Hutchins Center Working Paper #51

June 2019

Cyber Runs

Darrell Duffie

Graduate School of Business, Stanford University

National Bureau of Economic Research

Joshua Younger

J.P. Morgan Chase & Co.

ABSTRACT

Our analysis of a sample of twelve systemically important U.S. financial institutions suggests that these firms have sufficient stocks of high quality liquid assets to cover wholesale funding runoffs in a relatively extreme cyber run. Beyond their own stocks of liquid assets, these institutions have access to substantial additional emergency liquidity from Federal Reserve banks. The resiliency of the largest banks to cyber runs does not, however, ensure that the payment system would continue to process payments sufficiently rapidly to avoid damage to the real economy. During a severe cyber event, especially one whose reach into the banking system is uncertain, non-banks may be reluctant to send funds through customary bank payment nodes. As a potential safeguard, we raise the idea of an "emergency payment node," a narrow payment-bank utility that could be activated during operational emergencies to process payments between a key set of non-bank financial firms. We end with an overview of other forms of preparedness, including cyber-run stress tests.

 We are grateful for research assistance by Dan Luo and comments from Benoit Coeuré, Aaron Klein, Don Kohn, Antoine Lallour, Nellie Liang, Serafín Martinez, Jamie McAndrews, Patricia Mosser, John Taylor, and David Wessel.

The authors did not receive financial support from any firm or person for this article or from any firm or person with a financial or political interest in this article. Joshua Younger is currently a managing director for J.P. Morgan Chase & Co..

1. Introduction

Could a cyber attack on a large bank's wholesale depositors morph into a serious and contagious bank run? Our purpose is to briefly analyze the financial-stability implications of such a "cyber run."

We consider scenarios in which a significant cyber attack on a bank's deposits, whether by theft, data corruption, or denial of access, may lead wholesale depositors in the same and other large banks to withdraw their funds rapidly enough to threaten the liquidity of these institutions or the effectiveness of the payment system. After a brief review of potential triggering cyber events, we outline run dynamics and magnitudes.

Our analysis of a sample of twelve systemically important U.S. financial institutions suggests that these firms have sufficient stocks of high quality liquid assets to cover wholesale funding runoffs in a relatively extreme cyber run. Beyond their own stocks of liquid assets, these institutions have access to substantial additional emergency liquidity from Federal Reserve banks. The resiliency of the largest banks to cyber runs does not, however, ensure that the payment system would continue to process payments sufficiently rapidly to avoid damage to the real economy. During a severe cyber event, especially one whose reach into the banking system is uncertain, non-banks may be reluctant to send funds through customary bank payment nodes. As a potential safeguard, we raise the idea of an "emergency payment node," a narrow payment-bank utility that could be activated during operational emergencies to process payments between a key set of non-bank financial firms.

We end with an overview of other forms of preparedness, including cyber-run stress tests.

2. What is a cyber run?

Cyber risks to financial stability have received significant attention from policy makers.[1] These risks are worsened by the increasing diversity of perpetrators—including state and non-state actors, cyber terrorists, and "hacktivists"—who are not necessarily motivated by financial gain. In fact, for some actors, the potential of exploiting a cyber event to inject systemic risk into our highly interconnected global financial system may actually be an enticement (Ablon, 2018).

Beyond general concerns about cyber risks that are common to many firms, discussion papers and official-sector policy documents have noted the threat of cyber attacks on financial market infrastructure

. . .

1. For summaries, see Healey, Mosser, Rosen, and Tache (2018), Howell (2018), and Kashyap and Wetherilt (2018). For official-sector policy summaries, see Bank for International Settlements, Financial Stability Institute (2017), Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation (2016), Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions (2016), Federal Financial Institutions Examination Council (2015), Office of Financial Research (2017), and Rosengren (2015).

and bank deposits.[2] Some reports mention the implications for confidence in financial institutions and the potential for runs.[3] We are not aware, however, of prior work on the nature of a cyber run, including its propagation dynamics, potential scale, and ancillary effects on the payment system.

Cyber attacks on bank deposits have included theft and denials of service.[4,5] A third relevant form of attack is the corruption or theft of deposit account data. Industry initiatives such as Sheltered Harbor mitigate these risks but do not yet provide complete coverage.[6,7] And even if a cyber incident is resolved in a timely manner, there may remain a significant risk that some (if not all) depositors at affected institutions are locked out of their accounts for a meaningful period of time. Sophisticated financial firms place significant value not just on the safety of their deposits, but also on continual access to these deposits, a large proportion of which are needed on short notice to meet high volumes of payment obligations associated with everyday activities. Our focal concern is that, in the face of any of these forms of attack on a bank, large institutional depositors that have not yet been affected by the attack could rapidly and *en masse* take the precaution of redeeming their deposits, or could be unwilling to process additional payments via their deposit accounts. A large bank could suffer a liquidity crisis if a sufficient fraction of its wholesale deposit funding were to suddenly disappear.

The ensuing liquidity crisis could be contagious. Credible reports of a serious cyber attack on Bank A could lead wholesale customers of Bank B to immediately withdraw their deposits at Bank B, in light of the heightened conditional probability that Bank B may also be under attack. Even if Bank B is not under attack, there could be a self-fulfilling expectation that *other* large depositors in Bank B will make precautionary withdrawals, thus generating the threat of a liquidity crisis for Bank B that is itself a rationale for any large depositor to run. This kind of herding behavior has been observed during credit

. . .

2. See CPMI-IOSCO (2016), Office of Financial Research (2017), and Bouveret (2018). Rosengren (2015) writes that "A more serious case would be an attack on payment systems aimed at disrupting transactions, for example by a rogue state or entity. Prevention is difficult because the attacker does not need to `enter' the system to be disruptive, and there is no need to exit with confidential data – all the attacker needs to do is flood the public-facing `front door' of a payments processor with enough traffic to make the system unavailable."

3. Healey, Mosser, Rosen, and Tache (2018) state that, "Whatever the trigger, a sufficiently extreme loss of confidence could cause a 'run on the banks.'" Boveret describes how "Cyber-attacks can also be used to undermine customers' confidence in an institution. For example, on June 27, 2014, Bulgaria's largest domestic bank FIB experienced a depositor run, amid heightened uncertainty due to the resolution of another bank— following phishing emails indicating that FIB was experiencing a liquidity shortage."

4. The largest reported cyber theft of deposits was the 2016 theft of $81 million from the account of the Bangladesh central bank at the Federal Reserve Bank of New York, as reported by Rubenfeld (2019).

5. The U.S. Department of Justice (2016) described attacks by Iran on large U.S. banks. "The defendants and/or their unindicted co-conspirators then sent orders to their botnets to direct significant amounts of malicious traffic at computer servers used to operate the websites for victim financial institutions, which overwhelmed victim servers and disabled them from customers seeking to legitimately access the websites or their online bank accounts."

6. Sheltered Harbor is a non-profit initiative of the Financial Services Information Sharing and Analysis Center (FS-ISAC; see discussion in the Appendix for more details) which acts as a centralized data repository to protect the resilience of the financial system in the event of a catastrophic cyber event.

7. Sheltered Harbor currently covers approximately 70 percent of deposit accounts. For more details, see https://shelteredharbor.org/.

events—most recently the run on prime money market mutual funds after the Lehman bankruptcy, including prime funds with limited or no direct exposure—and would likely be triggered by cyber incidents as well.

A deposit-based liquidity crisis could deepen if other normal sources of funding to a large bank were to react cautiously by declining to provide or renew funding. For example, some large U.S. banks have securities dealer affiliates that rely on over a hundred billion dollars (each) of overnight financing in the repo market, in order to maintain their securities inventories. A liquidity crisis among the largest banks can also be amplified by the normal reliance of these banks on each other as liquidity shock absorbers.[8]

As explained by Afonso, Curti, and Mihov (2019), banks have substantial regulatory capital requirements associated with operational risks, including cyber attacks. However, regulations seeking to manage liquidity risk among large banks were designed primarily to address conventional run scenarios. A cyber incident, on the other hand, may trigger fears of an immediate loss of access to deposits. Thus, the resulting outflows could be faster moving and larger in magnitude than anticipated by the design of current liquidity regulations. A key question, which we address in the next section, is whether large U.S. banks currently hold enough high quality liquid unencumbered assets to weather such a run.

Even were banks to avoid an outright liquidity crisis, cyber runs could introduce significant frictions into the payment system. For example, activity on the Automated Clearing House—which makes up more than half of all non-cash payment activity—is highly concentrated among a few member institutions. Were one of these nodes to be taken down, even for a short period of time, the economic impact could be significant, as we will discuss in more detail. Though safeguarding the payment system has long been a focus of cyber policy, the potential for a cyber run to turn an operational event into a liquidity event makes outages in affected payment nodes more difficult to remedy.

Cyber run risk is compounded by the propensity of affected depositors to seek non-bank liquidity outlets such as government money market funds (MMFs), which are outside the payment system and are also unlikely to achieve high enough turnover to serve normal (let alone crisis) demands for transactions activity, especially on short notice. Money funds are also exposed to intraday liquidity events, given their lack of direct access for liquidity to the Federal Reserve System. A sudden reduction in the maximum attainable velocity of circulation of cash could have serious macroeconomic repercussions.

3. Quantifying the run risk

The first step in addressing cyber run risk is to identify and quantify the sources of bank funding that are potentially exposed to such a run. Though standard disclosures typically lack sufficient granularity for this exercise, Liquidity Coverage Ratio (LCR) regulations require larger financial institutions to identify,

. . .

8. Kopp, Kaffenberger, and Wilson (2017) write that "Close direct connections through interbank and transfer markets, and indirect relationships (liquidity cascades) allow shocks to spread quickly throughout the system. An institution's inability to meet payment or settlement obligations—for example because their internal record-keeping or payments systems have been compromised—can cause a name crisis, which would have adverse effects on funding liquidity and knock-on effects to other institutions which were counting on the availability of these liquidity flows."

model, and disclose details around how they fund themselves.[9] Relying in part on these disclosures, we consider a sample of 12 major bank holding companies (with at least $250bn in total assets), including major "money-center" banks, larger regional banks, institutions that are dominated by their securities custody services, and institutions whose most significant business is their broker-dealer.

The principle underlying the LCR is that all of a mandated bank's potential cash outflows within 30 days must be covered by conservatively estimated cash inflows and the bank's stockpile of unencumbered high quality liquid assets (HQLA). For the purposes of applying the rule, each of a bank's sources of funds is assigned an assumed adverse-scenario run-off rate. These assigned run-off rates are conservative with respect to empirical evidence on traditional bank runs, as explained by Martin, Puri, and Ufier (2018). For large banks, wholesale deposits tend to dominate the regulatory measure of total weighted net cash outflows because of their more aggressive run-off assumptions, although this effect varies across institutions. Within unsecured wholesale funding sources, the current LCR rule applies 25 percent and 40 percent runoff rates to operational deposits and non-operational deposits, respectively. A run-off rate of only 3 percent applies to stable retail deposits.

The LCR rule makes some allowance for cash inflows within the 30-day test window. Secured funding is assumed to be more easily accessible in a crisis, with an average inflow rate of roughly 25 percent across our sample of institutions, compared to a 10 percent inflow rate assumption for unsecured funding.

As of the third quarter of 2018, the twelve banks in our sample exceeded their LCR requirements, having enough weighted HQLA to cover their respective measures of stressed outflows, net of assumed inflows, with a comfortable management buffer. The banking system, both as a whole and among larger institutions, is apparently resilient to traditional run scenarios.

Cyber runs, however, could generate exceptionally high short-term run-off rates. Although the 2008 financial crisis does not provide an apples-to-apples comparison, the crisis experience suggests that wholesale funding runs could be more rapid than assumed by the LCR rule at times of extreme stress. For example, in the immediate aftermath of the Lehman Brothers bankruptcy in late 2008, raw institutional prime money market fund (MMF) outflows peaked at more than 10 percent *per day* (Kacpercyzk and Schnabl, 2010; Schmidt, Timmermann, and Wermers, 2016). Cyber runs could be even more rapid because operational events typically have shorter time scales than credit events.

Research by Martin, Puri, and Ufier (2018) suggests that traditional runs are mitigated by the long-standing institutional relationships between depositors and their banks. In a cyber run, however, relationships might impinge much less on the rationale for quick withdrawals. In such a scenario, a bank client who runs to safeguard "physical" access to its funds would not be showing disrespect for its bank's creditworthiness. Altogether, we suspect much larger and more front-loaded outflow rates in a serious cyber scenario than envisioned in the design of the current LCR rule.[10]

As we have discussed, a cyber event could envelope more than the directly affected institutions. During the massive 2008 flight of wholesale cash investors from prime money funds that was triggered by

. . .

9. For a detailed overview, see U.S. Basel III Liquidity Coverage Ratio Final Rule: Visual Memorandum, Davis Polk & Wardwell, 9/23/2014.

10. As a point of comparison, we direct the reader to Bush, Kirk, Martin, Weed, and Zobel (2019), who assume somewhat less front-loaded funding runoff associated with the more traditional scenario envisioned by LCR.

losses of the Reserve Primary Fund on its Lehman paper, the majority of the outfl.ows were from prime funds with no significant exposure to Lehman Brothers.

In principle, a bank's operational deposits are those most exposed to cyber runs because they are specifically associated with the high-frequency transactions needed for daily activities. The LCR rule identifies operational deposits as those associated with daily activities such as payment processing, payroll, settlement of financial transactions, and so on.

LCR disclosures for our sample of institutions imply that operational deposits account for nearly $1.8 trillion in aggregate, or 60 percent of wholesale unsecured funding. Three quarters of this total is held by the four largest names. In practice, however, the distinction between operational and non-operational deposits is not straightforward. Not only are these funds generally comingled, but the functional split between the two can vary significantly over long and short timescales. For the purposes of our quantitative exercise, we propose to view all institutional deposits—totaling more than $2.8 trillion in our sample as of the third quarter of 2018—as at risk in a cyber run.

As mentioned, the LCR rule allows for funding inflows to partially offset run-offs. Because cyber runs deal specifically with operational risks, it seems likely that affected institutions would have more difficulty accessing secured funding than in a traditional run. Both retail and wholesale customers would also be less keen to deposit funds because of fears of lack of access. The fear of loss of access, above and beyond aversion to credit exposure, would likely worsen net outflows and net inflows relative to LCR assumptions.

The LCR rule splits HQLA into various levels according to the speed with which the assets can be liquidated at low cost. Reserves held at the Fed are "Level-I," and are the most effective form of HQLA for addressing intraday liquidity needs at large scale. There is in fact evidence that the overall supply of bank reserves is driven in part by their utility in pre-funding stressed day-one outflows (Bush, Kirk, Martin, Weed, and Zobel , 2019). Next-day needs can be met with the remaining forms of Level-I HQLA, primarily Treasuries and T-Bills, which have daily trade volumes of several hundred billion dollars.[11] Lower-level HQLA would contribute significant liquidity over roughly weekly time frames. Based again on data from the third quarter of 2018, we find that, in aggregate across our sample, reserves cover roughly 25 percent of wholesale unsecured funding. Other Level-I HQLA totals to about 37 percent of wholesale funding, split roughly 2-to-1 on average between treasuries and GNMA mortgage-backed securities [MBS].[12] The remainder of HQLA (largely composed of conventional MBS) covers another 15 percent of wholesale funding, for 78 percent coverage in total. However, as illustrated in Figure 1, there is significant variation in coverage across institutions. The coverage of money center and regional banks is around 80 percent (of which 25 percent consists of reserves, though this can be as high as about 40 percent for some banks), while the coverage of custody banks is closer to 50 percent (of which 17 percent is reserves). All else equal, this leaves custody banks more exposed to liquidity risk in the event of a cyber run.

Beyond comparing the stock of HQLA to potential wholesale deposit flight, it is important to consider the timing of outflows relative to a canonical bank's ability to raise liquidity. For this purpose, Figure 2

. . .

11. See Primary Dealer Statistics provided by the Federal Reserve Bank of New York at: https://www.newyorkfed.org/markets/gsds/search.html

12. See Ihrig, Kim, Kumbhat, Vojtech, and Weinbach (2017).

shows the resiliency of the "average" money-center bank in our sample to three hypothetical runoff scenarios, the specifications of which are detailed in Appendix A:

a. A scenario consistent with the design of the LCR rule, based on stressed and weighted gross outflows, leading to a cumulative total runoff rate of approximately 24 percent over a 30-day window.
b. An adverse cyber run, with an assumed cumulative total runoff of 50 percent of wholesale deposits over 30 days.
c. A severe cyber run, with an assumed total runoff of 75 percent.

For each of the three scenarios, the daily profile of runoff rates across the 30-day window, detailed in the appendix, is assumed to be front-loaded. Any such assumptions are highly conjectural, as the urgency to run is difficult to model and likely to be subject to multiple self-fulfilling equilibria (Diamond and Dybvig, 1983). In this sense our scenarios should be taken as purely illustrative but intended to represent relatively conservative situations.

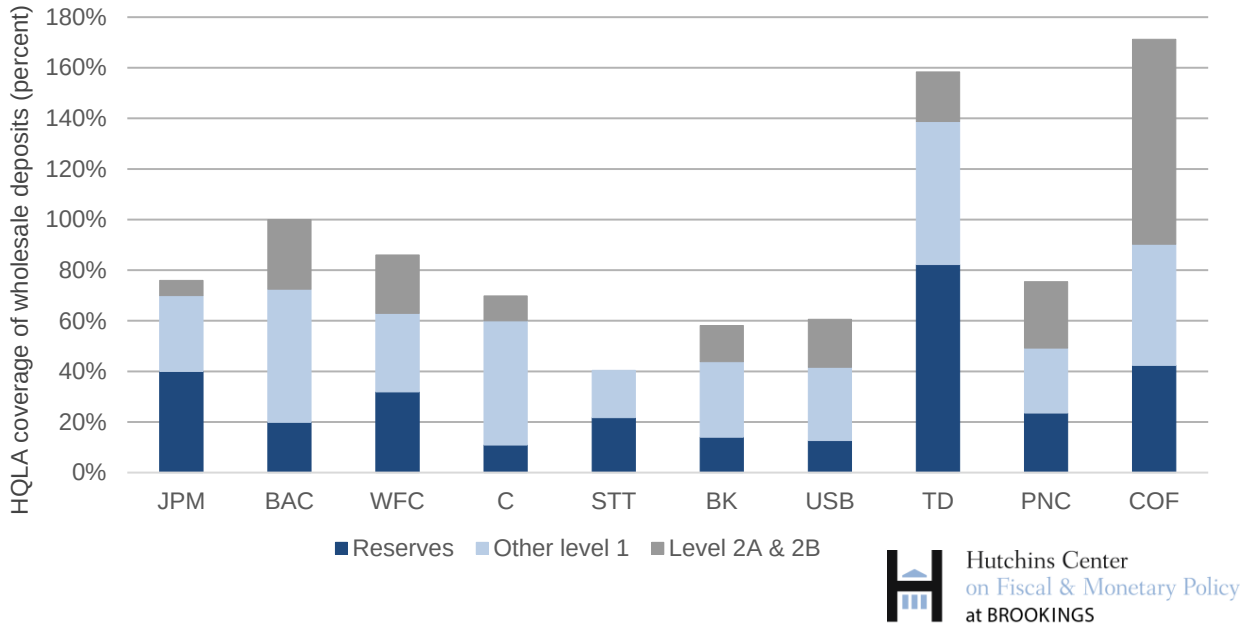

Figure 1. HQLA coverage of wholesale deposits for selected banks.

For each bank, the height of the colored segments represent the levels, as of the end of the third quarter of 2018, of various types of high quality liquid assets (HQLA) as a fraction of total wholesale deposits (operational and non-operational) of selected banks: JP Morgan (JPM), Bank of America (BAC), Wells Fargo (WFC), Citibank (C), State Street (STT), Bank of New York Mellon (BK), U.S. Bank (USB), Toronto Dominion (TD), PNC Bank (PNC), and Capital One (COF). For COF we include all eligible HQLA, though it is important to note that this may differ from the reported LCR measurement due to level 2 asset caps in the rule.

The ability to raise cash within a given time window is limited by the composition of the HQLA portfolio. For our illustrative purposes, we assume the "average" HQLA composition of money-center banks across reserves, Treasuries, and MBS, exploiting the empirical analysis of Ihrig, Kim, Kumbhat,

Vojtech, and Weinbach (2017). We assume that the ability of our hypothetical bank to liquidate Treasuries and MBS within a given time frame is limited by historical turnover in these respective markets, for which we rely on trading volume data.[13] We conservatively assume T+1 settlement for Treasuries and MBS, though in principle both of these types of assets could be used as collateral to source same-day cash via secured funding sources such as repurchase agreements (repos).[14] For simplicity, we assume no price impact for sale of these two asset classes. Sales can be avoided by reliance instead on repos.

Our results, although based on crude and preliminary assumptions, suggest that our hypothetical representative money-center bank has ample liquidity to survive scenarios anticipated by the LCR rule and even adverse cyber runs. Our hypothetical bank experiences moderate liquidity shortfalls under our assumptions for a severe cyber run, but, as we have emphasized, the bank could accelerate its access to cash by using its Treasuries and MBS as collateral for more immediate access to cash via repurchase agreements. Moreover, the Fed is available as a robust additional source of liquidity and would presumably not hesitate to offer ample additional reserves against good collateral during an extreme cyber event, just as the Fed did during the operational outages at BONY in 1985 (Ennis and Price, 2015) and at 9/11/2001 (Lacker, 2003).[15]

In summary, all of our analysis, although quite basic, suggests that banks have sufficient liquidity—both stock and flow—to survive even a relatively extreme cyber run.

As a caveat, a systemic bank's liquidity situation could worsen sharply during scenarios in which secured funding turns skittish. Though seemingly extreme on the surface, we do not believe that such a scenario is entirely implausible in the wake of a cyber incident involving a major bank. It should be noted that while repo markets were in many ways the epicenter of the 2008 financial crisis, their composition has changed dramatically in favor of higher quality collateral. For example, using money market funds (MMFs) as a proxy, Federal Reserve data suggest that Treasuries and Agencies (mostly MBS; Baklanova, Copeland, and McGaughrin, 2015) make up more than 95 percent of collateral, up from 75 percent in 2010 (the earliest date covered in their analysis).[16] However, even secured lenders rely on ready access to cash for daily liquidity, particularly banks subject to minimum operating liquidity and other operational requirements. Given the risk that their cash may be frozen by a cyber event in progress, there could be strong incentives among cash investors to avoid any affected institutions regardless of collateral quality. This is not our base case for even a severe cyber run, but is a plausible risk in an extreme event.

. . .

13. For treasuries, we rely on Primary Dealer Statistics provided by the Federal Reserve Bank of New York. For MBS, we use TRACE data on pass-throughs, as summarized by SIFMA's U.S. Structured Finance Trading Volume data at https://www.sifma.org/resources/research/us-sf-trading-volume/

14. In principle, MBS can be settled same-day for cash, however it is unclear what volume of such transactions the market can accommodate.

15. Ennis and Price (2015) describe how, in 1985, The Fed provided The Bank of New York (BONY) with $23 billion in discount-window funding when a software failure left BONY unable to meet its agreements to deliver large quantities of securities.

16. These Federal Reserve data are at https://www.federalreserve.gov/releases/efa/efa-project-money-market-funds-investment-holdings-detail.htm

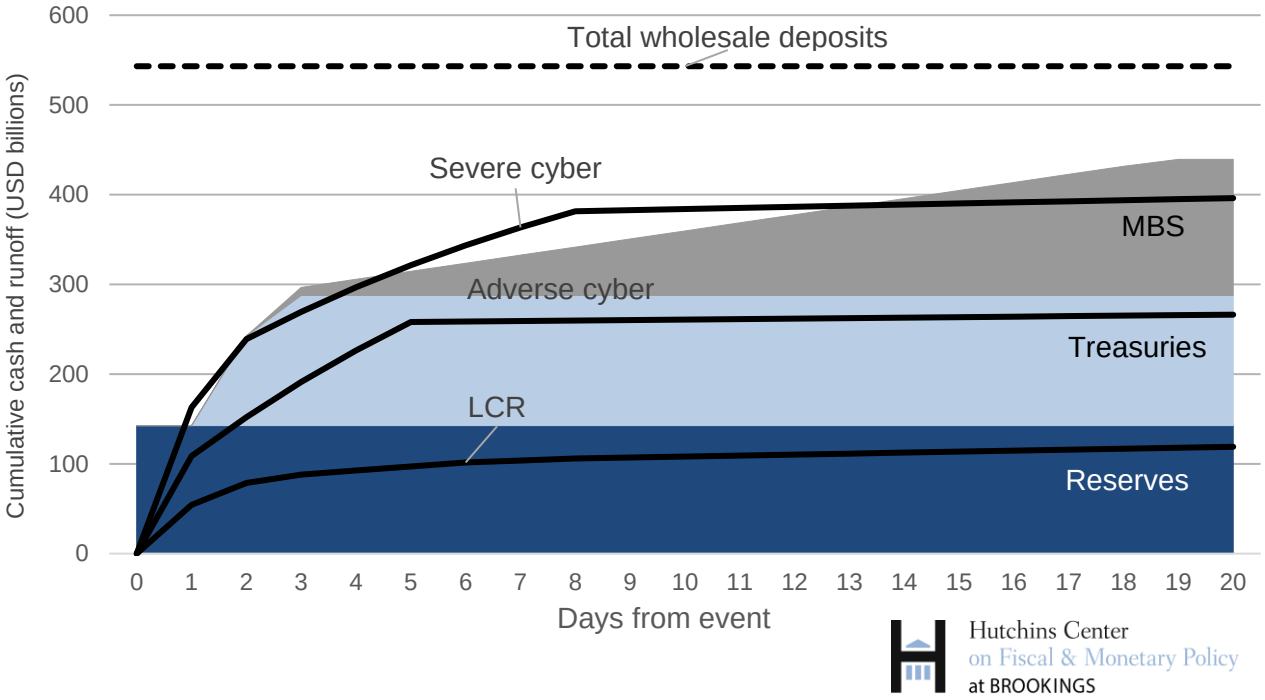

Figure 2. Resiliency of an "average" money-center bank to hypothetical cyber runs.

The height of the stack of colored segments shows the cumulative cash available at a given number of days from an event, stemming from three sources of high quality liquid assets (reserves, treasuries, and mortgage backed securities) based on liquidation timing assumptions stated in Appendix A. The lines plotted in black show the cumulative runoffs of wholesale deposits (both operational and non-operational), based on runoff rate assumptions stated in Appendix A. Cumulative runoffs are shown for hypothetical scenarios associated with the design of the Liquidity Coverage Ratio (LCR) rule, an adverse cyber run, and a severe cyber run.

Section 23 of the Federal Reserve Act strongly limits the ability of the largest U.S. securities dealers to obtain emergency liquidity from the bank subsidiaries within the same bank holding companies.[17] Worsening the situation, the Dodd-Frank Act prevents the Fed from providing emergency funding to individual securities dealers under its emergency lending authority, Section 13-3 of the Federal Reserve Act. In an industry-wide crisis, however, the Fed retains its legal authority to set up programmatic liquidity facilities for multiple securities dealers, just as it did in 2008 around the failures of Bear Stearns and Lehman.

. . .

17. Petrasic (2010) outlines how the Dodd Frank Act significantly reduces the ability of the Fed to obtain exemptions to restrictions on affiliate funding under Section 23 of the Federal Reserve Act, "Relations with Affiliates," which can be found at https://www.federalreserve.gov/aboutthefed/section23a.htm

4. Payment-system network effects

Having discussed the resiliency of individual institutions to cyber runs, we turn to the network impacts of a cyber run on the payment system, and spillover effects on the real economy. The Federal Reserve Payments Study reveals that the Automated Clearing House (ACH) is the single largest source of non-cash payments in the United States—recently handling more than half of gross transfers.[18,19] A potential side effect of a cyber run is that deposit accounts at a large financial institution become inaccessible. This would effectively lock the institution out of ACH and other payment systems that interact directly with the real economy. ACH payment activity is highly concentrated on a few nodes. As an illustration, 2017 network statistics suggest that the five most active originators generated more than 60 percent of total ACH payment activity.[20] It stands to reason that other key payment systems—such as CHIPS, Fedwire Funds and Securities, DTCC and derivatives clearing—are similarly concentrated. Were just one of these critical payment nodes to be rendered inoperative or otherwise inaccessible, the interruption or slowdown of consumer and business-related payments could have materially adverse economic implications.

Though cyber risks to the payment system have been recognized for some time (Borghard 2018; Bouveret 2018; CPMI-IOSCO 2016; Kopp, Kaffenberger, and Wilson 2017; Office of Financial Research 2017; Rosengren 2015) there has been little discussion of the potential for cyber runs to exacerbate the impacts. An outflow of deposits would likely rapidly deplete the reserve balances of affected institutions. Banks rely on these reserves for the intraday settlement liquidity that facilitates the smooth functioning of the payment system (Bech, Martin, and McAndrews, 2012; Belton, 2018; McAndrews & Kroeger 2016).[21] One could in principle turn to overdrafts on Federal Reserve accounts as a substitute—as was commonly the case in the pre-crisis era. However, in the extreme, continued outflows could make these overdrafts much more difficult to cure by the end of a day, forcing affected banks to downscale their FedWire, ACH, and other payment activity. The Fed's discount window is available, but tends to be a last resort because of the associated cost, stigma, and collateral requirements. As a result, cyber runs can exacerbate and prolong disruptions in the payment system in the wake of a cyber incident, potentially long after the proximate cause has been cured.

A severe cyber incident in the banking system could therefore not only induce, but also prolong, a payment-system gridlock. With one or more nodes in the system essentially inaccessible because of a cyber event, and amid heightened fears of placing funds at certain other payment nodes, there could be a significant slowdown in the circulation of reserves. This increases the incentives of an institution to hoard

. . .

18. The 2017 Annual Supplement shows roughly 55 percent of non-cash payment activity was processed via the ACH network, relative to ~10 percent in checks (excluding interbank payments) and just under 8 percent on credit, debit, and prepaid cards. For details, see Federal Reserve Board (2017) available at this link: https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm

19. See Federal Reserve Board (2017).

20. The 2017 and historical network statistics, including the top 50 originators and receivers, are available on the ACH website at https://www.nacha.org/ach-network/timeline

21. The appropriate steady-state balance of reserves to facilitate interbank payments is an ongoing area of active research and discussion, while the Federal Reserve has been reducing the size of its balance sheet as part of its policy normalization process.

liquidity, even if unaffected itself by the cyber event and even if unconcerned about counterparty credit risk.

Indeed, Ashcraft, McAndrews, and Skeie (2009) find evidence that a bank with significant intra-day inflows and outflows, whenever concerned that it may not receive inflows sufficiently in advance of outflows, has a tendency to delay its own payments. In severe cases, hoarding liquidity would become a self-fulfilling equilibrium behavior. When describing the impact of operational outages during the events of September 11, 2001, Lacker (2003) wrote "The general disruption in payment flows would also have meant uncertainty for many banks about whether scheduled incoming payments would be received as planned. This may have induced banks to delay or withhold payments." McAndrews and Potter (2002) provide supporting evidence of hoarding behavior on 9/11, writing that "While some banks that experienced technological difficulties in sending payments accumulated higher-than-desired balances, other banks' increased uncertainty (regarding which payments they might receive later in the day) led them to have higher precautionary demand for liquid balances. Consequently, the sources of liquidity internal to the banking system were not available or capable of addressing the widespread demand for liquidity."

5. Non-bank liquidity outlets

If wholesale depositors and secured cash investors run from payment-system nodes, they would substitute with other forms of cash instruments. As in late 2008, government MMFs could prove to be an attractive non-bank liquidity outlet in a cyber run. These funds are backed almost entirely by high-quality (sovereign or government-agency) short-maturity assets. In principle, MMFs offer same-day liquidity for large shareholders. The government MMF complex is large, holding more than $2.3 trillion in total assets as of this writing, roughly $1.6 trillion of which constitutes institutional funds.[22,23] These MMFs have access to sufficient investable assets, meeting 2a-7 regulatory requirements, to absorb even the most extreme inflows related to a cyber run. For example, after excluding current government MMF holdings as well as those of the Federal Reserve and foreign official-sector investors, the stock of T-Bills, agency discount notes, eligible Treasuries, agencies and floating rate notes (FRNs) exceeds $4.5 trillion, which is

. . .

22. As of 1/9/19, based on data provided by the Investment Company Institute (ICI).

23. At present, roughly 40 percent of the government MMF complex is restricts its shareholders to natural persons per the same ICI data.

well in excess of the $2.8 trillion in wholesale deposits among the twelve banks in our sample.[24,25, 26,27] (This does not rule out some costly price impacts.)

On the other hand, given the rapidity that we would assume for cyber-run-related desired investments in MMFs, it may be difficult for government MMFs to grow their assets quickly enough. In the past, repurchase agreements intermediated by the banking system have proven to be a key outlet for short-term demands, constituting the majority of the expansion of these funds around the implementation of new U.S. MMF rules in 2016, including more than $200bn in September and October of that year alone.[28] However, regulatory constraints on large bank balance sheets—including G-SIB surcharges and the supplementary leverage ratio (SLR) rule—have made it more difficult for large bank-affiliated dealers to intermediate a large increase in demand for repos.[29] This would be even more difficult to accomplish on very short notice, barring an emergency waiver of these capital rules. For example, the SLR rule, at 5 percent for U.S. G-SIB dealers, implies an extra $5 billion capital requirement for each $100 billion expansion of the balance sheet. The Fed's Overnight Reverse Repurchase Agreement (RRP) Facility offers a critical outlet for these funds. Based on the current $30bn limits and the list of its counterparties, the

. . .

24. ICI data shows government MMF holdings at approximately $2.3 trillion as of this writing, including both retail and institutional funds.

25. The FRBNY posts daily detailed holdings of Treasuries and Agencies on its website at https://www.newyorkfed.org/markets/soma/sysopen_accholdings.html.

26. Sales of any USD holdings, including T-Bills and Treasuries, by foreign central banks would, if not washed via buying other USD assets, have significant exchange rate implications. Further, a stock of USD is required for facilitating international trade as well as managing capital inflows and outflows. As a result USD assets held in foreign official accounts.

27. All as of September 2018 to align with our LCR disclosure sample. We begin with the Monthly Statement of the Public Debt (MSPD) from the U.S. Treasury, which indicates roughly $2.1tn of T-Bills, $1.8tn of Notes and Bonds (<397 days remaining maturity), and just under $370bn of FRNs. Of those, TIC data from the same period indicates roughly $370bn of T-Bills and $3.6tn of Notes and Bonds (we believe roughly 10 percent of which are <397 days remaining maturity) are held by foreign official institutions, and therefore likely part of FX reserves and more removed from the freely tradeable float. Data on holdings of long-term securities from the Federal Reserve Bank of New York indicates that $420bn of short Notes and Bonds, and $18bn of FRNs, were held in its System Open Market Account (SOMA) holdings, and therefore also not free to trade. The various government agency issuers (FNMA, FHLMC, FHLB, etc.) have approximately $600bn in total outstanding debt inside one-year remaining maturity, and the June 2017 TIC Foreign Holdings Survey suggests the majority of that is not held by foreign official accounts. Finally, Federal Reserve Board H.8 data on large commercial bank holdings shows roughly $2.5tn of repurchase agreements, the vast majority of which likely have Treasury or Agency collateral, and therefore would be eligible for government MMF investment.

28. New MMF reforms implemented in October 2016 imposed gates, fees and floating NAVs on prime MMFs that made them much less attractive to institutional investors. This led to an exodus of those accounts to the government MMF complex, which was not subject to many of these new rules. As a result, NYFRB data shows that their assets grew by nearly $1.5tn over the course of that year, peaking at more than $200bn per month in September, October, and November. Dealer-intermediated triparty repo constituted the majority of the increase in assets over 2016, and more than that in several of the more disruptive months.

29. Among other impacts, these rules penalize in-scope banks when they grow their balance sheet, which would be required to hold the collateral supplied by government MMFs via repo. For details see Duffie (2018) and references therein.

RRP Facility could in principle provide significant capacity, in the hundreds of billions of dollars, in short order—and has done so when dealers have been unable to intermediate large repo flows.[30]

Even if the government MMF complex could absorb these flows sufficiently quickly and in principle provide same-day liquidity, it would be highly problematic to rely on them as *de facto* payment nodes for operational funds. First and foremost, it is not clear that managing the requisite volume of payment activity would be operationally feasible on short notice. Because MMFs are not directly linked to the payment system, processing daily payroll, settlement, and other financial transactions would require high-volume intraday share creation and redemption. Based on the LCR disclosures in our sample, roughly two thirds of wholesale deposits currently held at large banks—about $1.8 trillion—are considered operational, and therefore likely to demand a high rate of turnover. Substitution of a large fraction of operational deposits with MMF investments in the wake of a cyber run would dramatically increase the demand for MMF share redemption and creation activity. Along these lines, MMF regulations allow the boards of these funds to impose gates and fees in the event that they cannot manage high transaction volumes.[31]

Second, and perhaps more importantly, net payment activity can vary significantly throughout the day, with frequent and unpredictable shortfalls that must be actively managed (McAndrews and Kroeger, 2016). In light of potential intra-day liquidity shortfalls, the Fed provides two forms of daylight settlement liquidity to the banking system: overdrafts and excess reserves (Bech, Martin, and McAndrews, 2012). Since the financial crisis, as shown in Figure 3, an abundance of excess reserves has allowed banks to substantially reduce their reliance on overdrafts to manage intraday liquidity needs—materially reducing risks to the payment system (McAndrews and Kroeger, 2016). Government MMFs, however, do not have direct access to reserves or daylight Fed liquidity. As of this writing, the weighted average maturity (WAM) of their holdings is around 30 days with approximately 60 percent in overnight liquidity.[32] The amount of potentially needed intra-day liquidity could be substantial. Pre-crisis peak daylight overdrafts, a rough proxy, reached approximately $185 billion in Q3 2008.

Putting this all together, non-bank liquidity outlets are sufficient in potential size to serve as a safe haven, and in principle have same-day liquidity. However, were significant operational funds to migrate to the government MMF complex, the resulting needs for high-volume payments and turnover could easily overstrain the operational capabilities of these money funds. Their lack of access to Fed daylight liquidity sources might introduce significant frictions to the payment system, which could have severe negative spillover consequences for real sectors of economy.

Digital token-based currencies, whether publicly or privately issued, could eventually become an additional safe haven. This would enhance both the ability of depositors to instantly place their deposits in a safe place from which payments could be made. On the other hand, the availability of such an easily

. . .

30. For example, this can occur around quarter-ends and year-ends when regulatory snapshots make balance-sheet intensive trades like repo particularly punitive. The list of RRP counterparties is available on the New York Fed's website.

31. Government MMFs are generally exempt from the gates and fees required for prime funds by recently revised 2a-7 U.S. money market rules. That said, the boards of all funds have the right to impose these restrictions in the event they determine it is required to maintain compliance with those rules and/or their fiduciary duty to shareholders.

32. From the Investment Company Institute data on money market fund portfolios, available on their website: https://www.ici.org/research/stats/mmfsummary/nmfp_11_18.

accessible safe haven heightens run risk, as explained by the Committee on Payments and Market Infrastructure (2018).

A further possibility would be to provide a group of key institutional depositors, such as money funds, with temporary emergency accounts at Federal Reserve banks, giving them direct and safe access to the payment system. This would presumably require new legislation. Sweden, perhaps among other countries, has already begun to consider broad access to central bank accounts, creating a new form of central bank digital currency (Sveriges Riskbank, 2018).

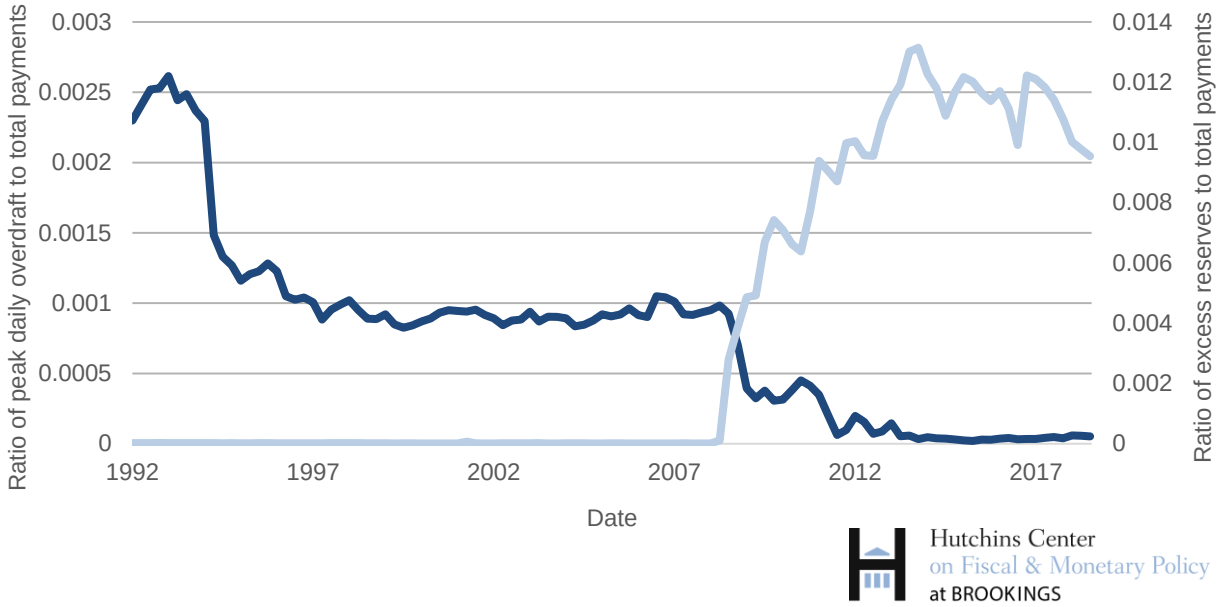

Figure 3. Quarterly peak daylight overdrafts, normalized by quarterly aggregate payment volume, and excess reserves, also normalized by quarterly aggregate payment volume.
Data source: Federal Reserve.

6. Emergency payment nodes

As we have discussed, a sufficiently extreme cyber run could dangerously slow down the processing of wholesale payments, even if every systemically important bank has ample liquidity for its own survival. As potential remedies, we have mentioned the potential use of digital token-based payments (whether private or central bank) or emergency temporary central-bank accounts for non-banks such as money market funds that could become de-facto payment nodes. These approaches bring significant costs and benefits.

A further possibility is an "emergency payment node" (EPN), which we envision as follows.

An EPN would be a bank that remains dormant except during an operational crisis in the payment system. When activated, an EPN processes payments, as requested, within a prescribed wholesale payment network consisting of eligible banks and non-bank financial firms, such as primary dealers,

money market funds, and government sponsored enterprises.[33] The EPN's only assets would consist of Federal Reserve deposits, presumably held at the Federal Reserve Bank of New York.[34] Each eligible EPN account holder would have a standing deposit account at the EPN, normally holding zero or *de minimis* balances. As depicted in Figure 4, during a crisis, the EPN would become available to its account holders for sending and receiving payments. Depending on the type of account holder (bank versus non-bank), payments could be settled by an EPN in its own deposits or in reserves.

An EPN is therefore a form of narrow bank.[35] Given the nature of its balance sheet and payment function, the EPN would presumably have no regulatory capital requirements other than perhaps the capital requirement associated with operational risk (Afonso, Curti, and Mihov, 2019).

Analogously, in the aftermath of the financial crisis, repo market participants considered setting up a special-purpose financial institution that could be activated in an emergency to backstop a tri-party repo clearing bank.[36] This "New Bank" project never came to fruition, possibly because of the significant associated need for standby capital commitments.

Although an EPN would not be perfectly immune to a cyber event, under normal safeguards it would be significantly more resistant to cyber risk than a large operating bank, given the extremely narrow function of an EPN, the highly proscribed set of eligible account holders, the limited points of network access, and the lack of normal account activity outside of an operational payment crisis. On the other hand, it would be costly to maintain an EPN in a constant state of operational readiness. Potential users would also bear costs for maintaining durable, albeit dormant, account access. Moreover, running periodic stress tests of an EPN increases the risk that the EPN itself could become infected with latent cyber viruses.

Without countervailing protections, an EPN could accelerate a run on banks because it would be an excellent haven for depositors seeking both safety and liquid access to the payment system. This flight risk can be mitigated by restricting or discouraging EPN account holders from using their accounts heavily as a store of value. While non-zero EPN account balances would be necessary to obtain intra-day payment netting efficiencies, very large balances would be unnecessary. For example, deposits could be non-interest bearing, and opening balances could be limited. Keeping an EPN in moth balls until needed and closing it immediately after an operational incident is resolved would also mitigate the run risk posed by

. . .

33. The relevant set of EPN account holders could be similar to the set of firms that is eligible to participate in the Fed's Reverse Repurchase (RRP) facility. As stated by the Federal Reserve Bank of New York, "Participation in the [RRP] operations is open to the Federal Reserve's primary dealers as well as its expanded RRP counterparties. Expanded RRP counterparties include a wide range of entities, including 2a-7 money market funds, banks, and government-sponsored enterprises. Additional details on the RRP counterparties are available on the New York Fed's website." https://www.newyorkfed.org/markets/rrp_faq.html

34. As an operational backup, accounts at Federal Reserve Bank of New York can be accessed in an emergency via satellite FRBNY facilities at the Federal Reserve Bank of Chicago. A Reuters report cited sources indicating that this backup is in part designed to address operational risks with a cyber attack. See "Wary of natural disaster, NY Fed bulks up in Chicago," Jonathan Spicer, Reuters, April 14, 2015.

35. As a matter of disclosure, one of the authors is a member of the board of directors of TNB Inc., which proposes to offer an unrelated form of narrow-banking product to cash investors.

36. See Federal Reserve Bank of New York (2010) at Footnote 13.

an EPN. In the event that flows to the EPN do begin to stress the liquidity of large banks, the Fed remains an available source of liquidity to those banks.

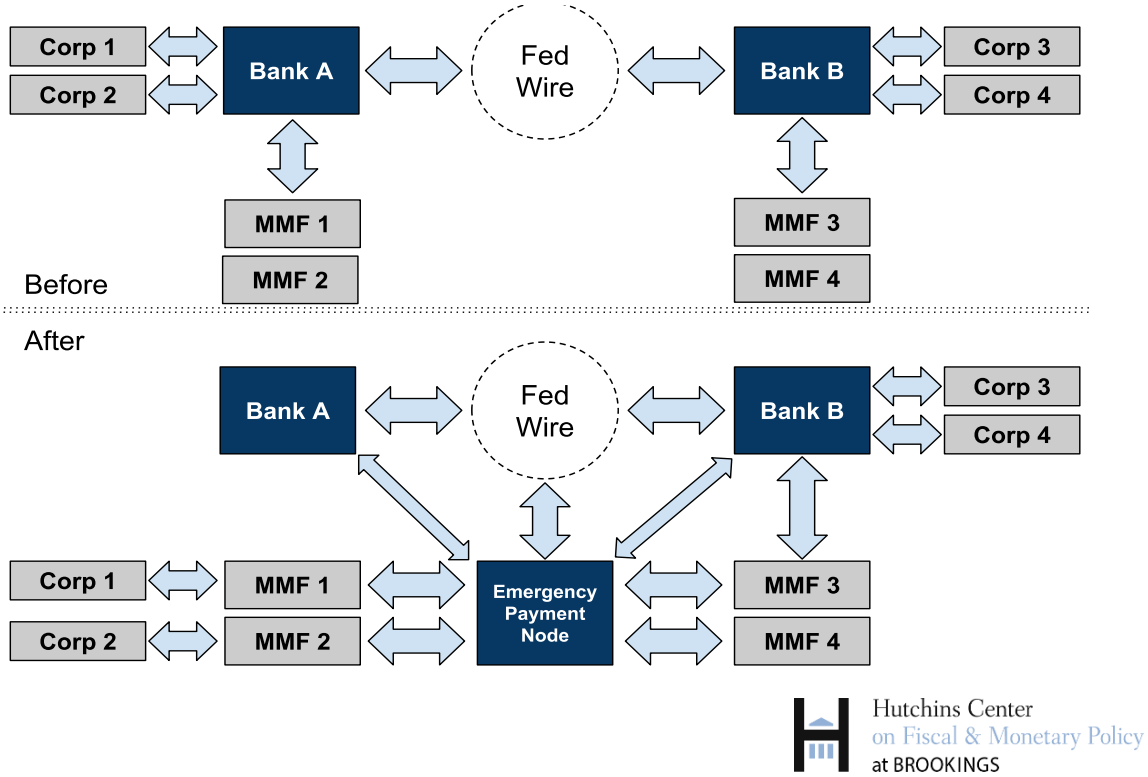

Figure 4. Schematic of the role of an emergency payment node (EPN), before being deployed for an operational payment-system emergency ("Before"), and after being deployed ("After").

The EPN could perhaps be operated and governed as an industry utility, in the spirit of the New York Clearing House Association (NYCHA), which was a crisis backstop to the bank deposit system before the Fed existed (Gorton, 1985). Like an EPN, the NYCHA was not only an inter-bank clearinghouse – it also provided direct access to non-bank depositors who were concerned about holding their funds in conventional bank accounts.[37] The NYCHA was designed to mitigate run risk associated with uncertainty over the credit quality of banks, rather than the risk of payment slowdowns or gridlock associated with operational risk.

. . .

37. As noted by Gorton (1985), "During the panics of 1893 and 1907 clearinghouses took the further step of issuing loan certificates, in small denominations, directly to the public. Since this did not involve replacing gold in the clearing process, but instead was the direct monetization of bank portfolios, large amounts of money could be created and issued to the public in exchange for demand deposits."

7. Incorporating cyber events into stress tests

An EPN would not, on its own, be a sufficient safeguard. The effectiveness of an EPN in reducing the impact of a major cyber incident is contingent on detailed contingency planning by major participants and nodes in the financial system. Given the potential for adverse impacts on financial and economic stability through shortfalls in bank liquidity and the fluidity of the payment system, the stakes are large. Much of the literature on cyber security, particularly as it pertains to the banking system, is vague. This is probably partly by design, to avoid disclosure of defenses that may be instructive to malicious actors. Official-sector U.S. preparedness policies, summarized in Appendix B, have focused on guidelines, metrics, and information sharing. The natures and targets of cyber attacks, not to mention their downstream impacts, vary enormously.

Scenario analysis, despite its limitations, has proven valuable for the purpose of preparing for extreme but plausible adverse systemic events. Examples include the famous Long-Term Studies group at Royal Dutch Shell (Wilkinson and Kupers, 2013). The financial private sector has already engaged—in partnership with the U.S. Treasury and other government agencies—in the "Hamilton Series" of cyber event simulations.[38] Going further, bank regulators could include cyber scenario analyses into their Dodd-Frank mandated stress-tests, within the existing frameworks for operational risk (Federal Reserve Board, 2018). Given the interactions that we have outlined between cyber runs, financial stability, payment systems, and the macro-economy, holistic scenarios incorporating cyber runs could reveal some of the most pertinent systemic interactions.

Consistent with our emphasis on testing for the implications of contagion in a cyber event, Kashyap and Weltherit (2018) stated a principle of *"cyber stress tests that explore common vulnerabilities that may amplify the impact of a cyber shock."* The Bank of England, set in motion by its Financial Policy Committee (FPC), plans to conduct cyber stress tests in 2019 with this principle in mind, and with a focus on payments.[39]

The FPC and the Committee on Payments and Market Infrastructure (2016) place heavy emphasis on rapid within-day recovery from cyber events. The FPC calls for within-day recovery, but concedes that this is currently not attainable. The CPMI standard for the cyber resilience of financial market infrastructure is a 2 hour recovery time, or "2hRTO," but this standard remains aspirational for most payments-related FMI. Moreover, it is difficult to predict how the arriving new generation of 24/7 fast payment systems will affect minimum critical recovery times.[40]

It would also be useful to incorporate non-bank liquidity outlets—including government MMFs—into cyber stress tests, given their potential to act as *de facto* payment nodes during a cyber run. Recently revised 2a-7 money market fund rules do require some stress testing of MMFs, but these tests focus

. . .

38. The Financial Systemic Analysis and Resilience Center (FSARC, 2016) was stood up by the Financial Services - Information Sharing and Analysis Center (FS-IAC) in order to "proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cyber security threats." FSARC ran the "Hamilton Series" of simulations in conjunction with the public sector, to improve the capacity to identify, resolve, and recover from cyber incidents (Feeney, 2017; Waterman, 2018).

39. See Bank of England (2018), Box 1, at pp. 40-41.

40. See Federal Reserve System (2018).

mainly on outflows triggered by credit events and interest rate shocks rather than by stresses associated with surges in inflows and turnover (Berkowitz, 2015). The ability of an EPN to successfully reduce frictions in the payment system following a cyber run relies on certain non-banks such as MMFs to have adequate contingency plans and systems to operate under that kind of stress.

Unfortunately, the specific nature of scenario analysis is also a limitation. History offers relatively little guidance regarding the most likely proximate causes and channels of cyber stresses. Nevertheless, building processes that will answer these questions is a key part of the value of the exercise. In designing and responding to cyber stress tests, regulators and systemically important institutions—including banks and MMFs—are forced to think holistically and granularly about likely scenarios, propagation channels, and responses. This is especially useful in the relatively uncharted area of cyber runs.

REFERENCES

Ablon, Lillian, 2018, "Data Thieves," Testimony before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, March. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf

Afonso, Gara, Filippo Curti, and Atanas Mihov, 2019, "Coming to Terms with Operational Risk," *Liberty Street Economics,* Federal Reserve Bank of New York, January 7, 2019. https://libertystreeteconomics.newyorkfed.org/2019/01/coming-to-terms-with-operational-risk.html

Ashcraft, Adam and Darrell Duffie, 2007, "Systemic Illiquidity in the Federal Funds Market, *AEA Papers and Proceedings,* Volume 97, pages 221-25.

Ashcraft, Adam, James McAndrews, and David Skeie, 2009, "Precautionary Reserves and the Interbank Market," Federal Reserve Bank of New York, Staff Report Number 370, May. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr370.pdf

Baklanova, Viktoria, Adam Copeland, and Rebecca McGaughrin, 2015, "Reference Guide to U.S. Repo and Securities Lending Markets," Federal Reserve Bank of New York Staff Report No. 740, December. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr740.pdf

Bank of England, 2018, Financial Stability Report," Issue 43, June. https://www.bankofengland.co.uk/-/media/boe/files/financial-stability-report/2018/june-2018.pdf

Bank for International Settlements, Financial Stability Institute, 2017, "Regulatory Approaches to Enhance Banks' Cyber-Security Frameworks," Bank for International Settlements, Basel. http://www.asbasupervision.com/en/bibl/recommended-reading/1556-lr241/file

Bech, Morten, Antoine Martin, and James McAndrews, 2012,"Settlement Liquidity and Monetary Policy Implementation," *Economic Policy Review,* Vol. 18, No. 1, March. https://www.newyorkfed.org/research/epr/12v18n1/exesum_mart.html

Belton, Terry, 2018, "Treasury Supply, Liquidity, and Demand for Reserves," presented at Reserve Reduction, Money Markets, and Futures Frameworks, a conference at the Columbia School of International Affairs, September. https://www.newyorkfed.org/medialibrary/media/newsevents/events/markets/2018/Terry-Belton-Treasury-Supply-Liquidity-and-Bank-Demand-for-Reserves.pdf

Berkowitz, Jeremy, 2015, "Money Market Mutual Funds: Stress Testing and New Regulatory Requirements," Harvard Law School Forum on Corporate Governance and Financial Regulation, July. https://corpgov.law.harvard.edu/2015/07/14/money-market-mutual-funds-stress-testing-new-regulatory-requirements/

Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation, 2016, "Enhanced Cyber Risk Management Standards," Joint Advanced Notice of Proposed Rulemaking, Board of Governors, OCC, and FDIC, Washington D.C., October. https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20161019a1.pdf

Boer, Martin, and Jaime Vazquez, 2017, "Cyber Security and Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System. Institute of International Finance, September. https://www.iif.com/Portals/0/Files/IIF%20Cyber%20Financial%20Stability%20Paper%20Final%2009%2007%202017.pdf?ver=2019-02-19-150125-767

Borghard, Erica, 2018, "Protecting Financial Institutions Against Cyber Threats: A National Security Issue," Carnegie Endowment for International Peace, September. https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324

Bouveret, Antoine, 2018, "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment," Working Paper 18/143, International Monetary Fund, June https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx

Bush, Ryan, Adam Kirk, Antoine Martin, Phil Weed, and Patricia Zobel, 2019,"Stressed Outflows and the Supply of Bank Reserves," *Liberty Street Economics*, February 20. https://libertystreeteconomics.newyorkfed.org/2019/02/stressed-outflows-and-the-supply-of-central-bank-reserves.html

Carnegie Endowment for International Peace, 2017, "Toward a Global Norm Against Manipulating the Integrity of Financial Data," March. https://carnegieendowment.org/files/Cyber_Financial_Data_white_paper.pdf

Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions, 2016, "Guidance on Cyber Resilience for Financial Market Infrastructures," Bank for International Settlements, June. https://www.bis.org/cpmi/publ/d146.pdf

Committee on Payments and Market Infrastructure, Markets Committee, 2018, Central bank digital currencies. Committee on Payments and Market Infrastructures, Bank for International Settlements, March. https://www.bis.org/cpmi/publ/d174.pdf

Curti, Filippo, and Atanas Mihov, 2018, "Diseconomies of Scale in Banking: Evidence from Operational Risk," Working paper, Federal Reserve Bank of Richmond, April. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3210206

Diamond, Douglas, and Philip Dybvig, 1983, "Bank Runs, Deposit Insurance, and Liquidity," *Journal of Political Economy,* Volume 91, pages 401-419.

Duffie, Darrell, 2018, "Post-Crisis Banking Regulations and Financial Market Liquidity," Paolo Baffi Lecture on Money and Finance, Banca d'Italia, Eurosystem, March. https://www.darrellduffie.com/uploads/policy/DuffieBaffiLecture2018.pdf

Ennis, Huberto, and David Price, 2015, "Discount Window Lending: Policy Trade-offs and the 1985 BoNY Computer Failure." Economic Brief no. 15-05. Richmond, Va.: Federal Reserve Bank of Richmond, May. https://www.richmondfed.org/%7E/media/richmondfedorg/publications/research/economic_brief/2015/pdf/eb_15-05.pdf

Federal Financial Institutions Examination Council, 2015, "Cybersecurity Assessment Tool," Washington D.C., June. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf

Federal Register, 2016, "Enhanced Cyber Risk Management Standards," Volume 81, No. 207, pages 74315-74326, Washington D.C., October. https://www.govinfo.gov/content/pkg/FR-2016-10-26/pdf/2016-25871.pdf

Federal Reserve Bank of New York, 2010, "Tri-Party Infrastructure Reform," White Paper, May. https://www.newyorkfed.org/medialibrary/media/banking/nyfrb_triparty_whitepaper.pdf

Federal Reserve Board, 2017, "Federal Reserve Payments Study: 2017 Annual Supplement," Washington D.C., December. https://www.federalreserve.gov/newsevents/pressreleases/files/2017-payment-systems-study-annual-supplement-20171221.pdf

Federal Reserve Board, 2018, "Dodd-Frank Act Stress Test 2018: Supervisory Stress Test Methodology and Results," Washington D.C. https://www.federalreserve.gov/publications/files/2018-dfast-methodology-results-20180621.pdf

Federal Reserve System, 2018, "Potential Federal Reserve Actions To Support Interbank Settlement of Faster Payments, Request for Comments," Federal Register of Proposed Rules. 12 CFR Chapter II, Docket No. OP–1625, Washington, November. https://www.govinfo.gov/content/pkg/FR-2018-11-15/pdf/2018-24667.pdf

Feeney, Christopher, 2017, "Testimony on Behalf of the Business Roundtable to the United States Senate Committee on Homeland Security & Governmental Affairs," Washington D.C., June 21. https://www.hsgac.senate.gov/imo/media/doc/Testimony-Feeney-2017-06-21.pdf

Financial Services Information Sharing and Analysis Center, 2016, "FS-ISAC Announces The Formation Of The Financial Systemic Analysis & Resilience Center (FSARC), Established by Financial Institutions, FSARC Deepens Analytic Capabilities to Combat Cyber Risk and Strengthen Resiliency of U.S. Financial System," Press Release, FS-IAC, October 24. https://www.prnewswire.com/news-releases/fs-isac-announces-the-formation-of-the-financial-systemic-analysis--resilience-center-fsarc-300349678.html

Gorton, Gary, 1985, "Clearinghouses and the Origin of Central Banking in the United States," *The Journal of Economic History,* Volume 45, pages 277-283.

Healey, Jason, Patricia Mosser, Katheryn Rosen, and Adriana Tache, 2018, "The Future of Financial Stability and Cyber Risk," Brookings Institution Report, October 10, 2018. https://www.brookings.edu/wp-content/uploads/2018/10/Healey-et-al_Financial-Stability-and-Cyber-Risk.pdf

Howell, Jen Patja, 2018, "Cybersecurity and Financial Stability," The Lawfare Podcast, November 3, 2018. https://www.lawfareblog.com/lawfare-podcast-cybersecurity-and-financial-stability

Ihrig, Jane, Edward Kim, Ashish Kumbhat, Cindy Vojtech, and Gretchen C. Weinbach, 2017, "How Have Banks Been Managing the Composition of High Quality Liquid Assets?" Federal Reserve Board, Finance and Economics Discussion Paper 2017-092. https://www.federalreserve.gov/econres/feds/files/2017092pap.pdf

Kacperczyk, Marcin and Philipp Schnabl, 2010, "When Safe Proved Risky," *Journal of Economic Perspectives,* Volume 24, Number 1, pages 29–50. https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.24.1.29

Kacperczyk, Marcin, and Philipp Schnabl, 2013, "How Safe Are Money Market Funds?" The *Quarterly Journal of Economics,* Volume 128, pages 1073-1122.

Kashyap, Anil, and Anne Wetherilt, 2018, "Some Principles for Regulating Cyber Risk," Bank of England, Prudential Regulatory Authority, December. http://faculty.chicagobooth.edu/anil.kashyap/research/papers/Some_Principles_for_Regulating_Cyber_Risk.pdf

Kopp, Emanuel, Lincoln Kaffenberger, and Christopher Wilson, 2017, "Cyber Risk, Market Failures, and Financial Stability," International Monetary Fund Working paper 17/185, August. https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104

Lacker, Jeffrey, 2003, "Payment System Disruptions and the Federal Reserve Following September 11, 2001," Working paper 03-16, Federal Reserve Bank of Richmond, December. https://www.richmondfed.org/~/media/richmondfedorg/publications/research/working_papers/2003/pdf/wp03-16.pdf

McAndrews, James J., and Simon Potter, 2002, "Liquidity Effects of the Events of September 11, 2001," *FRBNY Economic Policy Review,* Volume 8 (1), pages 59-79.

McAndrews, James J., and Alexander Kroeger, 2016, "The Payment System Benefits of High Reserve Balances," Federal Reserve Bank of New York Staff Reports, No. 779, June. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr779.pdf?la=en

Martin, Christopher, Manju Puri, and Alexander Ufier, 2018, "Deposit Inflows and Outflows in Failing Banks," FDIC Center for Financial Research Working Paper No. 2018-02, May. https://www.fdic.gov/bank/analytical/cfr/2018/wp2018/cfr-wp2018-02.pdf

Office of Financial Research, 2017, "Cybersecurity and Financial Stability: Risks and Resilience," Viewoint paper, Office of Financial Research, Washington D.C., February. https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf

Petrasic, Kevin, 2010. "The Dodd-Frank Wall Street Reform and Consumer Protection Act: Affiliate Transaction and Insider Lending Restrictions," Paul Hastings, Stay Current, July. https://www.paulhastings.com/docs/default-source/PDFs/1690.pdf

Rosengren, Eric, 2015, "Cyber Security and Financial Stability," Remarks at Forum on "Strengthening Financial Sector Supervision and Current Regulatory Priorities," organized by the Basel Committee on Banking Supervision and the Financial Stability Institute. January.

Rubenfeld, Samuel, 2019, "Bangladesh Bank Sues Filipino Lender in U.S. Court Over Hack Heist: The New York Fed is assisting the Bangladeshi central bank with the lawsuit," *Wall Street Journal,* February 4, 2019. https://www.wsj.com/articles/bangladesh-bank-sues-filipino-lender-in-u-s-court-over-hack-heist-11549294562

Schmidt, Lawrence, Allan Timmermann, and Russ Wermers, 2016, "Runs on Money Market Mutual Funds, *American Economic Review,* Volume 106, pages 2625-2657. https://www.aeaweb.org/articles?id=10.1257/aer.20140678

Sveriges Riksbank. 2018. Distributed ledgers: The Riksbank's e-krona project: Report 2. White paper. Stockholm, October. https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf

U.S. Department of Justice, 2016, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," Press release, March 24. https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

Waterman, Shaun, 2016, "Bank Regulators Briefed on Treasury-Led Cyber Drill," Fedscoop, July 20, 2016. https://www.fedscoop.com/us-treasury-cybersecurity-drill-july-2016/

Wilkinson, Angela & Roland Kupers, 2013, "Living in the Futures," *Harvard Business Review,* May.

APPENDIX A: ILLUSTRATIVE RUNOFF ASSUMPTIONS

As part of this exercise we have assembled several runoff scenarios under different assumptions. To summarize.

1. *LCR runoff*: We assume 30-day cumulative outflows consistent with weighted net LCR assumptions for a given bank, including industry aggregates or averages, based on 3Q 2018 disclosure (24 percent for an average money center bank). For timing, we assume a 10 percent initial runoff rate converging to a constant daily rate over a two week period.
2. *Adverse cyber run*: We assume a runoff rate of 20 percent on the first day of the incident, remaining at 10 percent for the next week, before slowing to a constant rate consistent with 50 percent cumulative runoff over 30 business days.
3. *Severe cyber run*: We assume an initial daily runoff rate of 30 percent daily, slowing to 20 percent on day 2 and 10 percent on day 3, remaining there until day 10 before slowing to a constant daily rate consistent with 75 percent cumulative runoff over 30 business days.

We make some assumptions regarding the ability of that bank to raise cash from sales of HQLA, informed by Primary Dealer Statistics provided by the New York Fed as well as TRACE data summarized by SIFMA.

1. *Federal Reserves* (level 1) are available for intraday liquidity.
2. *Treasuries* (level 1) can be sold at a rate of $100bn per day, with T+1 settlement.
3. *Ginnie Mae MBS* (level 1) can be sold at a rate of $3bn per day with T+1 settlement.
4. *Conventional MBS* (level 2A) can be sold as a rate of $6bn per day with T+1 settlement.

It is important to note that this ignores the ability of banks to raise intraday cash via Treasury and MBS repo, which in principle provides an important and substantial source of short-term liquidity. As stated in the main text of our paper, we also ignore price impacts.

APPENDIX B: WHAT IS THE CURRENT STATE OF PREPAREDNESS POLICY?

Resilience against cyber attack has become a key element of not just economic but also national security policy. Policy responses in the United States revolve around the identification and protection of critical infrastructure, defined by Executive Order as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." For financial services in particular, the Sector-Specific Plan (SSP) put forth by the U.S. Departments of the Treasury and Homeland Security specifically enumerates four critical services provided by financial institutions: "(1) deposit, consumer credit, and payment systems products; (2) credit and liquidity products; (3) investment products; and (4) risk transfer products."[41] Since the initial SSP was published in 2015 there has been significant progress towards establishing preparedness guidelines and metrics, as well as coordination and information sharing across each of these areas.

The Dodd-Frank Act of 2010 led to the creation of the Financial Stability Oversight Council (FSOC), charged with monitoring and—to some extent—taking actions to mitigate emergent risks to financial stability, including cyber attacks.[42] In the specific area of cyber security, the Financial and Banking Information Infrastructure Committee (FBIIC) is charged with identifying critical infrastructure assets and their vulnerabilities, as well as facilitating secure communication among regulators and other public sector stakeholders in the event of an emergency.[43] The prudential regulators have also made an advanced notice of proposed rulemaking regarding enhanced cybersecurity standards (Federal Register 2016).

International organizations have also taken important steps, including guidance from the Bank for International Settlements (BIS), a standardized lexicon for study and discussion of cyber threats from the Financial Stability Board (FSB), and proposed global norms safeguarding the integrity of financial data.[44]

On the private side, the Financial Systemic Analysis and Resilience Center (FSARC), stood up by the Financial Services - Information Sharing and Analysis Center (FS-IAC), in order to "proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cyber security threats."[45] In conjunction with official-sector actors, the technology policy division Financial Services Roundtable facilitated a series of simulations (the "Hamilton Series") that were designed to improve the capacity to identify, resolve, and recover from cyber incidents (Feeney, 2017). The FS-IAC is also responsible for Sheltered Harbor, a non-profit subsidiary tasked with safeguarding the integrity of systemically important financial data in order to maintain customer access to funds.

. . .

41. Financial Services Sector Specific Plan, Depts. of the Treasury and Homeland Security, 2015.

42. See 2018 FSOC Annual Report.

43. At https://www.fbiic.gov/

44. See Toward a Global Norm Against Manipulating the Integrity of Financial Data, Carnegie Endowment for International Peace, March 2017.

45. See FSARC Formation Announcement, 10/24/16.

Hutchins Center
on Fiscal & Monetary Policy
at BROOKINGS

The mission of the Hutchins Center on Fiscal and Monetary Policy is to improve the quality and efficacy of fiscal and monetary policies and public understanding of them.

Questions about the research? Email communications@brookings.edu.
Be sure to include the title of this paper in your inquiry.