THE FEDERAL RESERVE
FedLine® Solutions

FedLine® Solutions Security and Resiliency Assurance Program participant expectations

This document outlines the high-level steps that your organization must take to complete the Security and Resiliency Assurance Program ("Assurance Program"). **Your organization must complete the program by December 31, 2021.** All End User Authorization Contacts (EUACs) at your organization will receive Assurance Program communications.

Plan and prepare

- Identify a primary EUAC. This individual will:
  - Coordinate the assessment, including the submission of your organization's attestation which indicates the completion of the program.
- Identify a senior management official within your organization who will electronically attest that the assessment was conducted. This individual should be an official or executive officer in charge of electronic payments operations or payments security for the organization. In some cases the signer may also be the primary EUAC.
- Add the following domains to your organization's safe senders list: @echosign.com and @adobesign.com

Get started

- Review all applicable documentation sent to you from the domains above, including the program guide and the attestation letter.
- Based on the instructions provided in the communications, determine if your organization is required to conduct an independent review to complete the assessment. If this is required for your organization, refer to Appendix A within the program guide.

Conduct the assessment

- Conduct the assessment using the program guide for guidance.

Review the assessment results

- Review the assessment results with the senior management contact who will sign the attestation letter to ensure he/she is prepared to submit their electronic signature.

Submit the attestation

- Access the attestation letter and submission instructions from the email that was sent from the domains mentioned above.
- If necessary, "delegate" the information to the individual who will sign the attestation letter.
- Notify the signer when it is time to fill in the applicable information and then click "submit" to electronically sign the attestation.

Complete

- Thank you for completing the program!

If you have questions throughout the process, call the Customer Contact Center (CCC) at (888) 333-7010. As a reminder, your account executive is also available to assist you. To find a list of Federal Reserve Bank contacts specific to your organization, use the Find Your Contacts tool.

THE FEDERAL RESERVE
FedLine® Solutions

FedLine® Solutions Security and Resiliency Assurance Program Guide

August 2020

Contents

Overview

The Federal Reserve Banks' FedLine® Solutions are a critical component of the U.S. electronic payments system and provide access to FedACH® Services, Fedwire® Services, FedCash® Services and other electronic payment and information solutions. While FedLine Solutions benefit from numerous embedded security features, institutions and their service providers with access to these solutions ("Organizations") play a vital role in safeguarding the endpoints that are used to interact with the Federal Reserve Banks. Accordingly, the Federal Reserve Banks require Organizations to comply with Federal Reserve Bank policies, procedures and security controls ("Security Requirements").

As a part of the Security Requirements, each Organization must also exercise its own independent judgment about security and resiliency, and take all commercially reasonable measures necessary to prevent fraud, unauthorized access, other unauthorized use or disruption to the operations of any FedLine Solution.

Program purpose

The expansion of cyber threats and attacks on payment networks and systems necessitates a holistic approach to endpoint risk management across all financial industry stakeholders. Given the evolving threat landscape, the Federal Reserve Banks are implementing the FedLine Solutions Security and Resiliency Assurance Program ("Assurance Program") described in this guide.

The Assurance Program requires that Organizations:

- Conduct a self-assessment of their compliance with the Security Requirements.
- If required by the Federal Reserve Banks, ensure that the assessment is conducted or reviewed by an independent internal function or third party.
- Attest to the Federal Reserve Banks that the self-assessment was completed.
- To the extent any deficiencies or gaps were identified in the self-assessment, develop a remediation plan to address such deficiencies.

Some financial institutions may have elected to outsource some or all of their payment or electronic connections to a third-party service provider. Although the use of third-party agents is permitted, these outsourcing arrangements do not transfer an Organization's obligations or responsibility for complying with required security measures and controls.

Program benefits

The Assurance Program is designed to:

- Reinforce the safety, security, resiliency and trust of the Federal Reserve Banks' services for all financial institutions and service providers.
- Reduce the risk of fraudulent transactions and promote executive-level awareness of any gaps or control deficiencies within an Organization.
- Enhance an Organization's risk management and resiliency focus to help ensure endpoint environments are secure and resilient.
- Increase confidence that controls are in place and being monitored to protect payment systems and customers.
- Enhance an Organization's vigilance against cyber-attacks and foster discussions and planning to address key risks and develop timely remediation plans for any non-compliance or deficiencies.

Organization responsibilities

By accessing services or applications from the Federal Reserve Banks or by sending data to or receiving data from the Federal Reserve Banks, directly or through a service provider, an Organization agrees to the Security Requirements applicable to the electronic communication facility that the Organization uses. An Organization must periodically conduct reviews to confirm its compliance with the Security Requirements, consisting of the applicable Federal Reserve Bank policies, procedures and security controls, as well as any other security measures an Organization considers appropriate to prevent fraud or other unauthorized access to any FedLine Solution.

The Assurance Program engages your Organization's senior management in the FedLine security review process in order to encourage holistic risk management practices and risk-based decision making. As noted above, under the Assurance Program, your Organization must:

- Conduct a self-assessment of its compliance with the Security Requirements.
- If required by the Federal Reserve Banks, ensure that the assessment is conducted or reviewed by an independent internal function or third party.
- Attest to the Federal Reserve Banks that the self-assessment was completed.
- To the extent any deficiencies or gaps were identified in the self-assessment, develop a remediation plan to address such deficiencies.

Your assessment may be completed by your internal staff; however, some Organizations may be required to obtain an independent review of their assessment. These organizations should refer to Appendix A for additional instructions. The individual(s) conducting the assessment should have demonstrated experience in cybersecurity and auditing of payment systems.

Your Organization is ***not*** required to submit the results of your risk assessment to the Federal Reserve Banks as part of the attestation process. However, your Organization is responsible for retaining its assessment and related artifacts in accordance with your internal record retention policy. These may support your internal compliance and remediation efforts and may facilitate engagements with external auditors or regulatory agencies.

To assist your Organization in performing a periodic assessment against the Security Requirements, the following section highlights key reference materials that describe the security measures in greater detail.

Supporting documentation

FedLine Solutions Security Requirements

FedLine Security Requirements are documented in Operating Circular 5 (Electronic Access), the *Certification Practice Statements*, the *Password Practice Statement,* and the *Security and Control Procedures* document that is associated with each FedLine Solution.

Operating Circular 5 – Electronic Access

Operating Circular 5 sets forth the general terms under which an Organization may access services and applications provided by the Federal Reserve Banks over an electronic connection. The Certification Practice Statement and the Password Practice Statement describe supplemental procedures and requirements surrounding digital credentials used to access Federal Reserve Bank services and applications. All of these documents can be found on FRBservices.org® on the Operating Circulars page.

FedLine Security and Control Procedures

FedLine Security and Control Procedures contain detailed security requirements and are part of the FedLine documentation provided to your Organization during the FedLine implementation process. These documents are available to your Organization's End User Authorization Contacts (EUACs).

The FedLine Web® and FedLine Advantage® Security and Control Procedures documents are available in the EUAC Center, which is accessible via FedLine Home. FedLine Web EUACs have access to the *FedLine Web Security and Control Procedures*, and FedLine Advantage EUACs have access to both the *FedLine Web Security and Control Procedures* and the *FedLine Advantage Security and Control Procedures* documents.

The FedLine Command® and FedLine Direct® Security and Control Procedures are contained in Section Orange of the *FedLine Command Security and Implementation Guide* and the *FedLine Direct Security and Implementation Guide*, respectively, which are provided to FedLine Command and FedLine Direct EUACs via encrypted, password-protected email.

Please contact the Customer Contact Center if you need copies of these documents.

The Security and Control Procedures for each FedLine Solution contain security controls that are relevant for the specific FedLine Solution. Key controls include:

- **PC Controls** (FedLine Web and FedLine Advantage only) – requirements related to PCs that Organizations use to access FedLine Web and FedLine Advantage.
- **Hardware Controls** – requirements related to VPN devices that are used to access FedLine Advantage and FedLine Command, or Dedicated WAN routers that are used to access FedLine Advantage, FedLine Command and FedLine Direct.
- **Middleware Controls** (FedLine Command and FedLine Direct only) – requirements related to middleware software used for the FedLine Command and FedLine Direct Solutions and the servers that the software is installed on.
- **Network Controls** – requirements related to the network connections that include elements of a FedLine Solution implementation and an Organization's network.
- **Operational Controls** – requirements related to an Organization's operation of its FedLine Solution.
- **Documentation and Data** – requirements for the handling of confidential FedLine documentation and connection and configuration data.
- **Assurance** – requirements for review of compliance with security controls and correction of variances.

Organizations must review the Security and Control Procedures for all of the FedLine Solutions that they utilize.

Additional tools such as general awareness articles, emails and other FedLine documentation (e.g., Subscriber guides, contingency guides, etc.) are available to remind Organizations of their obligations.

Attestation

Organizations are required to attest that they have completed an assessment by submitting an attestation to the Federal Reserve Banks. The substantive provisions of the required attestation are provided in Appendix B.

The Federal Reserve Banks will leverage an electronic workflow and signature solution to support the attestation process. The required attestation template workflow instructions will be electronically provided to your Organization's EUACs. The attestation must be signed by a senior management official or executive officer in charge of electronic payments operations or payments security for your Organization.

The electronically signed attestation response is the only document that will be required to be submitted to the Federal Reserve Banks.

Appendix A – Instructions for Independent Assessment

Your Organization will be notified if an independent assessment is required. For those Organizations, the requirement of independence can be satisfied by having:

- An independent third party, such as an external audit firm or security consultant, perform the assessment.
- An independent internal department/function perform the assessment, such as an internal audit or compliance department (i.e., a function that is not in the reporting line of the senior executive in charge of payment services).
- If the assessment was conducted by a non-independent party or function, an independent third party must review the work conducted in connection with the assessment to establish that it was designed and conducted in a manner reasonably sufficient to identify any material noncompliance with the Security Requirements.

As part of your attestation, your Organization will be required to provide details about which of the above approaches was used, including information about who performed the independent assessment or review, the date the assessment or review was concluded, and contact information. The attestation template that you will receive will include fields to capture this information.

Evidence of work performed or independent opinions need not be submitted to the Federal Reserve Banks, but should be maintained according to the Organization's record retention policy.

Appendix B – Attestation Provisions

The attestation you will be required to submit (we will provide you with a form) will include the following substantive provisions:

1. We understand the Institution's responsibility to adhere to the security policies, procedures, and requirements set forth in Operating Circular 5, *Electronic Access*, and its Appendix A, including those for the Institution's use of FedLine Solutions and associated electronic connections used to access Federal Reserve Bank services or applications.
2. We confirm that the Institution has conducted a self-assessment of its compliance with the security policies, procedures, and requirements identified in item 1 (the "Self-Assessment"). The Institution calibrated its Self-Assessment based on its view of the risks it faces with respect to complying with such policies, procedures, and requirements.
3. [For Organizations notified that the Self-Assessment must be conducted by an independent party: We further confirm that the Self-Assessment was either (i) conducted by an independent third party, (ii) conducted by an independent internal function such as internal audit or compliance, or (iii) to the extent the Self-Assessment was conducted by a non-independent party or function, an independent third party reviewed the work conducted in connection with the Self-Assessment to establish that it was designed and conducted in a manner reasonably sufficient to identify any material noncompliance with the security policies, procedures, and requirements identified in item 1.]
4. [Not applicable to third party service providers] To the extent the Institution uses a third party service provider or other agent with respect to an electronic connection used to access Federal Reserve Bank services or applications, we understand that the Institution is responsible for that service provider's or other agent's compliance with the security policies, procedures, and requirements identified in item 1.
5. The Institution has remediation plans in place, including appropriate procedures to escalate concerns to the appropriate leaders within the Institution, to promptly address any areas of noncompliance with the security policies, procedures, and requirements identified in item 1.
6. We understand that the Institution or its service provider or other agent must immediately notify the Federal Reserve Banks' Customer Contact Center by telephone at (888) 333-7010 of any suspected or confirmed fraud, infringement, or security breach relating to any electronic connection and must promptly confirm that notification in writing.
7. The Institution shall maintain in its records (1) the Self-Assessment; (2) appropriate documentation supporting the results of the Self-Assessment; and (3) a copy of the electronically signed attestation letter.

Date:

To: The Federal Reserve Banks

Re: Attestation Regarding Performance of Self-Assessment of Compliance with Security Requirements

The undersigned officer, based on his or her knowledge, makes the following attestations as of the date above on behalf of APPLE BANK FOR SAVINGS ("Institution"):

1. We understand the Institution's responsibility to adhere to the security policies, procedures, and requirements set forth in Operating Circular 5, *Electronic Access*, and its Appendix A, including those for the Institution's use of FedLine® Solutions and associated electronic connections used to access Federal Reserve Bank services or applications.

2. We confirm that the Institution has conducted a self-assessment of its compliance with the security policies, procedures, and requirements identified in item 1 (the "Self-Assessment"). The Institution calibrated its Self-Assessment based on its view of the risks it faces with respect to complying with such policies, procedures, and requirements.

3. We further confirm that the Self-Assessment was either (i) conducted by an independent third party, (ii) conducted by an independent internal function such as internal audit or compliance, or (iii) to the extent the Self-Assessment was conducted by a non-independent party or function, an independent third party reviewed the work conducted in connection with the Self-Assessment to establish that it was designed and conducted in a manner reasonably sufficient to identify any material noncompliance with the security policies, procedures, and requirements identified in item 1.

4. To the extent the Institution uses a third party service provider or other agent with respect to an electronic connection used to access Federal Reserve Bank services or applications, we understand that the Institution is responsible for that service provider's or other agent's compliance with the security policies, procedures, and requirements identified in item 1.

5. The Institution has remediation plans in place, including appropriate procedures to escalate concerns to the appropriate leaders within the Institution, to promptly address any areas of noncompliance with the security policies, procedures, and requirements identified in item 1.

6. We understand that the Institution or its third party service provider or other agent must immediately notify the Federal Reserve Banks' Customer Contact Center by telephone at (888) 333-7010 of any suspected or confirmed fraud, infringement, or security breach relating to any electronic connection and must promptly confirm that notification in writing.

7. The Institution shall maintain in its records (1) the Self-Assessment; (2) appropriate documentation supporting the results of the Self-Assessment; and (3) a copy of this signed attestation letter.

☐ The attestation must be signed by a senior management official, or executive officer in charge of electronic payments operations or payments security for your Organization. Each Organization must attest to the provisions provided by Appendix B.

Signature:

Email:

Title:

Company:

Independent Assessment Information

The self-assessment was (select one): Select...

If an independent internal party (select one): Select...

If an independent third party, company name:

Independent Party Point of Contact Information:

Name:

Title:

Email: