall as users' service is restored. To capture the mitigating effect of the TSP's restoring users' service, columns 4 and 8 of Table I replicate the analysis of columns 3 and 7, respectively, but adjust the set of user banks each day to be those for which the TSP had not restored service before the close of business that day. Importantly, no users had service restored before the midperiod's last day. By the close of business that day, 8% were able to send payments through the TSP; they are dropped from the user group for that day before averaging days to get mid-period payments. Another 30% of users were in the process of having service restored at that time. Those users most likely were able to use the TSP by the close of business the next day (which was the last day of the attack), so they and the other 8% are dropped as users for the last day.³² The results from this approach, when compared with columns 3 and 7, provide bounds on the actual effect because the data only suggest the day service was restored to a user, not the time of day.

Because so few users had their service restored by the end of the mid-period, the results should be little changed for those days (columns 4 and 8 relative to 3 and 7, respectively). In contrast, on the last day the drop in payments sent by users should be larger with restored users excluded. Table I confirms that this is the case. The estimates for the first day and mid-period in columns 4 and 8 are essentially unchanged from columns 3 and 7, respectively. On the last day, however, the

³² Users are dropped as user banks once service is restored, but not added to the non-user group at that point.

estimated drop in the number (value) of payments sent by users whose service likely was not restored was 27% (46%), almost the same disruption as on the first day of the cyberattack and about 2.5 times larger than the last-day estimate when all users are included (columns 3 and 7, respectively). That is, by restoring service to some users, the TSP reduced the disruption in Fedwire payments on the last day from 0.33% (0.464*0.7%) to 0.12% (0.176*0.7%). Had the TSP restored service to users earlier, the effect on those days could have been dramatically reduced as well.

2. Users send payments by other means, making other mitigation possible. Users' options for mitigating the effect of the cyberattack had to start with their switching to the other available ways that Fedwire offers to send payments. By switching, they were able to continue to send payments and thus had the opportunity to implement additional BCPs.

Fedwire data do not indicate how banks communicate their payment requests to Fedwire. In lieu of that, the effect of users not switching at all is considered. This is the case where no mitigants of any kind were used. It is equivalent to the case where users were hit directly by the cyberattack or where the attack spread to them from the TSP. With no switching and no mitigants, users would have experienced a 100% drop in payments sent.³³ That would have disrupted 0.7% of all Fedwire payments, more than double the share actually disrupted.

3. Users send payments during extended Fedwire operating hours. Given that users were sending payments, they could—and did—request extensions of the Fedwire business day (Figure III) to gain additional time to send payments, as described in <u>Section III</u>. Whereas Table I reports the effect of the cyberattack considering all payments made, even during the evening, Table II considers only payments that settled before 6:30 p.m., during the normal business day.³⁴ For the preferred specification (columns 4 and 8), there is a 33% (51%) estimated drop in the number (value) of payments sent by users relative to non-users on the first day. Comparing these estimates

³³ Estimates (not shown) for this case show a 100% drop in the value of payments sent by users versus non-users.

³⁴ For the mid-period, payments after 6:30 p.m. are dropped from each day before taking the log differences and subsequently averaging.

with the results in Table I, the extension of Fedwire's operating hours increased the value of payments sent by users by 6 percentage points but did not improve the number of payments sent. This result implies that users sent relatively larger payments in the evening, which is considered in more detail next. On later days of the cyberattack, the extra hours did not improve the value of payments sent, although they reduced the significance of the mid-period drop in payments.

Regardless of which organization requests an extension of Fedwire's hours, Fedwire announces the extended hours (usually for 15 minutes at a time) and makes them available for all senders. Because of this, there are two caveats in interpreting Table II's results. First, an announcement of extended hours in the afternoon may incentivize organizations to take their time and delay sending payments until the evening, knowing that they have extra time. From this perspective, the results in Table II may overstate the effect of the extended hours (Figure V) and Tables I and II estimate changes in users' behavior relative to non-users', the estimates may understate the effect of the extension. The next subsection takes a closer look at when users sent payments during the day, while <u>Section VI</u> examines the cyberattack's effect on non-users.

4. Users prioritized sending larger payments. If users mitigated the cyberattack by prioritizing larger payments, as recommended by the Federal Reserve, the average value sent would have increased. To examine this, the model is run with log(Payments) sent by users as the dependent variable rather than $\Delta log(Payments)$ because there are no extensions of Fedwire's operating hours in the weeks before and after the cyber event. *Payments* is measured as the number, value, and value per payment sent by users. *Afternoon* is a dummy variable that is one for any payment settled between 12:00 p.m. to 6:29 p.m., and zero otherwise. *Evening* is constructed similarly, taking value one for payments settled from 6:30 p.m. to 8:30 p.m. Dummy variables *Pre-cyberattack* and *Post-cyberattack* also are constructed to estimate pre- and post-trends. The former (latter) takes value one in the period before (after) the cyberattack and zero otherwise. *Pre-cyberattack* is constructed to account for changes in the economic and policy environment before the cyberattack that may have affected the number and value of payments sent over Fedwire. The

exact policy changes and their dates cannot be identified to protect the confidentiality of the event. However, any such changes would have affected users and non-users comparably. Day and timeof-day fixed effects are included as well.

Table III presents estimates for all users (columns 1 through 3) compared with only users for whom service was not restored (columns 4 through 6). The latter group would be expected to account for most payments sent in the evening. The results (columns 1, 2, 4, and 5) confirm what Figure III shows: users sent more payments in number and value in the afternoon and evening throughout the event. As before, the results are similar on the first day and in the mid-period, regardless of whether restored users are excluded. On the last day, the increase in the value of payments sent in the afternoon and especially in the evening rises much more for users still sending payments by alternative methods.

Table III (columns 3 and 6) also shows that the value per payment sent by users increased in the afternoon and evening of the first day, as well as in the afternoon in the later days of the cyberattack.³⁵ These findings indicate that users prioritized sending larger payments, and as the cyberattack wore on, without certainty in the afternoon that Fedwire's operating hours would continue to be extended, users sent larger payments in the afternoons but not the evenings.

No trends are evident in the number or value of payments sent or the value per payment sent before or after the cyberattack (rows 7 and 8). This supports attribution of the estimated effects to the cyberattack.

V.C. Robustness tests

A number of tests are conducted to check the robustness of the findings that users sent fewer and smaller payments. Each test is conducted with all users included, even if the TSP has restored their service, which is a higher bar for finding effects of the cyberattack.

The first test runs the empirical model with the U.S. G-SIBs as sender-banks. The G-SIBs send

³⁵ Table III estimates the value per payment sent by users on certain days and times relative to those times on other days, whereas Table I implies the value per payment sent by users on certain days relative to non-users (from subtracting row 1 of column 3 from column 6).

the vast majority of payments, so omitting them as non-user senders could bias the results. Appendix Table II, columns 1 and 5, shows that the estimated drop in the number and value of payments sent during the attack with the G-SIBs as senders is very similar to the estimates from Table I. Hence, the estimates of the first-round effect in Table I are not sensitive to the inclusion of these very large financial institutions.

The second test considers pre- and post-trends in the number and value of payments sent by users and non-users. The results in Table I relied on the assumption that before and after the cyberattack, the number and value of payments sent by the two groups followed similar trends (a parallel trends assumption). However, the cyberattack may have occurred earlier and not previously been discovered. To this end, a *Pre-Cyberattack* dummy variable is constructed that takes value one before the cyberattack and zero otherwise. As before, this variable is constructed to account for changes in the economic and policy environment before the cyberattack that may have affected the number and value of payments sent over Fedwire. These changes would have affected users and non-users comparably. Similarly, a *Post-Cyberattack* and zero otherwise. The results, shown in Appendix Table II, columns 2 and 6, indicate no trends in payments sent by users and non-users before or after the cyberattack.

The next test checks for the role of sender size. Relatively large banks may have better contingency plans and be able to send payments more effectively during a cyberattack, so failing to control for the size channel may lead to biased estimates. Columns 3 and 7 of Appendix Table II show the results without pre- and post-trends, while columns 4 and 8 include those trends. The estimated effect of size is negligible and about the same for the number and value of payments and with and without trends. Sender-bank size does not matter for the results.

VI. Second-round Effect

Because banks rely heavily on incoming payments to provide the funds to send their own

payments (Afonso et al., 2022), a disruption in incoming payments, like the one documented here (the *first-round effect*), can leave banks on the receiving-end with a shortage of liquidity and unable to send their own payments (the *second-round effect*). Unless receiver-banks have sufficient reserves or can tap other funding sources to continue to send their own payments, the cyberattack could propagate to yet other banks and parts of the financial system that were not directly exposed to the cyberattack (the *third-round effect*). This and the next section explore these issues.

VI.A. Incoming payments of exposed receiver-banks

A receiver-bank is either a user or non-user of the TSP. A user receiver-bank would still receive payments into its account at the Fed but could not send payments, as described in <u>Section V</u>. This section therefore considers how, through contagion through the payment system, the cyberattack affected non-user receiver-banks by reducing their incoming payments from user sender-banks.

To this end, this section examines the experience of *exposed receiver-banks*, receiver-banks expected to have exposure to the cyberattack through their typical payment inflows. A new variable, *Exposure*, represents the share of an exposed receiver's total incoming payments from users for a period before the cyberattack.³⁶ For example, if a receiver-bank received payments of \$100 over some weeks before the cyberattack, of which users sent \$20 and non-users sent \$80, the receiver-bank's exposure to the shock would be 20%. Intuitively, a higher exposure indicates that a receiver-bank is more exposed to a drop in incoming payments from users during a cyberattack. Exposed receivers were about 60% of all receiver-banks and had an average exposure of 15%. The U.S. G-SIBs, all non-users, were exposed receivers.

The model regresses the log change of incoming payments of an exposed receiver-bank r on day t compared with the same day a week earlier on this measure of indirect exposure, interacted with the day dummies:

³⁶ The look-back window for calculating exposure is at least several weeks and sufficiently long to perform the analysis without including economic and policy events that might influence payment flows, although the start and endpoint cannot be stated to maintain the confidentiality of the cyberattack.

$$\Delta \log(Payments)_{rt}$$
(2)
= $\sum_{days} (\beta_{day} \times Exposure \ of \ Receiver_r \times Day \ Dummy_t)$
+ $FE + \varepsilon_{rt}.$

The model accounts for all time-invariant observed and unobserved heterogeneity among receiverbanks (receiver-bank fixed effects) and time-varying shocks that are common to all receiver-banks (day fixed effects). Standard errors are two-way clustered at the receiver-bank and day level.³⁷

Table IV presents the results for all exposed receiver-banks and for those with above (below) average assets. For all exposed receivers, a 1% increase in their exposure to the cyberattack is associated with a 0.7% decrease in incoming payments from users on the first day of the attack (column 1). The effect is about half as large and still statistically significant in the mid-period, and small and not significant on the last day. Looking across banks, the decrease in incoming payments is almost twice as big and more significant at small exposed receivers compared with large ones. The improvement in the mid-period for exposed receivers of all sizes is in line with the more successful use of mitigants and restoration of service by the TSP that reduced the first-round effect, allowing less scope for contagion to exposed receivers.

VI.B. Alternative sources of funding

The drop in incoming payments at exposed receiver-banks during the cyberattack is statistically significant for most exposed receivers through the mid-period, but whether it is economically significant depends on whether it materially disrupted liquidity for the receivers. Because exposed receivers would be expected to take steps to address material shortfalls in funding in order to continue sending payments, the next step is to examine if and how these banks addressed the drop in incoming payments. Larger banks may be less likely to need to borrow because of their

³⁷ Standard errors are not biased downward because the number of clusters is above 50 in both dimensions (for receiver-bank and day). This reinforces the previous point that the time-windows used are of sufficient length.

reserve holdings, and, if they borrow, are more likely to access the fed funds market. For example, the 12 systemically important U.S. banks may have enough liquid assets to withstand the wholesale funding runs that might occur in a severe cyberattack (Duffie and Younger, 2019). Smaller banks are more likely to access the discount window (Ashcraft, McAndrews, and Skeie, 2011). Their borrowing may also depend on their reserves held at the Federal Reserve and the Federal Reserve district in which they are located.³⁸ The analysis covers discount window borrowing, then interbank borrowing, and finally reliance on reserves. The findings suggest that the shortfall in liquidity from the decrease in incoming payments from users was material for banks of all sizes.

1. Discount window borrowing. Table V presents estimates of exposed receivers' use of the discount window during the cyberattack. The dependent variable is a dummy that takes value one if an exposed receiver-bank borrowed from the discount window at time t, conditional on no past use at time t-1.³⁹ This dummy variable is regressed on the interaction of the exposure variable with each of the day-of-event dummy variables and fixed effects for receiver-banks and Federal Reserve districts. For all exposed receiver, regardless of size (column 1), there is no evidence of discount window borrowing. However, when exposed receivers are distinguished by size, the large ones (those with above-average assets) are less likely to borrow from the discount window throughout the cyberattack; the reverse is true for small ones. The increased likelihood of borrowing is statistically significant for small exposed receivers that had not previously borrowed in the federal funds market; they may not have had arrangements in place to tap the fed funds market when the

³⁸ Lending through the discount window is administered by regional Federal Reserve Banks, not the Federal Reserve Board. As Ennis and Klee (2021) documents, regional Federal Reserve Banks differ in their willingness to lend, so it is important to control for the district in which a bank is located through the inclusion of district fixed effects.

³⁹ In contrast to the construction of the dependent variables above, the construction of a dummy variable in Table V is trickier with anonymization of the length of the mid-period of the event. As already discussed, all variables are constructed (for example, log differences taken) before that anonymization process. Then, the average of those dependent variables is taken for the mid-period of the cyberattack (the average of the log differences). However, if, for example, the dummy variable takes values of zero, one, and zero during the three days of a hypothetical three-day mid-period, the average will not be zero or one anymore, and the dummy variable ceases to be a dummy. To avoid this problem, the dummy is set equal to one if an exposed receiver-bank accessed the discount window in any one of the days during the mid-period of the cyberattack, and it is zero otherwise.

cyberattack occurred. A 1% increase in the exposure of a small receiver that had not borrowed in the fed funds market or at the discount window the previous day is associated with a 0.03% increase in its probability of obtaining discount window funding on the first day (column 4).

To capture the role of liquidity buffers, the set of small receivers that did not access the fed funds market is split into those with high (above median) and low (at or below median) reserves, with reserves measured as a bank's ex-ante ratio of reserves to total assets (columns 5 and 6). A 1% increase in the exposure of these small receivers with fewer reserves is associated with a 0.04% increase in their probability of obtaining discount window funding on the first day (column 6). This compares with a 0.01% increase for those with higher reserves. However, in the mid-period, the increase in the likelihood of discount window borrowing is of similar magnitude for these small exposed receivers regardless of reserves, perhaps because those with higher reserves relied more heavily on their reserves on the first day and had less capacity to do so in the mid-period.

2. *Interbank borrowing*. Table V (columns 4, 5, and 6) reinforced the importance of the federal funds market. Larger banks generally access that market, and they borrow predominately from the FHLBs. Table VI shows the results from regressing the log of fed funds borrowing on the exposure variable for all large exposed receivers interacted with each day dummy. The coefficients for all large banks (column 1) for the first day and mid-period of the cyberattack are positive but not statistically significant. When this set of large exposed receivers is split further into two groups based on size, the estimates (columns 2 and 3) indicate that smaller (larger) large banks borrowed more (less) from the fed funds market on the first day. They do so in later days as well, although the extent is not statistically significant.

To better understand the reaction of these banks, the sample of larger-than-median large banks is split again into two groups: those with high and low ex ante reserves as a share of their total assets.⁴⁰ On the first day of the cyberattack, relatively larger banks with relatively more (fewer)

⁴⁰ In analyzing interbank borrowing, the sample of large banks is split by size at the median bank so that smaller large

reserves borrowed less (more) from the fed funds market (columns 4 and 5, respectively). These results are as expected.

3. *Liquidity buffers*. Exposed receivers with high reserve-to-asset ratios relative to their peers should be better able to rely on their reserves to send payments in the face of a shortfall of incoming payments from users and have less need to borrow. Tables V and VI show the role of reserves for small and large exposed receivers generally, but many of the larger ones are required to hold additional liquidity buffers, which may better position them to rely on their reserves. To explore this possibility, Table VII presents the findings from regressing the log of reserves for the larger-than-median large banks with relatively high reserves (those analyzed in Table VI, column 4) on the exposure measure interacted with each day dummy and the fixed effects. These banks saw their reserves decrease on the first and subsequent days of the cyberattack, relative to all other days, although only the first day's decline was significant. On the first day, a 1% increase in exposure was associated with a 17.7% decrease in reserves. This result is consistent with the finding of Duffie and Younger (2019) about the largest banks' ability to rely on their reserves in a hypothetical cyberattack, and it supports the importance of liquidity buffers in mitigating the effect of a cyberattack.

VII. Third-round Effect

The results of <u>Section VI</u> indicate that exposed receivers across the size spectrum reacted differently to the drop in incoming payments from users because of the cyberattack. This section examines whether their efforts to borrow funds or tap reserves addressed their liquidity shortfall and avoided a decline in their own payments sent and accompanying spillover effects.

Table VIII shows the results from regressing the change in the log value of payments sent by

banks are ones with assets at or below the median. To estimate the effect of reserves, the sample of relatively larger banks is split at the average reserve-to-asset ratio because using the median left no meaningful variation. Lower reserve banks are those with reserve-to-asset ratios at or below the average.

exposed receivers versus a week earlier on the interaction of the exposure measure with dummies for each day of the event. Receiver-bank * day fixed effects and exposed receiver-bank (as a sender) * receiver-bank fixed effects are included. Two cases are shown: one with and one without the extension of Fedwire's operating hours because any bank is free to send payments during an extension. The estimates, when payments sent during the evening are included (column 1), indicate a drop in payments on the first day that is just shy of being statistically significant (consistent with payments sent being relatively low compared with the same weekday in other weeks, as seen in Figure V). In contrast, looking just at payments sent during the normal business day (column 2), the first-day drop in payments is of similar magnitude but statistically significant. Taken together, these results suggest that exposed receivers may have sent payments during Fedwire's extended operating hours to compensate for delays they incurred in sending payments while borrowing funds. In later days, there is no statistically significant drop in payments sent by these receiverbanks. In fact, in the mid-period, the estimated coefficient is positive, which might suggest some small effect from catch-up payments from the delays on the first day.

These findings are consistent with Afonso et al. (2022), which shows that a 1% increase in the cumulative payments received by a bank in the previous 15 minutes is associated with a 0.4% increase in the value of payments the bank sends during the subsequent minute. For the cyberattack studied here, a 1.412% decrease in exposure is associated with a 1% (1.412%*0.708) increase in incoming payments at exposed receiver-banks (Table IV, row 1, column 1), and a 0.33% (1.412%*0.234) increase in payments sent by these banks (Table VIII, row 1, column 1), very close to the Afonso et al. (2022) result.

Table IX reports the results of regressions that analyze exposed receivers' payments sent by time of day, analogous to the regressions in Table III for user banks. Table IX shows that the number and value of payments increased in the afternoon and evenings relative to the same times on other days, but only the effects in the evenings were statistically significant throughout the cyberattack. The magnitude of the increase in the evenings gradually decreased during the event.

Collectively, the results in Tables VIII and IX show that exposed receivers sufficiently replenished the shortfall in their incoming payments and took advantage of the extra time available

to send Fedwire payments so that they were able to send payments without disrupting incoming payments at yet other exposed receivers or parts of the financial system. Thus, there was no thirdround effect from the cyberattack.

VIII. Conclusion

This article uses confidential data to understand how an actual cyberattack on a TSP propagated through the financial system by disrupting payment flows and, in turn, bank liquidity. The first-round effect of the attack was a common shock to bank users of the TSP's services, while the second-round effect resulted from contagion from users to non-user banks through disruptions in the flow of payments. Non-users' efforts to respond to the resulting shortfall in their reserves averted third-round effects from further contagion. Each round's effect is quantified.

Although the cyberattack had a material impact on individual financial institutions that were directly and indirectly connected to the TSP, it did not affect the overall financial system because banks' and the TSP's use of their BCPs and Federal Reserve support dramatically mitigated the disruption. User banks' BCPs included switching to more manual ways to send Fedwire payments and prioritizing sending larger payments. The TSP's BCPs included restoring user's access to its services as soon as possible. The Federal Reserve granted requests to extend Fedwire's operating hours, and users took advantage of the extra time to make up for delays sending payments during normal business hours. Without all of these mitigants, the disruption to payments sent by users would have been more than twice as large.

Even with the first-round mitigants, non-users of the TSP that normally received payments from users saw a statistically significant reduction in incoming payments from users. This reduction constituted a material liquidity shortfall, driving these banks to borrow at the Federal Reserve's discount window or in the interbank market or to rely on their reserves. These banks also made use of Fedwire's extended hours to send payments. With these actions, the exposed nonusers avoided a significant disruption in sending their own payments, which, in turn, prevented further rounds of contagion and broader financial instability. Three policy lessons stand out. First, business continuity planning matters. Banks switched to alternative processes that the Federal Reserve makes available to access Fedwire. However, they did not switch to them quickly enough to avoid a material drop in their payments sent over the multiple days of the cyberattack. Delays in the TSP restoring service to users prolonged the drop in payments sent, highlighting the importance of the TSP's own continuity plans. Second, liquidity buffers matter. Banks that had sufficient reserves could draw on those reserves to send payments themselves. Third, Federal Reserve support matters. The Federal Reserve extended the time available for processing Fedwire payments and liquidity through discount window loans, both of which mitigated the effect of the cyberattack.

Cyberattacks are the new normal across the economy. While the findings of this article concern the banking sector, they are more broadly relevant and highlight the critical role of business continuity planning in achieving operational resilience in any sector. Additionally, and more specifically to the financial sector, this article shows that actions that the Federal Reserve has used to mitigate harm from traditional operational or liquidity events also can help ensure the financial system's resilience in the face of cyberattacks.

References

- Acemoglu, Daron, Asuman Ozdaglar, and Alireza Tahbaz-Salehi (2015). "Systemic risk and stability in financial networks," *The American Economic Review*, vol. 105, no. 2 (February), pp. 564-608.
- Acemoglu, Daron, Azarakhsh Malekian, and Asu Ozdaglar (2016). "<u>Network security and</u> <u>contagion</u>," *Journal of Economic Theory*, vol. 166 (November), pp. 536-585.
- Afonso, Gara, and Hyun Shin (2011). "Precautionary demand and liquidity in payment systems," Journal of Money, Credit, and Banking, vol. 43, no. 2 (October), pp. 589-618.
- Afonso, Gara, and Ricardo Lagos (2015). "<u>Trade dynamics in the market for federal funds</u>," *Econometrica*, vol. 83, no. 1 (January), pp. 263–313.
- Afonso, Gara, Anna Kovner, and Antoinette Schoar (2011). "<u>Stressed, not frozen: The federal</u> <u>funds market in the financial crisis</u>," *The Journal of Finance*, vol. 66, no. 4 (August), pp. 1109-1139.
- Afonso, Gara, Darrell Duffie, Lorenzo Rigon, and Hyun Song Shin (2022). "<u>How abundant are</u> <u>reserves? Evidence from the wholesale payment system</u>," NBER Working Paper 30736. Cambridge, Mass: National Bureau of Economic Research, December.
- Ahnert, Toni, Michael Brolley, David Cimon, and Ryan Riordan (2022). "<u>Cyber security and</u> <u>ransomware in financial markets</u>," Working Paper 2022-32. Ottawa: Bank of Canada, July 14.
- Aldasoro, Iñaki, Leonardo Gambacorta, Paolo Giudici, and Thomas Leach (2020). "<u>The drivers of</u> <u>cyber risk</u>," BIS Working Paper 865. Basel: Bank for International Settlements, May.
- Allen, Franklin, and Douglas Gale (2000). "Financial contagion," Journal of Political Economy, vol. 108, no. 1 (February), pp. 1-33.
- Almeida, Isis, Mark Burton, and Katherine Doherty (2023). "<u>US plays down ION cyberattack</u>, <u>sees no 'systemic financial risk</u>,' *Bloomberg*, online publication, February 1 (updated 4:51 p.m. est).
- Anand, Kartik, Chanelle Duley, and Prasanna Gai (2022). "Cybersecurity and financial stability," Discussion Paper 08/2022. Frankfurt: Deutsche Bundesbank, March 14.

- Armantier, Oliver, and Adam Copeland (2015). "<u>Challenges in identifying interbank loans</u>," Federal Reserve Bank of New York, *Economic Policy Review*, vol. 21, no, 1 (October), pp. 1-17.
- Armantier, Oliver, Jeffrey Arnold, and James McAndrews (2008). "<u>Changes in the timing</u> <u>distribution of Fedwire funds transfers</u>," Federal Reserve Bank of New York, *Economic Policy Review*, vol. 14, no. 2 (September), pp. 83-112.
- Asensio, Carolina, Antoine Bouveret, and Alexander Harris (2022). "<u>Financial stability risks from</u> <u>cloud outsourcing</u>," ESMA Working Paper 2022-2. Paris: European Securities and Markets Authority, May.
- Ashcraft, Adam, and Darrell Duffie (2007). "Systemic illiquidity in the federal funds market," *AEA Papers and Proceedings*, vol. 97, no. 2 (May), pp. 221-25.
- Ashcraft, Adam, James McAndrews, and David Skeie (2011). "<u>Precautionary reserves and the</u> <u>interbank market</u>," *Journal of Money, Credit, and Banking*, vol. 43, supplement 2 (October), pp. 311-348.
- Baldwin, Richard, and Daria Taglioni (2006). "<u>Gravity for dummies and dummies for gravity</u> <u>equations</u>," NBER Working Paper 12516. Cambridge, Mass: National Bureau of Economic Research, September.
- Bank Governance Leadership Network (2019). "<u>Upgrading legacy banking platforms</u>," EY, online publication, May.
- Barrot, Jean-Noël, and Julien Sauvagnat (2016). "Input specificity and the propagation of idiosyncratic shocks in production networks," *The Quarterly Journal of Economics*, vol. 131, no. 3 (August), pp. 1543-1592.
- Berger, Allen N., Filippo Curti, Atanas Mihov, and John Sedunov (2022). "<u>Operational risk is</u> <u>more systemic than you think: Evidence from U.S. bank holding companies</u>," *Journal of Banking and Finance*, vol. 143 (October), pp. 1-22.
- Bertrand, Marianne, Esther Duflo, and Sendhil Mullainathan (2004). "<u>How much should we trust</u> <u>differences-in-differences estimates?</u>" *The Quarterly Journal of Economics*, vol. 119, no. 1 (February), pp. 249-275.
- Bianchi, Javier, and Saki Bigio (2022). "Banks, liquidity management and monetary policy," *Econometrica*, vol. 90, no. 1 (January), pp.391-454.

- Board of Governors of the Federal Reserve System (BoG) (2021). "Fedwire funds services," webpage, accessed September 1.
- Board of Governors of the Federal Reserve System (BoG), Federal Deposit Insurance Corporation (FDIC), and Office of the Comptroller of the Currency (OCC) (2020). "<u>Sound practices to</u> <u>strengthen operational resilience</u>," online publication, November 2.
- Boehm, Christoph E., Aaron Flaaen, and Nitya Pandalai-Nayar (2019). "<u>Input linkages and the</u> <u>transmission of shocks: Firm-level evidence from the 2011 Tōhuku earthquake</u>," *The Review of Economics and Statistics*, vol. 101, no. 1 (March), pp. 60-75.
- Boer, M., and J. Vasquez (2017). "<u>Cyber security and financial stability: How cyber-attacks could</u> <u>materially impact the global financial system</u>," Institute of International Finance, online publication, September.
- Bouveret, Antoine (2019). "Estimation of losses due to cyber risk for financial institutions," Journal of Operational Risk, vol. 14, no. 2 (June), pp. 1-20.
- Brando, Danny, Antonis Kotidis, Anna Kovner, Michael Lee, and Stacey L. Schreft (2022). "Implications of cyber risk for financial stability." FEDS Notes. Washington: Board of Governors of the Federal Reserve System, May 12.
- Brunnermeier, Markus, and Martin Oehmke (2013). "Bubbles, financial crises, and systemic risk," *Handbook of the Economics of Finance*, vol. 2, part B (January), pp.1221-1288.
- Caballero, Ricardo J., and Alp Simsek (2013). "Fire sales in a model of complexity," *The Journal* of Finance, vol. 68, no. 6 (December), pp. 2549-2587.
- Carvalho, Vasco M., Makoto Nirei, Yukiko U. Saito, and Alireza Tahbaz-Salehi (2021). "Supply chain disruptions: Evidence from the Great East Japan Earthquake," *The Quarterly Journal of Economics*, vol. 136, no. 2 (May), pp. 1255-1321.
- Carvalho, Vasco M., Matt Elliott, and John Spray (2022). "<u>Network bottlenecks and market</u> power," online publication, April.
- Cooper Mountain Mining Corporation (2022). "<u>Copper Mountain Mining subject to ransomware</u> <u>attack and implements risk management systems and protocols</u>." News release, December 29.
- Copeland, Adam, Darrell Duffie, and Yilin Yang (2021). "<u>Reserves were not so ample after all</u>," NBER Working Paper 29090. Cambridge, Mass: National Bureau of Economic Research,

July.

- Council of Economic Advisors (2018). "<u>The cost of malicious cyber activity to the U.S. economy</u>," Executive Office of the President, online publication, February.
- Crosignani, Matteo, Marco Macchiavelli, Andre F. Silva (2023). "<u>Pirates without borders: The</u> propagation of cyberattacks through firms' supply chains," *Journal of Financial Economics*, vol. 147, no. 2 (February), pp. 432-448.
- Denbee, Edward, Christian Julliard, Ye Li, and Kathy Yuan (2021). "<u>Network risk and key players:</u> <u>A structural analysis of interbank liquidity</u>," *Journal of Financial Economics*, vol. 141 (September), pp. 831-859.
- de Vries, C. G. (2005). "<u>The simple economics of bank fragility</u>," *Journal of Banking and Finance*, vol. 29, no. 4 (April), pp. 803-825.
- Duffie, Darrell, and Joshua Younger (2019). "<u>Cyber runs</u>," Hutchins Center on Fiscal & Monetary Policy Working Paper #51. Washington, DC: Brookings Institution, June.
- Duffie, Darrell, Thierry Foucault, Laura Veldkamp, and Xavier Vives (2022). "<u>Technology and</u> <u>finance</u>," Fourth report in the series on *The Future of Banking*. IESE Business School, online publication, May.
- Eisenbach, Thomas, Anna Kovner, and Michael Junho Lee (2022). "<u>Cyber risk and the U.S.</u> <u>financial system: A pre-mortem analysis</u>," *Journal of Financial Economics*, vol. 145, no. 3 (September), pp. 802-826.
- Eisenberg, Larry, and Thomas H. Noe (2001). "Systemic risk in financial systems," *Management Science*, vol. 47, no. 2 (February), pp. 236-249.
- Elliott, Matthew, and Benjamin Golub (2022). "Networks and economic fragility," Annual Review of Economics, vol. 14 (August), pp. 665-696.
- Elliott, Matthew, Benjamin Golub, and Matthew O. Jackson (2014). "Financial networks and contagion," *The American Economic Review*, vol. 104, no. 10 (October), pp. 3115-3153.
- Elliott, Matthew, Benjamin Golub, and Matthew V. Leduc (2022). "Supply network formation and fragility," *The American Economic Review*, vol. 112, no. 8 (August), pp. 2701-2747.
- Ennis, Huberto M., and David A. Price (2015). "Discount window lending: Policy trade-offs and the 1985 BoNY computer failure," Economic Brief 15-05. Richmond, Vir.: Federal

Reserve Bank of Richmond, May.

- Ennis, Huberto M., and Elizabeth Klee (2021). "<u>The Fed's discount window in 'normal' times</u>," Finance and Economics Discussion Series 2021-016. Washington: Board of Governors of the Federal Reserve System, March.
- Erol, Selman, and Rakesh Vohra (2022). "<u>Network formation and systemic risk</u>," *European Economic Review*, vol. 148 (September).
- European Systemic Risk Board (ESRB) (2020). "Systemic cyber risk," online publication, February.
- Farrell, Joseph, and Paul Klemperer (2007). "Coordination and lock-in: Competition with switching costs and network effects." In M. Armstrong and R. Porter (Eds.), Handbook of Industrial Organization, vol. 3, pp. 1967-2072.
- Financial and Banking Information Infrastructure Committee (FBIIC) (2003). "<u>Impact of the</u> <u>Recent Power Blackout and Hurricane Isabel on the Financial Sector</u>," U.S. Department of the Treasury, online publication, October 20.
- Financial Stability Board (2019). "<u>Third-party dependencies in cloud services: Considerations on</u> <u>financial stability implications</u>," FSB online publication, December 9.
- Financial Stability Board (2020). "<u>Regulating and supervisory issues relating to outsourcing and</u> <u>third-party relationships</u>," FSB Discussion Paper, November 9.
- Florackis, Chris, Christodoulos Louca, Roni Michaely, and Michael Weber (2023). "Cybersecurity risk," *The Review of Financial Studies*, vol. 36, no. 1 (January), pp. 351-407.
- FRBServices.org (2021a). "FedLine[®] solutions," webpage, accessed September 1, 2021.
- FRBServices.org (2021b). "Fedwire[®] offline services as a limited contingency tool," webpage, accessed September 1, 2021.
- Gai, Prasanna, and Sujit Kapadia (2010). "<u>Contagion in financial networks</u>," *Proceedings of the Royal Society A*, vol. 466 (March 24), pp. 2401-2423.
- Gai, Prasanna, Andrew Haldane, and Sujit Kapadia (2011). "<u>Complexity, concentration and</u> <u>contagion</u>," *Journal of Monetary Economics*, vol. 58, no. 5 (July), pp. 453-470.
- Ghadge, Abhijeet, Maximilian Wei, Nigel Caldwell, and Richard Wilding (2020). "Managing

cyber risk in supply chains: A review and research agenda," Supply Chain Management: An International Journal, vol. 25, no. 2, pp. 223-240.

- Gissler, Stefan, and Borghan Narajabad (2017). "<u>The increased role of the Federal Home Loan</u> <u>Bank System in funding markets, Part 1: Background</u>," FEDS Notes. Washington: Board of Governors of the Federal Reserve System, October 18.
- Gogolin, Fabian, Ivan Lim, and Francesco Vallascas (2021). "<u>Cyberattacks on small banks and the</u> <u>impact on local banking markets</u>," online publication available at SSRN, April 8.
- Goyal, Sanjeev, and Adrien Vigier (2014). "<u>Attack, defence, and contagion in networks</u>," *Review* of Economic Studies, vol. 81, no. 4 (July), pp. 1518-1542.
- Halvorsen, Robert, and Raymond Palmquist (1980). "<u>The interpretation of dummy variables in</u> <u>semilogarithmic equations</u>," *The American Economic Review*, vol. 70, no. 3 (June), pp. 474-475.
- Healey, Jason, Patricia Mosser, Katheryn Rosen, and Alexander Wortman (2018). "<u>The ties that</u> <u>bind: A framework to assess the linkage between cyber risks and financial stability</u>," Columbia School of International and Public Affairs, Project on Cyber Risk to Financial Stability Working Paper. New York: Columbia University, December.
- Jamilov, Rustam, Helene Rey, and Ahmed Tahoun (2021). "<u>The anatomy of cyber risk</u>," NBER Working Paper 28906. Cambridge, Mass: National Bureau of Economic Research, June.
- Kamiya, Sinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M. Stulz (2021). "<u>Risk management, firm reputation, and the impact of successful cyberattacks on target firms</u>," *Journal of Financial Economics*, vol. 139 no. 3 (March), pp. 719-749.
- Kashyap, Anil K., and Anne Wetherilt (2019). "Some principles for regulating cyber risk," AEA Papers and Proceedings, vol. 109, no. 3 (May), pp. 482-487.

Kellermann, Tom (2022). "Modern bank heists 5.0." VMWare, online publication, April 20.

- King, W. B. (2021). "Interoperability a leading reason Workers Credit Union selects new core provider," Finopotamus, online publication, November 3.
- Klee, Elizabeth (2010). "Operational outages and aggregate uncertainty in the federal funds market," Journal of Banking & Finance, vol. 34, no. 10 (October), pp. 2386–2402.
- Kopp, Emanuel, Lincoln Kaffenberger, and Christopher Wilson (2017). "Cyber risk, market

failures, and financial stability," IMF Working Paper 17/185. Washington, DC: International Monetary Fund, August.

- Lacker, Jeffrey M. (2003). "Payment system disruptions and the Federal Reserve following September 11, 2001," Working Paper 03-16. Richmond, Vir.: Federal Reserve Bank of Richmond, December 23.
- Lagarde, Christine (2018). "Estimating cyber risk for the financial sector," IMF Blog, online publication, June 22.
- Lagunoff, Roger, and Stacey L. Schreft (2001). "<u>A model of financial fragility</u>," *Journal of Economic Theory*, vol. 99, no. 1-2 (July), pp. 220-264.
- Lewis, Tracy R., and Huseyin Yildirim (2005). "<u>Managing switching costs in multiperiod</u> procurements with strategic buyers," *International Economic Review*, vol. 46, no. 4 (November), pp. 1233-1269.
- McAndrews, James, and Samira Rajan (2000). "<u>The timing and funding of Fedwire funds</u> <u>transfers</u>," Federal Reserve Bank of New York, *Economic Policy Review*, vol. 6, no. 2 (July), pp. 17-32.
- McAndrews, James J., and Simon M. Potter (2002). "<u>Liquidity effects of the events of September</u> <u>11, 2001</u>," Federal Reserve Bank of New York, *Economic Policy Review*, vol. 8 no. 2, November), pp. 59-79.
- Office of Financial Research (2017). "<u>Vulnerabilities to cybersecurity incidents</u>." In 2017 *Financial Stability Report*. Washington, DC: Office of Financial Research, December, pp. 7-13.
- Parlour, Christine, Uday Rajan, and Johan Walden (2022). "Payment system externalities," The Journal of Finance, vol. 77, no. 2 (April), pp. 1019-1053.
- Petralia, Kathryn, Thomas Philippon, Tara Rice, and Nicolas Véron (2019). "<u>Banking disrupted?</u> <u>Financial intermediation in an era of transformational technology</u>," 22nd Geneva Report on the World Economy, September.
- Piazzesi, Monika, and Martin Schneider (2021). "Payments, credit and asset prices," online publication, May.
- Pierri, Nicola, and Yannick Timmer (2022). "<u>The importance of technology in banking during a</u> <u>crisis</u>," *Journal of Monetary Economics*, vol. 128 (May), pp. 88-104.

- Powell, Jerome (2019). "Full 60 Minutes interview with Fed Chair Jerome Powell." By Scott Pelley. CBS News 60 Minutes, March 10.
- Powell, Jerome (2021). "Fed Chair Jerome Powell tells 60 Minutes America is going back to work." By Scott Pelley. CBS News 60 Minutes, April 12.
- Ros, Greg (2020). "<u>The making of a cyber crash: A conceptual model for systemic risk in the</u> <u>financial sector</u>," Occasional Paper No. 16. Frankfurt: European Systemic Risk Board, May.
- Schreft, Stacey, and Simpson Zhang (2018). "<u>Network analysis: Defending financial stability by</u> <u>design</u>," OFR Brief 18-02. Washington, DC: Office of Financial Research, August 1.
- Sheffi, Yossi, and James B. Rice Jr. (2005). "<u>A supply chain view of the resilient enterprise</u>," *MIT Sloan Management Review*, vol. 47, no. 1 (Fall), pp. 40-48.
- Shleifer, Andrei, and Robert W. Vishny (1997). "<u>A survey of corporate governance</u>," *The Journal* of Finance, vol. 52, no. 2 (June), pp. 737-783.
- Soramäki, Kimmo, Morten L. Bech, Jeffrey Arnold, Robert J. Glass, and Walter E. Beyeler (2007). "The topology of interbank payment flows," *Physica A: Statistical Mechanics and its Applications*, vol. 379, no. 1 (June), pp. 589-619.
- U.S. Congress House Committee on Financial Services (2015). <u>Protecting critical infrastructure:</u> <u>How the financial sector addresses cyber threats. Hearing before the Subcommittee on</u> <u>Financial Institutions and Consumer Credit of the Committee on Financial Services</u>. 114th Cong., 1st sess., May 19.
- Vives, Xavier (2019). "Digital disruption in banking," Annual Review of Financial Economics, vol. 11 (December), pp. 243-272.
- Warren, Phil, Kim Kaivanto, and Dan Prince (2018). "<u>Could a cyber attack cause a systemic</u> <u>impact in the financial sector?</u>" Quarterly Bulletin, 2018 Q4. London: Bank of England, Fourth Quarter.
- Wellburn, Jonathan William, and Aaron Strong (2019). "Systemic cyber risk and aggregate impacts," Institute for Civil Justice WR-1311. Santa Monica: RAND Institute, September.
- Whitten, Dwayne, Subrata Chakrabarty, and Robin Wakefield (2010). "The strategic choice to continue outsourcing, switch vendors, or backsource: Do switching costs matter?"

Information & Management, vol. 47, no. 3 (April), pp. 167-175.

		∆log(Numb	er of Payments)		$\Delta \log(Value of Payments)$			
	All users, including those with Excluding service restored user		Excluding restored users	All use	se with	Excluding restored users		
	1	2	3	4	5	6	7	8
Users * First Day of Cyberattack	-0.338***	-0.371***	-0.396***	-0.397***	-0.454***	-0.545***	-0.611***	-0.612***
	(0.024)	(0.024)	(0.037)	(0.039)	(0.096)	(0.104)	(0.114)	(0.115)
Users * Mid-Period of Cyberattack	-0.111***	-0.129***	-0.140***	-0.152***	-0.169**	-0.216***	-0.217**	-0.234**
	(0.040)	(0.041)	(0.046)	(0.059)	(0.080)	(0.083)	(0.094)	(0.118)
Users * Last Day of Cyberattack	-0.086**	-0.117***	-0.122***	-0.317***	-0.174***	-0.197***	-0.193**	-0.623***
Sender-Bank FE	(0.039) yes	(0.039) yes	(0.044) no	(0.093) no	(0.003) yes	(0.071) yes	(0.08) no	(0.185) no
Day FE	yes	no	no	no	yes	no	no	no
Receiver-Bank x Day FE	no	yes	yes	yes	no	yes	yes	yes
Sender-Bank x Receiver-Bank FE	no	no	yes	yes	no	no	yes	yes
Observations	550379	550379	550379	549321	550379	550379	550379	549321
R^2	0.024	0.105	0.138	0.139	0.008	0.099	0.157	0.157

Table I: Effect of the Cyberattack on Payments Sent by Users Relative to Non-users

Note: The table presents estimates of the effect of the actual cyberattack relative to other times within a three month window around the attack (the month before, of, and after the cyberattack). $\Delta \log(\text{Number of Payments})$ ($\Delta \log(\text{Value of Payments})$) is the log change in the number (value) of Fedwire payments compared with the previous week. Users is a dummy variable that takes value one if a bank was a user of the TSP that was hit by the cyberattack and zero otherwise. First Day (Last Day) of Cyberattack is a dummy variable that takes value one on the first day (last day) of the cyberattack and zero otherwise. Mid-Period of Cyberattack is a dummy variable that takes value one between the first and the last day of the cyberattack and zero otherwise. Standard errors are two-way clustered at the sender-bank and day level. Statistical significance is denoted as *p<0.1, **p<0.05, ***p<0.01.

		∆log(Numb	er of Payments))	$\Delta \log(Value of Payments)$			
	All user	All users, including those with Exa			All use	All users, including those with		
		service restored	!	restored users		service restored		restored users
	1	2	3	4	5	6	7	8
Users * First Day of Cyberattack	-0.332***	-0.369***	-0.395***	-0.396***	-0.550***	-0.647***	-0.717***	-0.720***
	(0.022)	(0.022)	(0.038)	(0.043)	(0.093)	(0.101)	(0.108)	(0.111)
Users * Mid-Period of Cyberattack	-0.111***	-0.129***	-0.139***	-0.152***	-0.173**	-0.221***	-0.222**	-0.239**
	(0.038)	(0.039)	(0.044)	(0.058)	(0.074)	(0.078)	(0.088)	(0.114)
Users * Last Day of Cyberattack	-0.084**	-0.116***	-0.120***	-0.312***	-0.170***	-0.193***	-0.189**	-0.618***
	(0.038)	(0.038)	(0.043)	(0.094)	(0.060)	(0.067)	(0.076)	(0.177)
Sender-Bank FE	yes	yes	no	no	yes	yes	no	no
Day FE	yes	no	no	no	yes	no	no	no
Receiver-Bank x Day FE	no	yes	yes	yes	no	yes	yes	yes
Sender-Bank x Receiver-Bank FE	no	no	yes	yes	no	no	yes	yes
Observations	550089	550089	550089	549028	550089	550089	550089	549028
R^2	0.024	0.105	0.139	0.139	0.008	0.099	0.157	0.157

Table II: Effect of the Cyberattack on Payments Sent by Users Relative to Non-users, Excluding Extensions of the Fedwire Trading Day

Note: The table presents estimates from a counterfactual cyberattack identical to the actual attack but without any extensions of Fedwire's operationg hours. The analysis is relative to other times within a three month window around the attack (the month before, of, and after the cyberattack). $\Delta \log(\text{Number of Payments})$ ($\Delta \log(\text{Value of Payments})$) is the log change in the number (value) of Fedwire payments compared with the previous week. Users is a dummy variable that takes value one if a bank was a user of the TSP that was hit by the cyberattack and zero otherwise. First Day (Last Day) of Cyberattack is a dummy variable that takes value one on the first day (last day) of the cyberattack and zero otherwise. Mid-Period of Cyberattack is a dummy variable that takes value one between the first and the last day of the cyberattack and zero otherwise. Standard errors are two-way clustered at the sender-bank and day level. Statistical significance is denoted as *p<0.1, **p<0.05, ***p<0.01.

	All user	rs, including the service restored	ose with d	Excli	uding restored	users
	log(Number of Payments)	log(Value of Payments)	log(Value per Payment)	log(Number of Payments)	log(Value of Payments)	log(Value per Payment)
	1	2	3	4	5	6
Afternoon * First Day of Cyberattack	1.488***	2.348***	0.860***	1.479***	2.337***	0.858***
	(0.064)	(0.149)	(0.112)	(0.067)	(0.153)	(0.113)
Evening * First Day of Cyberattack	5.815***	6.459***	0.644***	5.771***	6.447***	0.675***
	(0.088)	(0.187)	(0.111)	(0.116)	(0.193)	(0.095)
Afternoon * Mid-Period of Cyberattack	1.281***	1.611***	0.330***	1.186***	1.469***	0.283**
	(0.064)	(0.149)	(0.112)	(0.067)	cluding restored u r log(Value) of Payments) 5 2.337*** (0.153) 6.447*** (0.193) 1.469*** (0.193) 1.469*** (0.153) 4.494*** (0.153) 4.494*** (0.153) 4.502*** (0.093) -0.003 (0.076) -0.030 (0.086) yes yes 1075 0.771	(0.113)
Evening * Mid-Period of Cyberattack	5.091***	4.481***	-0.610***	5.026***	4.494***	-0.531***
	(0.088)	(0.187)	(0.111)	(0.116)	(0.193)	(0.095)
Afternoon * Last Day of Cyberattack	1.294***	2.016***	0.722***	1.342***	2.123***	0.781***
	(0.064)	(0.149)	(0.112)	(0.067)	(0.153)	(0.113)
Evening * Last Day of Cyberattack	3.694***	3.377***	-0.317***	4.741***	4.502***	-0.239***
	(0.036)	(0.092)	(0.075)	(0.037)	(0.093)	(0.075)
Afternoon * Pre-Cyberattack	-0.012	-0.002	0.011	-0.013	-0.003	0.010
	(0.048)	(0.075)	(0.062)	(0.049)	(0.076)	(0.062)
Afternoon * Post-Cyberattack	0.045	-0.026	-0.072	0.043	-0.030	-0.073
	(0.055)	(0.086)	(0.057)	(0.055)	(0.086)	(0.057)
Day FE	yes	yes	yes	yes	yes	yes
Time of Day FE	yes	yes	yes	yes	yes	yes
Observations	1075	1075	1075	1075	1075	1075
R^2	0.898	0.768	0.249	0.903	0.771	0.246

Table III: Payments Sent by Users of the TSP by Time of Day

Note: The table presents estimates from the actual cyberattack on users' payments sent relative to other times within a three month window around the attack (the month before, of, and after the cyberattack). Log(Number of Payments) (log(Value of Payments)) is the log number (value) of Fedwire payments sent by users of the TSP. Log(Value per Payment) is the log average payment (that is, value of payments divided by the number of payments) sent by users of the TSP. Afternoon (Evening) is a dummy variable that takes value one if payments were settled anytime between 12:00 pm and 6:29 pm (between 6:30 pm) and 8:30 pm) and zero otherwise. First (Last) Day of Cyberattack is a dummy variable that takes value one on the first (last) day of the cyberattack and zero otherwise. Mid-Period of Cyberattack is a dummy variable that takes value one between the first and the last day of the cyberattack and zero otherwise. Pre-Cyberattack) is a dummy variable that takes value one during the period before (after) the cyberattack and zero otherwise. Standard errors are clustered at the day level. Statistical significance is denoted as *p<0.1, **p<0.05, ***p<0.01.

		$\Delta \log(Value of Payments)$	
	All banks	Large banks	Small banks
	1	2	3
Exposure * First Day of Cyberattack	-0.708***	-0.361*	-0.688***
	(0.108)	(0.186)	(0.111)
Exposure * Mid-Period of Cyberattack	-0.416***	-0.345	-0.416***
	(0.085)	(0.244)	(0.087)
Exposure * Last Day of Cyberattack	-0.096	-0.007	-0.104
	(0.104)	(0.229)	(0.106)
Receiver-Bank FE	yes	yes	yes
Day FE	yes	yes	yes
Observations	58505	5673	52832
\mathbf{R}^2	0.018	0.037	0.018

Table IV: Payments Received by Exposed Receiver-Banks

Note: The table presents estimates from the actual cyberattack on exposed receiver-banks' payments sent relative to other times within a three month window around the attack (the month before, of, and after the cyberattack). $\Delta \log(Value of Payments)$ is the log change in the value of Fedwire payments compared with the previous week. Exposure is the weighted average of a receiver bank's incoming payments from sender-banks before the cyberattack. The weights are the share of the receiver bank's total incoming payments sent by sender-banks, with users' payments weighted by one and non-users' payments weighted by zero. Large (Small) is a dummy variable that takes value one for banks above (below or equal) the average bank in terms of size. First (Last) Day of Cyberattack is a dummy variable that takes value one on the first (last) day of the cyberattack and zero otherwise. Mid-Period of Cyberattack is a dummy variable that takes value one between the first and the last day of the cyberattack and zero otherwise. Standard errors are two-way clustered at the receiver-bank and day level. Statistical significance is denoted as *p<0.1, **p<0.05, ***p<0.01.

			$P(DW_t > 0)$	$ DW_{t-1} = 0)$		
	All banks	Large banks		Small	banks	
			Accessed FF	Did not access		
			market	FF market	Did not acce	ess FF market
					High	Low
					reserves/Assets	reserves/Assets
	1	2	3	4	5	6
Exposure * First Day of Cyberattack	0.003	-0.169**	0.005	0.025***	0.013***	0.042***
	(0.004)	(0.067)	(0.003)	(0.005)	(0.005)	(0.005)
Exposure * Mid-Period of Cyberattack	0.002	-0.028	0.008	0.014**	0.015*	0.012*
	(0.005)	(0.079)	(0.005)	(0.007)	(0.008)	(0.006)
Exposure * Last Day of Cyberattack	-0.019***	-0.131***	-0.016***	-0.005	-0.012***	0.006
	(0.003)	(0.041)	(0.003)	(0.003)	(0.004)	(0.005)
Receiver-Bank FE	yes	yes	yes	yes	yes	yes
District x Day FE	yes	yes	yes	yes	yes	yes
Observations	58505	5673	52832	29031	16978	12053
R^2	0.067	0.154	0.067	0.094	0.077	0.141

Table V: Discount Window Borrowing by Exposed Receiver-Banks

Note: The table presents estimates from the actual cyberattack on the probability of exposed receiver-banks' borrowing from the discount window. P(DWt > 0 | DWt-1 = 0) is the probability of discount window borrowing by a receiver-bank at time t conditional on no past use at time *t*-*1*. Exposure is the weighted average of a receiver bank's incoming payments from sender-banks before the cyberattack. The weights are the share of the receiver bank's total incoming payments sent by sender-banks, with users' payments weighted by zero. Large (Small) is a dummy variable that takes value one for banks above (below or equal) the average bank in terms of size. Accessed (did not access) FF market denotes an exposed receiver-bank with positive (zero) fed funds borrowing on the relevant days. High (low) reserves/assets is a dummy variable that takes value one for banks above (below or equal) the median bank in terms of their reserves to assets ratio before the cyberattack. First (Last) Day of Cyberattack is a dummy variable that takes value one on the first (last) day of the cyberattack and zero otherwise. Mid-Period of Cyberattack is a dummy variable that takes value one between the first and the last day of the cyberattack and zero otherwise. Standard errors are two-way clustered at the receiver-bank and day level. Statistical significance is denoted as *p<0.1, **p<0.05, ***p<0.01.

			log(Fed Funds	5)	
		Relatively	-	·	
	All large banks	smaller banks		Relatively larger ban	iks
				High reserves/Assets	Low reserves/Assets
	1	2	3	4	5
Exposure * First Day of Cyberattack	2.578	3.620***	-11.189*	-23.683***	16.473***
$\begin{array}{c cccc} Relatively \\ \hline All \ large \ banks & smaller \ banks & smaller \ banks & Relatively \\ \hline \\ Relatively \\ \hline \\ Relatively \\ \hline \\ H \\ \hline \\ reserve \\ \hline \\ reserve \\ \hline \\ Relatively \\ \hline \\ H \\ \hline \\ reserve \\ \hline \\ reserve \\ \hline \\ Relatively \\ \hline \\ H \\ \hline \\ reserve \\ \hline \\ Relatively \\ \hline \\ H \\ \hline \\ reserve \\ \hline \\ Relatively \\ \hline \\ H \\ \hline \\ reserve \\ \hline \\ Relatively \\ \hline \\ Relativel \\ Relativel \\ R$	(4.415)	(5.153)			
Exposure * Mid-Period of Cyberattack	1.833	3.238*	-2.638	-3.036	3.699
	(2.555)	(1.568)	(4.508)	(5.569)	(2.256)
Exposure * Last Day of Cyberattack	-1.174	2.044	-5.755*	-6.452	-1.808
	(2.377)	(1.214)	(2.836)	(5.290)	(2.254)
Receiver-Bank FE	yes	yes	yes	yes	yes
Day FE	yes	yes	yes	yes	yes
Observations	463	261	201	82	102
R^2	0.876	0.924	0.752	0.775	0.807

Table VI:	Federal Fun	ds Market	t Borrowing	by Lar	ge Exposed	l Receiver-Banks

Note: The table presents estimates from the actual cyberattack of exposed receiver-banks' borrowing in the federal funds market. Log(Fed Funds) is the log of fed funds borrowing. Exposure is the weighted average of a receiver-bank's incoming payments from sender-banks before the cyberattack. The weights are the share of the receiver-bank's total incoming payments sent by sender-banks, with users' payments weighted by one and non-users' payments weighted by zero. All large banks are banks that accessed the fed funds market in the past. Relatively smaller (larger) banks is a dummy variable that takes value one for banks below or equal (above) the median bank within the set of banks that accessed the fed funds market (that is, large banks). High (low) reserves/assets is a dummy variable that takes value one for banks above (below or equal) the average bank in terms of their reserves to assets ratio before the cyberattack. First (Last) Day of Cyberattack is a dummy variable that takes value one on the first (last) day of the cyberattack and zero otherwise. Mid-Period of Cyberattack is a dummy variable that takes value one between the first and the last day of the cyberattack and zero otherwise. Standard errors are two-way clustered at the receiver-bank and day level. Statistical significance is denoted as *p<0.1, **p<0.05, ***p<0.01.

	log(Reserves)	
	1	
Exposure * First Day of Cyberattack	-17.657***	
	(3.626)	
Exposure * Mid-Period of Cyberattack	-7.404	
	(5.435)	
Exposure * Last Day of Cyberattack	-10.109	
	(5.427)	
Receiver-Bank FE	yes	
Day FE	yes	
Observations	82	
R^2	0.875	

Table VII: The Role of Liquidity Buffers

Note: The table presents estimates from the actual cyberattack of changes in log(reserves) of the subset of exposed receiver-banks analyzed in Table 6, column 4. Exposure is the weighted average of a receiver-bank's incoming payments from sender-banks before the cyberattack. The weights are the share of the receiver-bank's total incoming payments sent by sender-banks, with users' payments weighted by one and non-users' payments weighted by zero. First (Last) Day of Cyberattack is a dummy variable that takes value one on the first (last) day of the cyberattack and zero otherwise. Mid-Period of Cyberattack is a dummy variable that takes value one between the first and the last day of the cyberattack and zero otherwise. Standard errors are two-way clustered at the receiverbank and day level. Statistical significance is denoted as *p<0.1, **p<0.05, ***p<0.01.

Ū Ū		27
	$\Delta \log(Value)$	of Payments)
	Including extended	Excluding extended
	Fedwire hours	Fedwire hours
	1	2
Expoure* First Day of Cyberattack	-0.234	-0.246*
	(0.143)	(0.145)
Exposure * Mid-Period of Cyberattack	0.041	0.052
	(0.157)	(0.157)
Exposure * Last Day of Cyberattack	-0.037	-0.040
	(0.136)	(0.136)
Receiver-Bank x Day FE	yes	yes
Exposed Receiver-Bank (as Sender-Bank) x Receiver-Bank FE	yes	yes
Observations	304728	304585
R^2	0.177	0.177

Table VIII: Payments Sent by Exposed Receiver-Banks

Note: The table presents estimates from the actual cyberattack of changes in payments sent by exposed receiver-banks relative to other times within a three month window around the attack (the month before, of, and after the cyberattack), and it compares those to changes in a counterfactual cyberattack without any payments sent during extended Fedwire operating hours. $\Delta \log(Value of Payments)$ is the log change in the value of Fedwire payments compared with the previous week. Exposure is the weighted average of a receiver bank's incoming payments from sender-banks before the attack. The weights are the share of the receiver bank's total incoming payments sent by sender-banks, with users' payments weighted by one and non-users' payments weighted by zero. First (Last) Day of Cyberattack is a dummy variable that takes value one on the first (last) day of the cyberattack and zero otherwise. Mid-Period of Cyberattack is a dummy variable that takes value one between the first and the last day of the cyberattack and zero otherwise. Standard errors are two-way clustered at the exposed receiver-bank (as sender-bank) and day level. Statistical significance is denoted as *p<0.1, **p<0.05, ***p<0.01.

	log(Number of Payments)	log(Value of Payments)	log(Value per Payment)
	1	2	3
Afternoon * First Day of Cyberattack	0.41	0.31	-0.10
	(0.33)	(0.39)	(0.15)
Evening * First Day of Cyberattack	4.35***	5.05***	0.70*
	(0.74)	(1.10)	(0.42)
Afternoon * Mid-Period of Cyberattack	0.33	0.28	-0.05
	(0.27)	(0.35)	(0.11)
Evening * Mid-Period of Cyberattack	3.12***	3.62***	0.50
	(0.73)	(1.06)	(0.39)
Afternoon * Last Day of Cyberattack	0.16	0.25	0.09
	(0.19)	(0.27)	(0.13)
Evening * Last Day of Cyberattack	1.49***	1.81***	0.32
	(0.38)	(0.52)	(0.24)
Day FE	yes	yes	yes
Time of Day FE	yes	yes	yes
Observations	2087	2087	2087
R^2	0.941	0.911	0.590

Table IX: Payments Sent by Exposed Receiver-Banks by Time of Day

Note: The table presents estimates from the actual cyberattack on exposed receiver-banks' payments sent relative to other times within a three month window around the attack (the month before, of, and after the cyberattack). Log(Number of Payments) (log(Value of Payments) is the log of the number (value) of Fedwire payments sent by exposed receiver-banks. Log(Value per Payment) is the log (value of payments/number of payments) sent by exposed receiver-banks. Afternoon (Evening) is a dummy variable that takes value one if payments were settled anytime between 12:00 pm and 6:29 pm (6:30 pm and 8:30 pm) and zero otherwise. First (Last) Day of Cyberattack is a dummy variable that takes value one on the first (last) day of the cyberattack and zero otherwise. Mid-Period of Cyberattack is a dummy variable that takes value one between the first and the last day of the cyberattack and zero otherwise. Standard errors are clustered at the day level. Statistical significance is denoted as *p<0.1, **p<0.05, ***p<0.01.



Figure I: Size Distribution of Users and Non-users of the TSP

Note: The chart plots the size distribution measured by assets of users and nonusers of the TSP.





Note: The chart on the left (right) plots the number (value) of payments by type of bank (users and non-users) before and after the cyberattack. The red vertical dashed lines mark the first and last days of the cyberattack. The mid-period is anonymized by averaging the values for the middle days and plotting that average as the value over a single middle day.



Note: The charts on the left (middle, right) plot the half-hour distribution of the number of payments (top) and value of payments (bottom) by users of the TSP on the first day (mid-period, last day) of the cyberattack (marked as t=0, in red) and the same days in the previous and following weeks (lines in neutral colors). For the mid-period, the values for the middle days are averaged and the average is plotted as the value of a single middle day. The red vertical dashed line marks 6:30 pm, the latest time that Fedwire payments settle when Fedwire closes at its usual time.



Figure IV: Average Value of Payments Sent by Users and Cumulative Share of Users That Had Started Sending Payments by Half Hour

Note: The top charts show the half-hour distribution of the average value of payments by users of the TSP on each day of the cyberattack (in red) and on the same weekdays in the previous and following weeks (lines in neutral colors). The bottom charts show the cumulative share of user banks that had sent at least one Fedwire payment that day as of the end of each half hour. In all charts, the red vertical dashed line marks 6:30 pm, the latest time that Fedwire payments settle when Fedwire closes at its usual time.



Figure V: Payments Sent by Exposed Receiver-Banks by Half Hour

Note: The charts on the left (middle, right) plot the half-hour distribution of the number of payments (top) and value of payments (bottom) by exposed receiverbanks of the TSP on the first day (mid-period, last day) of the cyberattack (marked as t=0, in red) and the same days in the previous and following weeks (lines in neutral colors). For the mid-period, the values for the middle days are averaged and the average is plotted as the value of a single middle day. The red vertical dashed line marks 6:30 pm, the latest time that Fedwire payments settle when Fedwire closes at its usual time. On the first day of the cyberattack, there were no payments before 12:30 am; the charts plot payments starting at that time for all weeks.

Variables	Ν	mean	median	sd
A. Sender-Bank - Receiver-Bank level				
∆log(Number of Payments)	550379	0.008	0	0.642
$\Delta \log(\text{Value of Payments})$	550379	0.012	0	2.182
B. Receiver-Bank level				
Exposure (all banks)	58505	0.149	0.085	0.185
Exposure (large banks)	5673	0.103	0.080	0.095
Exposure (small banks)	52832	0.154	0.085	0.191
Exposure (small banks - did not access FF market)	29031	0.161	0.084	0.205
Exposure (small banks - did not access FF market - High Reserves/Assets)	16978	0.181	0.091	0.220
Exposure (small banks - did not access FF market - Low Reserves/Assets)	12053	0.132	0.072	0.179
Exposure (all large banks that accessed FF market)	463	0.047	0.049	0.034
Exposure (large banks - relatively smaller banks)	261	0.045	0.041	0.034
Exposure (large banks - relatively larger banks)	201	0.050	0.052	0.033
Exposure (large banks - relatively larger banks - High Reserves/Assets)	82	0.036	0.019	0.029
Exposure (large banks - relatively larger banks - Low Reserves/Assets)	102	0.059	0.052	0.030
∆log(Value of Payments)	58505	0.015	0.017	1.433
Access Discount Window	58505	0.008	0.000	0.086
log(Fed Funds)	463	20.172	20.292	1.424
log(Reserves)	82	23.704	23.737	0.891

Appendix Table I: Summary Statistics

Note: The table presents summary statistics of the main variables used in the analysis.

		∆log(Number	r of Payments)		$\Delta \log(\text{Value of Payments})$			
	Include GSIBs			Control for	Include GSIBs			Control for
	as sender-	Controls for	Control for	Size Channel	as sender-	Controls for	Control for	Size Channel
	banks	Trends	Size Channel	and Trends	banks	Trends	Size Channel	and Trends
	1	2	3	4	5	6	7	8
Users * First Day of Cyberattack	-0.381***	-0.407***	-0.399***	-0.409***	-0.574***	-0.618***	-0.611***	-0.619***
	(0.036)	(0.041)	(0.038)	(0.042)	(0.113)	(0.113)	(0.114)	(0.114)
Users * Mid-Period of Cyberattack	-0.147***	-0.150***	-0.141***	-0.152***	-0.225**	-0.225**	-0.219**	-0.226**
	(0.044)	(0.052)	(0.048)	(0.056)	(0.095)	(0.092)	(0.103)	(0.099)
Users * Last Day of Cyberattack	-0.110**	-0.133**	-0.122***	-0.132**	-0.138*	-0.200**	-0.190**	-0.197**
	(0.043)	(0.051)	(0.044)	(0.050)	(0.081)	(0.079)	(0.088)	(0.091)
Size * First Day of Cyberattack			-0.017***	-0.017***			-0.004	-0.004
			(0.003)	(0.003)			(0.006)	(0.006)
Size * Mid-Period of Cyberattack			-0.005*	-0.005*			-0.007	-0.007
			(0.003)	(0.003)			(0.005)	(0.005)
Size * Last Day of Cyberattack			0.002	0.002			0.016***	0.016***
			(0.003)	(0.003)			(0.005)	(0.005)
Users * Pre-Cyberattack		-0.025		-0.025		-0.028		-0.028
		(0.016)		(0.016)		(0.033)		(0.033)
Users * Post-Cyberattack		-0.007		-0.007		0.001		0.001
		(0.013)		(0.013)		(0.024)		(0.024)
Receiver-Bank x Day FE	yes	yes	yes	yes	yes	yes	yes	yes
Receiver-Bank x Sender-Bank FE	yes	yes	yes	yes	yes	yes	yes	yes
Observations	750103	550379	550379	550379	750103	550379	550379	550379
R^2	0.124	0.138	0.139	0.139	0.171	0.157	0.157	0.157

Appendix Table II: Robustness Tes

Note: The table presents estimates from robustness tests for the actual cyberattack relative to other times within a three month window around the attack (the month before, of, and after the cyberattack). $\Delta \log(\text{Number of Payments})$ ($\Delta \log(\text{Value of Payments})$) is the log change in the number (value) of Fedwire payments compared with the previous week. Users is a dummy variable that takes value one if a bank was a user of the TSP that was hit by the cyberattack and zero otherwise. First (Last) Day of Cyberattack is a dummy variable that takes value one on the first (last) day of the cyberattack and zero otherwise. Mid-Period of Cyberattack is a dummy variable that takes value one between the first and the last day of the cyberattack and zero otherwise. In columns 1 and 5, U.S. G-SIBs are included in the list of non-user sender-banks. In columns 2 and 6, the size channel is controlled for by interacting a bank's log of assets with day dummises for the first day, mid-period and last day of the cyberattack. In columns 3 and 7, the validity of the parallel trends assumption is checked by interacting the dummy variable Users with dummy variables for the pre- and post-periods of the cyberattack (the former (latter) takes value one during the period before (after) the cyberattack and zero otherwise. In columns 4 and 8, both the size channel is controlled for and the validity of the parallel trends assumption is checked. Standard errors are two-way clustered at the sender-bank and day level. Statistical significance is denoted as *p<0.1, **p<0.05, ***p<0.01.

Appendix Figure I: Illustration of How a Cyberattack Could Disrupt Payment Flows

	Bank 2 (non-user of TSP)		
Before Cyberattack	Reserves: \$50 Due to Bank 4: \$100		
Bank 1 (non-user of TSP)	Due from Bank 1: \$100	Bank 4 (non-user of TSP)	
Reserves: \$100 Due to Bank 2: \$100		Reserves: \$50 Due to Bank 1: \$200	
Due from Bank 4: \$200 Due to Bank 3: \$100	Bank 3 (user of TSP)	Due from Bank 2: \$100	
▲	Reserves: \$50 Due to Bank 4: \$100	Due from Bank 3: \$100	
	Due from Bank 1: \$100		
		-	

	Bank 2 (non-user of TSP)				
After Cyberattack	Reserves: \$50	Due to Bank 4: \$100			
Bank 1 (non-user of TSP)	Due from Bank 1: \$100		Bank 4 (non-user of TSP)		
Reserves: \$100 Due to Bank 2: \$100			Reserves: \$50	Due to Bank 1: \$200	
Due from Bank 4: \$200 Due to Bank 3: \$100	Bank 3 (user of TSP)		Due from Bank 2: \$100		
↑	Reserves: \$50	Due to Bank 4: \$100	Due from Bank 3: \$100		
	Due from Bank 1: \$100)			

Note: The chart illustrates how a cyberattack could disrupt the payment system and provides a graphical representation of this article's empirical exercise.



Appendix Figure II: Daily Payments Sent by Users and Non-users of the TSP One Year Before the Actual Cyberattack

Note: The chart on the left (right) shows the number (value) of payments sent by type of bank - users and non-users - before and after a hypothetical cyberattack one year before the actual cyberattack. The red vertical dashed lines mark the first and last day of the hypothetical cyberattack. The mid-period is anonymized by averaging the values for the middle days, and that average is plotted as the value over a single middle day.

Appendix Figure III: Comparison of Furfine Algorithm to Regulatory Data on FHLBs' Federal Funds Loans



Note: The chart shows federal funds loans made by FHLBs as identified using the Furfine algorithm compared to federal funds loans from three regulatory datasets for the period 2016q1 - 2020q1.