THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 14 | Number 4 Article 2

April 2020

Cyber-Security Risks of Fedwire

Mark J. Bilger
Norwich University, mbilger141@gmail.com

CYBER-SECURITY RISKS OF FEDWIRE

Mark J. Bilger
Norwich University
mbilger141@gmail.com

ABSTRACT

This paper will review the risks associated with the Federal Reserve's Fedwire network as a key resource necessary for the efficient function of the American financial system. It will examine the business model of the Fedwire system of real-time interbank transfers, the network characteristics of Fedwire, and the possibility of a successful attack on Fedwire and its potential impact on the U.S. financial system.

Keywords: Banking, Cyber-attack, Federal Reserve, Fedwire, Payment Networks.

1. THE CORE OF AMERICAN BANKING

Experts estimate the global gross domestic product (GDP) in 2017 was approximately $75 trillion - of which the United States GDP was the largest at 18 percent (Statistica, 2019). The central bank of the United States is the Federal Reserve Bank `(The Fed)`. Central banks play key roles in national economies by setting key interest rates, and influencing their commercial banking systems. As the Federal Reserve (2017) states, in establishing the Federal Reserve System, the United States was divided geographically into 12 Districts, each with a separately incorporated Reserve Bank. District boundaries were based on prevailing trade regions that existed in 1913 and related economic considerations, so they do not necessarily coincide with state lines" (para. 2).

The New York Federal Reserve Bank, located at 33 Liberty Street in Manhattan, manages more than half of the assets on the Fed's balance sheet. Author and professor of computer science Ted G. Lewis (2015) describes the New York Federal Reserve Bank simply as, `‘‘...the central hub of the banking system network’’` (p. 313). The Fed enables the transfer of funds between banks who maintain Federal Reserve accounts through the Fedwire Funds Service. Fedwire is a real-time settlement system. Fedwire transfers are one-way, which means banks can wire funds out, but cannot debit other banks and wire funds in. Fedwire is a payment system and does not perform the traditional banking functions of managing deposits and withdrawals. It simply transfers funds between accounts within the Federal Reserve System. Once Fedwire transactions are complete, they are irrevocable.

2. ORIGIN AND HISTORY

After the creation of the Federal Reserve System in 1913, the Fed began to offer leased-wire communications to enable the transfer of funds among the Reserve Banks and to member banks. This eliminated the previous need for regional exchanges that existed to ship

gold and currency between regions within the United States (Gilbert, Hunt, Winch, 1997, p.2). Fedwire began operation in 1918 using Morse-coded transfers on the Fed's private telegraphy network (Lewis, 2015, p. 316). Fedwire's book-entry transfers of account balances were a vast improvement over physical transfers of financial assets like gold, silver, and currency.

Fedwire evolved gradually from telegraphy to a public switched network of telex teleprinters, and finally to digital telecommunications (Federal Reserve, 2014, section Brief History, para. 2). With the advent of general-purpose commercial computing technologies in the 1960s, each Federal Reserve Bank deployed its own software, programmers, and data processing centers. We know this because the Federal Reserve admits that in the 1980s, it consolidated all Fedwire services onto a single software platform across all Reserve Banks (section Brief History, para. 3). Today, the Fedwire system is combined into a single network, FEDNET, which employs a common proprietary protocol for funds transfer (Gilbert, Hunt, Winch, 1997, p.4).

3. FEDWIRE AS A FORCE MULTIPLIER

The value of the funds transferred with Fedwire is staggering. In 2018, Fedwire executed 158 million transfers with an aggregate value of $716 trillion (Federal Reserve, 2019). While many of the fund transfers executed by Fedwire were of small value, the average value per transfer in 2018 was $4.5 million. By calculating a media payment value of $36,000 and an average value of $5 million, researchers Morten Bech and Enghin Atalay (2010) found Fedwire payments in 2016 were heavily skewed by a few large transactions (p. 5226). The U.S.

Bureau of Economic Analysis (2019) estimated that 2018 total gross domestic product (GDP) was $20.5 trillion (para. 12). Fedwire may be viewed as a kind of force multiplier for the American economy by processing annual banking payments at 35 times the country's GDP. Further evidence of Fedwire's role promoting the efficiency of American financial markets can be seen by considering Fedwire payments against the aggregate value of all deposits at U.S. lending institutions - $12.6 trillion in March of 2019 (Federal Reserve Bank of St. Louis, 2019). Fedwire payments for the previous year were 57 times this figure.

4. BANKING UNDER SIEGE

When Saturday Evening Post reporter Bob Yoder asked famed bank robber Willie Sutton why he robbed banks, he famously quipped, "I rob banks because that is where the money is" (Yoder, 1951, p. 17). The simple logic that Sutton used continues to motivate cyber-criminals today. In an article for Forbes magazine, contributing writer Bhakti Mirchandani (2018) sounds the alarm for an industry under siege, the risk of a cyber-attack on financial services firms cannot be overstated. Cyber-attacks cost financial services firms more to address than firms in any other industry at $18 million per firm (vs. $12 million for firms across industries).

Financial services firms also fall victim to cybersecurity attacks 300 times more frequently than businesses in other industries (para. 1). Her reference to `'300 times greater attack frequency'` may be an overstatement, but the point is clear: cyber-criminals go where the money is, leaving banks vulnerable. Mirchandani goes on to state that in 2017 cyber-criminals stole nearly $17 billion from banks (para. 3). In contrast to the likely overstatement on attack frequency, this is probably an understatement based on pervasive under-reporting of

banking cyber breaches. International Monetary Fund (IMF) economist Antoine Bouveret (2018) created a sophisticated model to pierce through the 'veil of secrecy' he believes banks cling to in under-reporting cyber-attacks. Bouveret analyzed data from The Operational Riskdata eXchange Association (ORX) and other banking industry data sources. ORX's website says the company was created for financial institutions to, "provide a platform for the secure and anonymized exchange of high-quality operational risk loss data from around the world" `https://managingrisktogether.orx.org`. ORX houses a worldwide database of banking losses, including those from cyber-attack. Bouveret combined ORX data with other cyber-attack loss data available from companies such as Advisen, who also specialize in that area. Bouveret's model computed a baseline case of expected losses from cyber-attacks of nine percent of global banking net income – $97 billion for 2016 (p.20). This is a much larger but more defensible figure than Mirchandani's $17 billion. However, even the lower figure spotlights that banking is an industry under siege by cybercriminals.

5. FEDWIRE NETWORK TOPOLOGY

Like other complex systems, Fedwire can be modeled as a graph. The Federal Reserve Branches, commercial banks, and other participants in the system can be represented as nodes. Payments between these entities can then be represented as links between the nodes. Studies of payment systems point out an important difference they have with network models of most other complex systems. For most systems, interactions (depicted as links) represent the transfer of some type of workload. In contrast, payment system links represent the transfer of capacity, not workload (Beyeler, Glass, Bech, Soromaki, 2007, p. 694). Visualization of the Fedwire network as a graph is a good way to gain an intuitive view of the nature of Fedwire. Kimmo Soramaki of the University of Helsinki led a small group of Federal Reserve and university researchers in analyzing the Fedwire network (Soramaki, Bech, Arnold, Glass, Beyeler, 2007). Using the graphical tool Pajek, they produced a network graph of Fedwire payments for a single day in 2004 (Figure 1). While appearing to resemble a child's random etching, the figure clearly shows high-value dark links. These links highlight massive aggregate payments to just a few financial institutions.

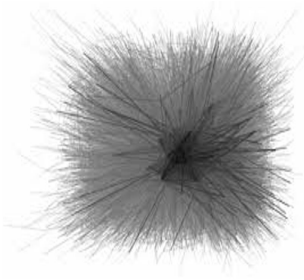

Figure 1. Fedwire network, 6600 nodes and 70,000 undirected links (p. 319)

By isolating those links and the nodes that connect them, the team was able to determine that just 66 nodes and 181 links comprised 75% of the value of daily payments. These core nodes and links are illustrated in figure 2. The inner ring of 25 densely connected financial institutions is evident in Figure 2. These institutions are completely interconnected, i.e., every node in the inner ring has a link with every other node. This is in sharp contrast to the Fedwire network as a whole. The study found the average degree (number of links per node) in the network was 15. Yet this figure can mask the fact that a few of the core nodes have thousands of links, and almost half of all nodes have less than four, with 15% linked to only a single other node (Soromaki et al., 2007, p. 325). Maximum ac-

tive links in a completely connected network would be *N*((N-1))/2* links (where N is the number of nodes). For 6,600 nodes that computes to 21.8 million links. The researchers found only 70,000 active links, indicating the network is very sparse, with only 0.3% of potential links carrying out actual payments. Fedwire is a scale-free network. A scale-free network is a network with most nodes having few connections but with highly connected hub nodes. In other words, Fedwire is a system that connects a lot of small financial institutions with a few banking giants. Bech

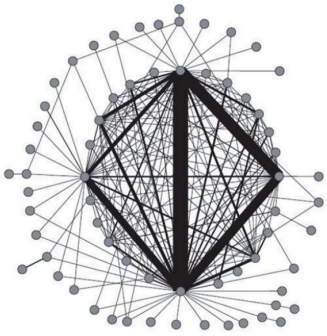

Figure 2. High-value payments of the Fedwire network (p. 320)

and Atalay (2010), analyzed nearly a decade of data on the Federal funds market from 1997-2006. Unlike Fedwire accounts, banks may both borrow and loan funds through Federal funds accounts. Larger banks typically use Fedwire to balance those accounts, and smaller banks do not make wire payments at all. They re-book loans with correspondent banks who are members of the Federal Reserve System (pps. 1-2). The study found that the network was "extremely sparse" (p.10). They also determined that the network exhibited the small-world phenomenon (p.1). Lewis describes Small-world as "a large network with a small diameter or a small number of hops to get from one node to any other" (Lewis, 2015, p.65).

Finally, they found strong evidence that the network is disassortative (p.1). Most social networks are assortative, meaning nodes link with similar nodes. We would expect assortative networks for groups of people with similar hobbies, professions, or locations. Technological systems are predominantly disassortative. Small systems (like workstations) connect primarily to large systems (like internet servers), not other small systems. While Bech and Atalay's study focused on the Federal funds market, their observations of small-world and disassortative characteristics most likely apply to Fedwire as well, since the Federal funds market relies on Fedwire to balance payments for all but the smallest institutions participating in Federal Funds. Xu, He, and Li (2016) from Nanjing University studied interbank markets and their evolution over time. Based on empirical evidence, they constructed a general model of interbank markets. They found the model to be dynamic (affected by systemic shocks like the mortgage crisis) but stable (having invariant network topology). They summarized this by concluding, "Interbank market network structure evolves with time dynamically, but the topological properties stay unchanged" (p.138). This gives us reason to believe the network topology of Fedwire remains constant, including its small-world, scale-free, and disassortative attributes.

6. SYSTEMIC RISKS OF THE FEDWIRE NETWORK

Scale-free networks like Fedwire have been shown to have significant tolerance for random failures but are highly vulnerable to targeted attacks (Crucitti, Latora, Marchiori, Rapisarda, 2007, p.394). This is because most nodes (in the case of random failure) have few links, but core nodes are highly con-

centrated (in the case of targeted attacks). As a payment network, Fedwire transfers liquidity (financial capacity) across nodes via links. Beyeler, Glass, Bech, and Soramaki (2007) studied payment systems and found low liquidity levels quickly cause network congestion. They observed that "at low liquidity, the system becomes congested and payment settlement loses correlation with payment instruction arrival, becoming coupled across the network" (p. 693). If a core node were targeted for attack, the Fedwire network might transition from a series of independent payment interactions between nodes to a coupled system where payments cannot be initiated until other payments complete. Like an engine that seizes up because it is too cold, Fedwire could grind to a glacial pace from lack of liquidity.

7. COUNTER ARGUMENTS TO FEDWIRE RISKS

There are two counter-arguments to the idea of catastrophic results from the core Fedwire node attack. First, Fedwire core nodes are most likely commercial banks classified by the government as too big to fail (TBTF). Government intervention to prop-up failing core nodes could mitigate systemic risk to overall liquidity and prevent congestion. The Fed itself states this was the case with Bear Sterns and the mortgage-crisis of 2008, Board members agreed that, given the fragile condition of the financial markets at the time, the prominent position of Bear Stearns in those markets, and the expected contagion that would result from the immediate failure of Bear Stearns, the best alternative available was to provide temporary emergency financing to Bear Stearns through an arrangement with JPMorgan Chase Co. (Federal Reserve, 2008).

However, while considered systemically important to the American economy by the Federal Reserve, Bear Sterns was not one of the commercial banks at the core of Fedwire. Also, the Fed had the luxury of time in deciding to rescue Bear Sterns since mortgages are long-lived financial instruments. Payment systems like Fedwire operate in real-time. Payments are only one aspect the Fed would need to consider in deciding to rescue a major commercial bank. It is also not clear that the impact on Fedwire would be a compelling factor in any government decisions in determining to rescue a bank. That decision would likely be driven by quality problems with the bank's lending portfolio. The second major argument against the likelihood of a catastrophic degradation to Fedwire is historical. Federal Reserve economists James McAndrews and Simon Potter (2002) studied the effects of the September 11th terrorist attacks on the Federal Reserve.

After the attacks on the morning of September 11, it was immediately clear to financial market participants that general operations and communications and computer systems in Lower Manhattan were not functioning well. A direct effect of these difficulties was a reduction in the value and volume of transfers on Fedwire on September 11 (p. 64). The value of total daily payments made through Fedwire dropped by 25% to $1.2 trillion on September 11th, from the previous day's trading of $1.6 trillion. Bank of New York has been cited as the core Fedwire participant most heavily degraded by the attack. We can think of this as the temporary removal of one of the 25 core nodes in the graph of the Fedwire network. However, by September 12th, the total payment value was restored to $1.7 trillion. Even this major catastrophe caused only a temporary drop in Fedwire payments.

8. ATTACK ON THE BANK OF BANGLADESH FEDERAL RESERVE ACCOUNT

If Fedwire is resilient to major catastrophic events, perhaps it is vulnerable to targeted cyber-attacks. An attack on the Federal Reserve account for the Bank of Bangladesh provides a recent example. According to Reuters News Service, the Bank of Bangladesh's cybersecurity in 2016 was so bad the bank lacked firewalls and used second-hand network switches (Das Spicer, 2016, Section – The Hack, para. 2). Even used switches were seen as progress for the bank, which only a decade before used an antique teleprinter over unencrypted phone lines to send and receive international payment instructions (Hammer, 2018). By 2016 the bank had upgraded its computer systems to access the SWIFT (Society for Worldwide Interbank Financial Telecommunication) financial payment network. SWIFT recommends its users deploy multi-factor authentication (MFA) to prevent stolen credentials from being used by hackers. The Bank of Bangladesh did not deploy this counter-measure – opening the bank to attack by anyone who could steal legitimate payment system credentials. Among at least five types of malware used against the bank was Dridex, a malware commonly used by Russian and eastern European cyber gangs to obtain credentials (The Straight Times, 2016, para. 2-3).

After months of lurking in the bank's systems, hackers chose the optimal time to strike at the bank's payment system, near the beginning of a long weekend on February 4th, 2016. The hackers used legitimate employee credentials to make 35 illegitimate requests for about $951 million in payments. All were immediately rejected. Reuters points to three anomalies in the payment requests, all 35 of the messages lacked the names of "correspondent banks" – the necessary next step in the payment chain... That fault meant the orders could not immediately be fulfilled. Second, most of the payments were to individuals rather than institutions.

And third, the slew of payments that morning was out of whack with the usual pattern of orders from Bangladesh Bank. Over the eight months to January 2016, Bangladesh Bank had issued 285 payment instructions to the Fed, averaging fewer than two per working day (Das Spicer, 2016, Section – The Hack, para. 7-8).

The hackers adapted by reformatting the payment requests properly and resubmitting all 35 requests. The unauthorized payment requests were then communicated via SWIFT to the Bank of Bangladesh's account at The Federal Reserve. While the Fed primarily serves U.S. financial institutions, it also facilitates payments for other central banks, such as the Bank of Bangladesh. The Federal Reserve System fulfills payments through Fedwire as its preferred network. Had the hackers directed their illicit payments to banks within the Fedwire system, the payments would have been executed immediately. But the hackers had not opened accounts with banks connected to Fedwire, so the Federal Reserve System sought to fulfill the payments via correspondent banks using payment networks other than Fedwire.

Five payments were made from the Bank's accounts with the Federal Reserve in New York to organizations in the Philippines and Sri Lanka. Fortunately, a quick-thinking bank clerk in the Sri Lankan bank held $20 million from being transferred (Quadir, 2016, para. 4). He thought it a very large amount to go to the bank's customer, an agricultural non-government organization (NGO). The Fed itself held up transferring the bulk of

the payments, $850 million, because of a lucky break, the losses could have been much higher had the name Jupiter not formed part of the address of a Philippines bank where the hackers sought to send hundreds of millions of dollars more. By chance, Jupiter was also the name of an oil tanker and a shipping company under United States' sanctions against Iran. That sanctions listing triggered concerns at the New York Fed and spurred it to scrutinize the fake payment orders more closely, a Reuter's examination of the incident has found. It was a "total fluke" that the New York Fed did not pay out... (Das Spicer, 2016, para. 3). This attack was directed through SWIFT, not Fedwire, but there seems little reason it could not have been. If the hackers had expertise in international bank payments comparable to their hacking skills, they would have selected accounts in banks that are part of the Fedwire network but outside the United States. Even delivering the payment requests via SWIFT would likely have led to actual payments being made with Fedwire with this approach, because Fedwire is the Fed's preferred payment method to settle accounts with Federal Reserve member organizations.

To date, only about 20% of the $81 million in stolen payments has been recovered. The hackers quickly transferred funds to casinos in the Philippines and then withdrew the funds in cash. Philippine authorities describe the casinos as having "no controls, none whatsoever" (Hammer, 2018). Subsequent investigation has led to the belief the hackers were agents of the government of North Korea (Groll, 2017, para. 1). A similar theft of payments was reported having occurred against Ecuadoran firm Banco del Austro in 2015. These two incidents represent the first known successful cyber-attacks against wholesale payment systems (Gimbert Hunter, 2018, para. 1, 3).

9. CONCLUSIONS

Hackers nearly got away with stealing $1 billion from the Bank of Bangladesh's Federal Reserve account. That is a lot of incentive for future attacks on wholesale payment systems in general – and the Federal Reserve in particular. Fedwire is a very high-value target, and there can be little doubt that it will face future hacking attempts. Given the high value of daily payments processed by the Fedwire network, it is safe to speculate that financial gain from stolen payments will be the primary motive of the hacking community, including nation-states.

We can also envision unintended consequences from successful hacking. A $1 billion payment theft against a single Fedwire customer could shake confidence in wholesale payments for the entire Federal Reserve member community. This could lead to a type of contagion – the temporary loss of confidence in Fedwire itself. Given the rapid recovery of Fedwire after 9/11, it is doubtful even this would do more than slow payments down to a crawl for a few days. However, even a moderate reduction in the liquidity Fedwire provides could have a measurable impact on the American economy. Payments in Fedwire are exceptionally large in aggregate. Congresswoman Carolyn B. Maloney, a senior member of the House Financial Services Committee, said of the attack on the Bank of Bangladesh and the Fed, "What struck me the most was that this action struck at trust in the international banking system, and if you can't trust international banking, then international commerce could grind to a halt" (Hammer, 2018). A corollary to representative Mahoney's logic is clear: if you can't trust Fedwire, you can't trust the Fed. The efficiency of American commerce depends on that trust.

REFERENCES

[1] Bech, Morten L., and Atalay, Enghin, (2010), The topology of the federal funds market, Physica A, volume 389, pps. 5223-5246.

[2] Beyeler, Walter E., Glass, Robert J., Bech, Morten L., and Soramaki, Kimmo, (2007), Congestion and cascades in payment systems, Physica A, pps. 693-718.

[3] Bouveret, Antione, (2018), IMF working paper - cyber risk for the financial sector: A framework for quantitative assessment, International Monetary Fund.

[4] Bureau of Economic Analysis, (2019, February 28th), Gross domestic product, fourth quarter and annual 2018 (initial estimate), https://www.bea.gov/news/2019/initial-gross-domestic-product-4th-quarter-and-annual-2018

[5] Crucciti, Paolo, Latora, Vito, Marchiori, Massimo, Rapisarda, Andrea, (2004), Error and attack tolerance of complex networks, Physica A, Volume 340, pps. 388-394.

[6] [6] Das, Krishna N., Spicer, Jonathon, (2016, July 21st), The SWIFT hack: How the New York Fed fumbled over the Bangladesh Bank cyber-heist, Reuters, https://www.reuters.com/investigates/special-report/cyber-heist-federal

[7] Federal Reserve, (2008, March 14th), Minutes of the Board of Governors of the Federal Reserve System, https://www.federalreserve.gov/other20080627a1.pdf.

[8] Federal Reserve, (2014), Fedwire Funds Services, https://www.federalreserve.gov/paymentsystems/fedfunds_coreprinciples.htm.

[9] Federal Reserve, (2017), Structure of the Federal Reserve System, https://www.federalreserve.gov/aboutthefed/structure-federal-reserve-system.htm

[10] Federal Reserve, (2019), Fedwire Funds Service—Annual, https://www.federalreserve.gov/paymentsystems/fedfunds_ann.htm.

[11] Federal Reserve Bank of St. Louis, (2019, March 29th), Deposits, all commercial banks, Federal Reserve Economic Data (FRED), St. Louis Federal Reserve Bank, https://fred.stlouisfed.org/series/DPSACBM027NBOG.

[12] Gilbert, Adam M., Hunt, Dara, and Winch, Kenneth C., (1997, July) Creating an integrated payment system: The evolution of Fedwire, Federal Reserve Bank of New York Economic Policy Review, Volume 3, Number 2. https://www.newyorkfed.org/medialibrary/media/research/epr/97v03n2/9707gilb.pdf

[13] Gimbert, Alaina, Hunter, Rob, (2018), Cyberthreats and wholesale payment systems, Bank Policy Institute – The Clearing House, https://www.theclearinghouse.org/banking-perspectives/2018/2018-q2-banking-perspectives/articles/cyberthreats-and-wholesale-payment-systems.

[14] Groll, Elias, (2017, March 21st), NSA official suggests North Korea was culprit in Bangladesh bank heist, Foreign Policy, https://foreignpolicy.com/2017/03/21/nsa-official-suggests-

north-korea-was-culprit-in-bangladesh-bank-heist/.

[15] Hammer, Joshua, (2018, May 3rd), The billion-dollar bank job, The New York Times Magazine, https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html

[16] Lewis, Ted G., (2015), Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, Second Edition, John Wiley Sons, Inc., Hoboken, New Jersey.

[17] McAndrews, James J., Potter, Simon M., (2002, November), Liquidity effects of the events of September 11, 2001. Federal Reserve Bank of New York Economic Policy Review.

[18] Mirchandani, Bhakti, (2018, August 28th), Laughing all the way to the bank: Cybercriminals targeting U.S. financial institutions, Forbes, https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#1f9f3a986e90.

[19] Quadir, Serajul, (2016, March 10th), How a hacker's typo helped stop a billion dollar bank heist, Reuters Business News, https://www.reuters.com/article/us-usa-fed-bangladesh-typo-insight-idUSKCN0WC0TC.

[20] Statistica, (2019), Gross domestic product (GDP) ranking by country 2017 (in billion U.S. dollars), https://www.statista.com/statistics/268173/countries-with-the-largest-gross-domestic-product-gdp/.

[21] The Straight Times, (2016, June 18th), Dridex malware linked to Bangladesh heist, https://www.straitstimes.com/business/dridex-malware-linked-to-bangladesh-heist.

[22] Soramaki, Kimmo, Bech, Morten L., Arnold, Jeffrey, Glass, Robert J., Beyeler, Walter E., (2007), The topology of interbank payment flows, Physica A, volume 379, pps. 317-333.

[23] Xu, Tao, He, Jianmin, Li, Shouwei, (2016), A dynamic network model for interbank market, Physica A, volume 463, pps. 131-138.

[24] Yoder, Robert M., (1951, January 20th), Someday they'll get slick Willie Sutton, The Saturday Evening Post, Volume 223, Issue 30.

