Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • http://www.ffiec.gov

Joint Statement

Cybersecurity of Interbank Messaging and Wholesale Payment Networks

PURPOSE

The Federal Financial Institutions Examination Council (FFIEC), on behalf of its members,[1] is issuing this statement, in light of recent cyber attacks, to remind financial institutions of the need to actively manage the risks associated with interbank messaging and wholesale payment networks. Financial institutions should review their risk management practices and controls over information technology (IT) and wholesale payment systems networks, including authentication, authorization, fraud detection, and response management systems and processes. The FFIEC members emphasize that participants in interbank messaging and wholesale payment networks should conduct ongoing assessments of their ability to mitigate risks related to information security, business continuity, and third-party provider management.

This statement does not contain new regulatory expectations. It is intended to alert financial institutions to specific risk mitigation techniques related to cyber attacks exploiting vulnerabilities and unauthorized entry through trusted client terminals running messaging and payment networks. Financial institutions should review their risk management practices (including services provided to clients) and refer to the appropriate *FFIEC IT Examination Handbook* booklets referenced in this statement for information on regulatory expectations regarding IT risk management. Financial institutions should also review and adhere to the technical guidance issued by payments and settlement networks for managing and controlling risks to critical systems.

BACKGROUND

Recent cyber attacks against interbank networks and wholesale payment systems to commit fraud have demonstrated capability to:

- Compromise a financial institution's wholesale payment origination environment, bypassing information security controls.
- Obtain and use valid operator credentials with the authority to create, approve, and submit messages.
- Employ sophisticated understanding of funds transfer operations and

[1] The FFIEC comprises the principals of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.

operational controls.
- Use highly customized malware to disable security logging and reporting, as well as other operational controls to conceal and delay detection of fraudulent transactions.
- Transfer stolen funds across multiple jurisdictions quickly to avoid recovery.

RISKS

Unauthorized transactions involving interbank messaging and wholesale payment networks may subject the originating bank to financial loss and compliance risk.[2]

RISK MITIGATION

Financial institutions should use multiple layers of security controls to establish several lines of defense. Financial institutions should also ensure that their risk management processes address the risk posed by compromised credentials. In taking these actions, financial institutions should reference the risk management information contained in the *FFIEC IT Examination Handbook*,[3] specifically the *Information Security*,[4] *Business Continuity Planning*,[5] *Outsourcing Technology Services*,[6] and the *Wholesale Payment Systems*[7] booklets. Additionally, institutions should consult their payment system provider's guidance for specific security control recommendations.

In accordance with regulatory requirements and FFIEC guidance, a financial institution should consider the following steps:

- **Conduct ongoing information security risk assessments.** Maintain an ongoing information security risk assessment program that considers new and evolving threat intelligence related to online accounts and adjust customer authentication, layered security, and other controls in response to identified risks. Identify, prioritize, and assess the risk to critical systems, including threats to applications that control various system parameters and other security and fraud prevention measures. In addition, ensure that third-party service providers:
  - Perform effective risk management and implement appropriate controls.
  - Properly maintain and conduct regular testing of their security controls simulating potential risk scenarios.
  - Are contractually obligated to provide security incident reports when issues arise that may affect the institution.

- **Perform security monitoring, prevention, and risk mitigation.** Ensure protection and detection systems, such as intrusion detection systems and antivirus protection, are up-to-date and firewall rules are configured properly and reviewed periodically. Establish a baseline environment to enable the ability to detect anomalous behavior. Monitor system alerts to identify, prevent, and contain attack attempts from all sources. In addition,

[2] e.g. U.S.A. PATRIOT Act, Bank Secrecy Act, Office of Foreign Assets Control (OFAC)
[3] See: http://ithandbook.ffiec.gov/
[4] See: http://ithandbook.ffiec.gov/it-booklets/information-security.aspx
[5] See: http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx
[6] See: http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx
[7] See: http://ithandbook.ffiec.gov/it-booklets/wholesale-payment-systems.aspx

- Follow software assurance industry practices for internally developed applications.
- Conduct due diligence of third-party software and services.
- Conduct penetration testing and vulnerability scans, as necessary.
- Promptly manage vulnerabilities, based on risk, and track mitigation progress, including implementing patches for all applications, services, and systems.
- Review reports generated from monitoring systems and third parties for unusual behavior.

- **Protect against unauthorized access**. Limit the number of credentials with elevated privileges across the institution, especially administrator accounts, and the ability to easily assign elevated privileges to access critical systems. Review access rights periodically to confirm approvals are still appropriate to the job function. Establish stringent expiration periods for unused credentials, monitor logs for use of old credentials, and promptly terminate unused or unwarranted credentials. Establish authentication rules, such as time-of-day and geolocation controls, or implement multifactor authentication protocols for web-based control panels. In addition,
  - Conduct regular audits to review the access and permission levels to critical systems for employees and contractors. Implement least privileges access policies across the entire enterprise. In particular, do not allow users to have local administrator rights on workstations.
  - Change default password and settings for system-based credentials.
  - Prevent unpatched systems, such as home computers and personal mobile devices from connecting to internal-facing systems.
  - Implement monitoring controls to detect unauthorized devices connected to internal networks.
  - Use secure connections when remotely accessing systems and services (e.g., virtual private networks).

- **Implement and test controls around critical systems regularly.** Ensure appropriate controls, such as access control, segregation of duties, audit, and fraud detection and monitoring systems, are implemented for systems based on risk. Limit the number of sign-on attempts for critical systems and lock accounts once such thresholds are exceeded. Implement alert systems to notify employees when baseline controls are changed on critical systems. Test the effectiveness and adequacy of controls periodically. Report test results to senior management and, if appropriate, to the board of directors or a committee of the board of directors. Include in the report recommended risk mitigation strategies and progress to remediate findings. In addition,
  - Encrypt sensitive data on internal- and external-facing systems in transit and, where appropriate, at rest.
  - Implement an adequate password policy.
  - Review the business processes around password recovery.
  - Regularly test security controls, such as web application firewalls.
  - Implement procedures for the destruction and disposal of media containing sensitive information based on risk relative to the sensitivity of the information and the type of media used to store the information.
  - Filter Internet access through Web site whitelisting where appropriate to limit employees' access to only those Web sites necessary to perform their job functions.
  - Conduct incremental and full backups of important files and store the backed-up data offline.

- **Manage business continuity risk.** Validate that business continuity planning supports the institution's ability to quickly recover and maintain payment processing operations. In addition,
    - Coordinate business continuity development and testing with all applicable third parties.
    - Coordinate testing with other industry players.

- **Enhance information security awareness and training programs.** Conduct regular, mandatory information security awareness training across the financial institution, including how to identify and prevent successful phishing attempts. Ensure training reflects the functions performed by employees.

- **Participate in industry information-sharing forums.** Incorporate information sharing with other financial institutions and service providers into risk mitigation strategies to identify, respond to, and mitigate cybersecurity threats and incidents. Since threats and tactics can change rapidly, participating in information-sharing organizations, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), can improve an institution's ability to identify attack tactics and to successfully mitigate cyber attacks involving destructive malware on its systems. In addition to the FS-ISAC, there are government resources such as the U.S. Computer Emergency Readiness Team (US-CERT) that provide information on vulnerabilities. The US-CERT portal may be found at www.us-cert.gov.

ADDITIONAL RESOURCES

The following are available payment systems risk management resources with practical information.

- FFIEC Joint Statement on Compromised Credentials. https://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf
- FFIEC Joint Statement on Destructive Malware. https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf
- FFIEC Joint Statement on Cybersecurity Threat and Vulnerability Monitoring and Sharing. https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf
- "SWIFT Security Issues Update – New information." SWIFT: May 13, 2016. https://www.swift.com/insights/press-releases/swift-customer-communication_customer-security-issues
- "SWIFT customer communication: Cooperating on cyber-security." SWIFT: May 20, 2016. https://www.swift.com/insights/press-releases/swift-customer-communication_cooperating-on-cyber-security
- Committee on Payments and Market Infrastructures, Cyber resilience in financial market infrastructures. http://www.bis.org/cpmi/publ/d122.pdf
- Federal Reserve Banks Operating Circular No. 5 ELECTRONIC ACCESS Effective June 30, 2016. https://frbservices.org/files/regulations/pdf/operating_circular_5_06302016.pdf

REFERENCES

FFIEC Information Technology Examination Handbook, "Wholesale Payment Systems" *http://ithandbook.ffiec.gov/it-booklets/wholesale-payment-systems.aspx*

FFIEC Information Technology Examination Handbook, "Business Continuity Planning"
http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

FFIEC Information Technology Examination Handbook, "Information Security"
http://ithandbook.ffiec.gov/it-booklets/information-security.aspx

FFIEC Information Technology Examination Handbook, "Outsourcing Technology Services"
http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx