BEST PRACTICES FOR BANKS

Reducing the Risks of Large-Value Funds Transfers

(Developed by the Bankers Electronic Crimes Task Force)

INTRODUCTION

"Large-value" funds transfers (also called payments or wire transfers) are generally transactions between financial institutions. Banks process these transfers on their own behalf or for the benefit of their corporate and consumer customers. For the purposes of these Best Practices, large-value funds transfers will also be called "wire transfers." Lower value transfers occur through consumer bill payment systems and through Automated Clearing House (ACH) transfers and are not addressed in this document.

These Best Practices address steps a financial institution can take to reduce its risk of itself becoming a victim of a "Corporate Account Takeover." The focus of these Best Practices is on protecting the financial institution's account balance at its correspondent banks. Reducing the risks of a bank's customers becoming victims a Corporate Account Takeover are not addressed in this document. However, practice for reducing those risks can be found on the Conference of State Bank Supervisors' website: Corporate Account Takeover Best Practices.

BACKGROUND ON LARGE-VALUE FUNDS TRANSERS

In 2015 and 2016, a series of thefts from foreign banks occurred using compromised credentials of bank employees to gain access to the SWIFT network. One of these thefts was just under $1 billion U.S. dollars and represented roughly 40% of that bank's capital. Fortunately, most of the theft was not successful. In 2012, the FBI released a Fraud Alert [FBI Wire Fraud Alert] indicating that cyber criminals were targeting employees of small to medium size financial institutions to obtain login credentials to the correspondent bank account of their financial institution and then conducting fraudulent funds transfers. In some cases, the criminals were obtaining credentials of multiple employees so they could bypass dual control and conduct all aspects of a wire transfer. Most of the fraudulent transfers were under $1 million. The recent theft of approximately $1 billion dollars using compromised SWIFT credentials shows the significant magnitude of the fraud and the importance for all banks to review their practices for "large-value" transfers. These incidents also show that all banks, not just banks using SWIFT, are potentially vulnerable. Additionally, the persistence of adversaries to steal ever increasing amounts of money and the consequence of a theft of a large portion of a bank's capital makes it vital that financial institutions review and strengthen their wire transfer controls.

SWIFT – A MESSAGING SYSTEM

The Society for Worldwide Interbank Financial Telecommunication, or SWIFT, is a financial telecommunications messaging system for sending financial messages, such as letters of credit, payment instructions, and securities transactions instructions between member banks worldwide. SWIFT's essential function is to deliver these messages quickly and securely. SWIFT does not hold funds or transfer funds but instead sends payment orders (instructions) between institutions. The payment orders must then be settled by correspondent accounts that the institutions have with each other. SWIFT is used to transmit payment instructions for the vast majority of international interbank transactions, which can be denominated in numerous currencies.

FUNDS TRANSFER SYSTEMS

Community banks in the United States generally do not have a user account with SWIFT but instead utilize their correspondent (intermediary) banks for sending large-value payments. In the United States, there are numerous financial intermediaries (such as regional and nation-wide correspondent banks) that, unlike SWIFT, actually process or transfer funds. Although there are numerous financial intermediaries in the US, the bulk of large-value payments are processed electronically over just two networks. The first is the Fedwire® Funds Service, which is operated by the Federal Reserve Banks. The second is the Clearing House Interbank Payments System (CHIPS), which is a privately operated payments system. CHIPS is owned by financial institutions. Fedwire® is often used for transfers between U.S. based financial institutions, and CHIPS is often used for international interbank transfers.[1]

Structurally, there are two components to wire transfers: the instructions (also known as the "clearing") contain information on the sender and receiver of the funds, and the actual movement or transfer of funds (also known as the "settlement"). The instructions may be sent in a variety of ways, including by electronic access to networks operated by the Fedwire® or CHIPS payment systems; by access to financial telecommunications systems, such as SWIFT; or by e-mail, facsimile, telephone, or telex. Fedwire® and CHIPS are used to facilitate U.S. dollar transfers between two domestic endpoints or the U.S. dollar segment of international transactions.[2]

As noted above, domestic wire transfer instructions can be made through different methods, such as online using proprietary messaging systems, by phone, email, and/or mobile banking systems, depending on the service provided by the intermediary bank. The associated risks vary greatly depending on the transfer process, and the process can vary based on the transfer network being used.

[1] FFIEC IT Examination Handbook – Wholesale Payment Systems
[2] FFIEC Bank Secrecy Act / Anti-Money Laundering Examination Manual, page 207 11/17/2014 edition

BEST PRACTICES FOR BANKS

Reducing the Risks of Large-Value Funds Transfers

(Developed by the Bankers Electronic Crimes Task Force)

SUMMARY

Due to the size, complexity, and frequency of attacks against the banking industry, staying ahead of adversaries is vital. The potential for large financial loss warrants all banks to make it a top priority to review their wire transfer controls to ensure they are strong and that only authorized access is granted to the networks. Most transfers cannot be canceled once processed. Since there are a large number of intermediary banks with varying processes, and since banks vary in size and complexity, there is not a single solution. Each bank must conduct a detailed review of its processes and fully understand how it processes and authorizes large-value payments, how it can protect systems utilized to process transfers, and the controls used by any third party vendors to conduct transfers.

IDENTIFY

1) What is the bank trying to protect? (Its correspondent bank accounts and funds transfer systems.)

2) What are the primary threats against it? (Adversaries using malware to gain access to terminals and funds transfer systems.)

I1 Identify each correspondent relationships.

- Federal Reserve Banks.
- Regional and national correspondent banks.
- Federal Home Loan Banks.

I2 Identify how the bank accesses and transfer money in and out of correspondent accounts.

- On-line banking systems.
- Proprietary funds transfer systems.
- Voice calls by phone using security codes, etc.

I3 Identify (list) the funds transfer systems at the bank (include systems that are not used but present). For example:

- Fedwire®,
- FHLBAccess®,
- CHIPS,
- Any on-line banking systems used to access the accounts at correspondent banks, and
- Any wire services (such as WireXchange) provided by core processing vendors or other third parties).

I4 Identify the security features and controls of each funds transfer system at the bank.

PROTECT

Implement processes and controls to protect against malware giving adversaries access to the bank's correspondent accounts and funds transfer systems.

P1 Reduce the attack surface.

- Minimize the number of computers / terminals that can access the funds transfer systems.

P2 Restrict Internet access.

- Use dedicated computers that are not connected to the bank's network or are segmented.
- Configure funds transfers computers to prevent email access, web access (other than to the correspondent banks), and use of USB drives, unless absolutely necessary.

P3 Ensure strong cyber hygiene is practiced on computers used for wire transfers.

- Strongly consider automatic patching.
- Remove applications / software (such as Adobe Flash and Java) that are not needed by the funds transfer systems that the bank accesses.
- Remove administrative access for all employees with funds transfer capability.
- Follow all recommendations of owners / operators of wire transfer systems.
- Remove any USB tokens when wire transfers are not being processed.
- Utilize enhanced security procedures offered by the correspondent banks, such as
    - Multi-factor authentication,
    - Maximum transfer limits without secondary authentication, such as call back,
    - Out-of-band authentication for large transfers,
    - Time of day controls, when available,
    - Confirmation procedures before security features are changed / disabled, and
    - Limit the number of employees with capability to change security settings.

P4 Implement the "Foundational Cyber Hygiene" controls of the Center for Internet Security (CIS). CIS provides a list of 20 top critical security controls (CSC) that if implemented will significantly reduce cyber risks. The first five critical security controls listed below are referred to as "Foundational Cyber Hygiene" and can reduce cyber risk by 85%. Each of the five controls requires implementation of several underlying measures. All institutions should implement these industry recognized essential controls. Refer to the Center for Internet Security for more information.

- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized software

- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges

Cyber defense must be driven by prioritization. Each bank will have to determine what it should do first to get the most value and protection.

P5 Ensure Remote Desktop Protocol (RDP) is disabled: Remote desktop software allows individuals not physically at the keyboard to access a computer over a network or the Internet. This is very useful in terms of remote servicing of the computer by an authorized technician but can also be exploited by hackers to take complete control of the computer and to compromise data. To check if RDP is enabled, consult the Operating System User's Guide as operating systems vary.

P6 Implement or strengthen cyber education for wire transfer personnel by:

- Providing frequent training on spear phishing,
- Keeping wire personnel updated on the cyber threat landscape,
- Ensuring wire employees know how to create strong passwords,
- Ensuring employees know to only access correspondent accounts and wire transfer systems from bank devices,
- Regularly reviewing outside resources to receive information regarding new threats,
- Changing or strengthening training methods – videos, in-person, on-line,
- Urging wire transfer personnel not to post their job function to social media,
- Keeping wire personnel vigilant by routinely testing their awareness of phishing emails, and
- Reviewing access lists to ensure that employees with wire transfer capability still have a need for their access level and that they don't have administrative access.

P7 Ensure that operating and security manuals for all funds transfer systems are not stored on machines used for funds transfer. Consider storing them on removable media.

P8 Consider having frequent audits of the wire transfer function.

DETECT

Develop and implement appropriate monitoring activities to identify unusual activity before it occurs.

D1 Educate bank employees of warning signs and red flags that fraud may be in progress.

- Bank employees should review all foreign wires with scrutiny.
- Consider implementing a limit that requires a higher level of risk review.
- Share new wire schemes.
- Remind employees that misspellings can sometimes be a red flag.
- Urgency can sometimes be a red flag - so remind employees to escalate when in doubt.

D2 Establish automated or manual monitoring systems.

- System & Activity Trend Analysis- Data Driven Analytics. Know what activity is an anomaly going across the systems.
- An automated system could be as simple as an excel file with all customer history and utilizing the find search.
- Review systems and logs that monitor malware.
- Be suspicious of requests for secrecy or urgency.

D3 The first notification of a problem might be a simple inquiry from another bank about a transfer they are processing / receiving. Be sure that personnel recognize such inquiries as potential red flags. Based on the size of a transfer (or combined with related transfers or other transfers occurring about the same time), train employees to inform the wire department supervisor, so a review can be made.

RESPOND

Respond to an incident immediately to increase the chance of recovering the money.

Rd1 Activate the incident response plans that include large-value funds transfers scenarios. Ensure the plan's emergency contact names and contact information is current, and leverage your state's *FS-ISAC 2017 Incident Response Playbook*. Establish a relationship with key contacts prior to an incident.

Rd2 Immediately verify if a suspicious transaction is fraudulent.

Rd3 Utilize ALL relevant resources for recovering funds (law enforcement, receiving bank, correspondent or intermediary banks, Fedwire messages), and be proactive if timely updates are not received. (The US Secret Service and/or FBI might have personnel stationed in the foreign city.)

Rd4 Immediately attempt to reverse all suspected fraudulent transactions.

Rd5 Immediately notify the receiving bank of the fraudulent transactions, and ask the bank to hold or return the funds:

- MAKE SURE TO SPEAK TO THE FRAUD DEPARTMENT FIRST, and if the institutions does not have a fraud department, ask for the wire department.
- If an intermediary / correspondent bank is not being cooperative in holding the funds, ask your local US Secret Service or FBI agents to request that the funds be held. It is rare for a bank not to hold the funds when a federal law enforcement agency notifies them the request is part of a fraud investigation.
- Some international banks may be difficult to contact due to language barriers or lack of available contact information. Often correspondent and intermediary bank fraud teams can assist in contacting receiving banks in the case of fraud. Additionally, phone conference calling language translation services (such as those used by hospitals) are available. Identify those in advance.
- For international wires, identify relevant time zones, so that the receiving bank can be contacted as soon as they open. This may require arranging to have personnel call during your non-business hours.

Rd6 Simultaneously while attempting to recover funds, have other personnel take the compromised wire transfer system off line and contact the appropriate correspondent bank(s) by phone and notify them to implement enhanced authentication or to discontinue processing wire requests from your account.

Rd7 Strongly consider using out-of-band communication with correspondents (both for discussions and to review recent transactions) until the depth of the compromise is determined.

Rd8 Consider hiring a forensic team to evaluate the bank's system before it goes back on-line. Have a forensic team identified in advance within the incident response plan. Consider having the team on-retainer so terms are not being negotiated during a crisis.

Rd9 Implement procedures for customer relations if a customer account was impacted by the theft and document the recovery efforts.

Rd10 Ensure the bank's Incident Response and Business Continuity Plans include recovery steps for cybersecurity incidents, as well as where the bank's backup systems are located and how they are protected from malware. These may need to be restored before further processing can take place.

Rd11 Report fraud to FINCEN, and file a Suspicious Activity Report (SAR).

Rd12 Contact your bank's state and federal banking regulators, your insurance carriers, and inform legal counsel.

RECOVER

Continue to attempt to recover the money until all responsible efforts have been exhausted.

Rr1 Restore affected wire transfer system from last known good backup.
If systems / data must be restored, it is important they are restored using a good backup unaffected by malware.

- Document how it will be determined which backup is unaffected.

Rr2 Confirm and test that the wire system has been properly restored. Notify correspondent bank(s) when they can resume processing wires from the bank's account.

- Document the process for testing and restoring the system(s).

Be aware that due to inter-connective risk, correspondent bank(s) may not allow the bank to reconnect / use their wire transfer network until they have some level of assurance that it is safe for them and their other customer banks. They may require documentation validating this assurance.

Rr3 Discuss lessons learned in order to update policies, procedures, and incident response plans and to close any other gaps that may exist.

ADDITIONAL RESOURCES

FS-ISAC Members' Portal

Link to paper issued in 2016 in response to the account take over attacks leveraging the SWIFT network.
https://www.fsisac.com/sites/default/files/news/Security%20of%20Payment%20Network%20Access%20Points%20June%2030%202016%20Final%20%28004%29.pdf