Recommendations for ACH Network Participants: Lessons Learned for Proactive Risk Management Following Attacks on the SWIFT Network

Sept. 8, 2016

Introduction: Cyber Events Leveraging the SWIFT Network

Recent cyber incidents involving the Society for Worldwide Interbank Financial Telecommunication (SWIFT) payment messaging network have been the focus of media attention due to the international nature and magnitude of the attacks. However, these incidents did not attack or breach the SWIFT network itself, but instead were the result of compromises in network access points which allowed for unauthorized entry into financial institution systems.

In each of the SWIFT-related incidents, the schemes involved phishing, the theft of legitimate bank employee credentials, and sub-optimal infrastructure management (e.g., lack of firewalls, inexpensive routers, and the use of weak and static passwords) to ultimately gain access to financial institution systems. In fact, these incidents follow more traditional Account Takeover (ATO) tactics experienced in recent years whereby intruders initiate fraudulent transfers through back-offices, PCs, or workstations connected to financial institution or network interfaces.

It is important to note that while these attacks were targeted and sophisticated, they allegedly combined known attack tactics such as phishing to steal legitimate credentials and provide attackers the ability to initiate fraudulent transfers. As a result of these recent events, SWIFT is working with network participants to implement appropriate security practices and controls to defend against these types of attack tactics.

Managing the Risk of Account Takeover in the ACH Network

There is a regulatory expectation that financial institutions conduct ongoing risk assessments that include a consideration of new and evolving threats. Cyber-attacks are part of the threat landscape, and financial institutions should be including attacks like the SWIFT attack as part of their risk assessment, and proactively working to mitigate that risk. As previously noted, this type of attack is not a direct attack against core systems or networks, but is instead an exploit against poor basic security practices and human error, including personnel not following basic security practices. Financial institutions should proactively apply knowledge of this type of threat as it relates to not only their customers, but as it may relate to interbank networks (including the ACH) and other access points including core processors, correspondent banks, and vendors.

Accordingly, it is important that financial institutions assess the effectiveness of risk controls in ACH activities to mitigate the risk of unauthorized access, and adopt best practices regarding cyber hygiene

and operational risk. This includes reviewing connectivity with ACH Operators with regard to both primary and back-up lines, ensuring that personnel have the appropriate entitlements and authorization to interact with the ACH Operator, and requiring dual controls for payment file initiation. Increasing sophistication of social engineering techniques can challenge systems without recommended redundancies and safeguards in place, so good cyber hygiene is necessary.

"Corporate Account Takeover Can Lead to Fraudulent Transactions"

NACHA's Operations Bulletin dated December 2, 2009, titled "Corporate Account Takeover Can Lead to Fraudulent Transactions," provides guidance for financial institutions on steps that they and their business customers each can take to reduce their respective vulnerabilities to account takeover. While the techniques used to access end-points grow more sophisticated in nature (e.g., advanced malware and more sophisticated social engineering) the basic underlying schemes for attacking corporates or financial institutions in order to gain access to the ACH Network remain unchanged and best addressed through traditional security and control practices. NACHA's Operations Bulletin summarizes what financial institutions and their business customers can do to mitigate the risk of account takeover.

Risk Management Recommendations

In light of recent industry cyber-attack events, the FFIEC provided a joint response to remind financial institutions to actively manage cyber-related risks, noting that there is no change in regulatory expectations. Financial institutions should review risk management for critical network systems, including the ACH Network, for secure processes for authentication, authorization, fraud detection, and response management.

Each financial institution should develop an assessment of its own risk profile with regard to Account Takeover and employ an effective security plan commensurate with that risk. Examples of sound business practices for financial institutions include:

- Maintaining cyber threat awareness through information sharing and keeping cyber risk assessments up to date;
- Employing a layered defense IT environment utilizing redundant controls;
- Deploying and maintaining strong access controls and operating procedures to manage the security of payment networks and systems;
- Ensuring a secure operating environment by implementing appropriate physical and logical security to protect the access control features, software, computers and any associated equipment that are used to exchange data with the ACH Operator. Updating all applicable workstation operating systems, anti-malware software and any other software used in connection with or comprising the institution's electronic connections;
- Ensuring that personnel have the appropriate entitlements, authorization, and authentication to interact with the ACH Operator;
- Ensuring the FI has an understanding of its obligations with respect to their ACH Operators in the event of an incident;

- Evaluating the risk in all access points, including its customers, correspondents, core processors and ACH Operators;
- Employing dual controls for payment file initiation;
- Being particularly vigilant in advance of holidays and long weekends in monitoring operations for anomalies, and reporting immediately to ACH Operators if detected;
- Enhancing event information sharing on a cross- department level within the financial institution; and
- Participating in information sharing forums such as FS-ISAC.

Additional Resources

- SWIFT Communications - https://www.swift.com/insights/press-releases/swift-customer-communication_customer-security-issues
- FFIEC Resources:
  http://www.ffiec.gov/press/PDF/Cybersecurity_of_IMWPN.pdf
  http://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf
- NACHA Operations Bulletin - https://www.nacha.org/system/files/resources/NACHA_Operations_Bulletin_-_Corporate_Account_Takeover_-_December_2_2009.pdf
- FS-ISAC Joint Statement - http://www.fsisac.com/sites/default/files/news/Security%20of%20Payment%20Network%20Access%20Points%20June%2030%202016%20Final%20%28004%29.pdf