THE FEDERAL RESERVE
FedLine® Solutions

Security and Resiliency Assurance Program Overview

Presented by:
Becca Campbell and Peter Nikoloff (Customer Relations & Support Office)

Agenda

The 3-part educational series will focus on one of the major topics outlined below:

- **Program Overview**
  1. **Assurance Program Basics** (Friday, August 13th & Wednesday, September 8th)
  2. **Conducting the Security Assessment** (Friday, August 20th & Wednesday, September 15th)
  3. **Completing the Assurance Program** (Friday, August 27th & Wednesday, September 22nd)
- **Q&A**

The primary goal of the educational webinar series is to provide an overview of the Security and Resiliency Assurance Program and provide a forum for organization's associated questions, in order to promote the completion of the Attestation Letter due by December 31, 2021.

Program Overview

The Security and Resiliency Assurance Program (hereinafter "Assurance Program") builds on already existing obligation related to compliance with FedLine® Security and Control Procedures and the assessment process. The completion of the Assurance Program confirms compliance with relevant security controls and procedures and provides for a holistic approach to risk management. As an annual initiative, the program will consistently start in the month of January and be due by end of December.

The Assurance Program encourages senior management understanding of the organization's security posture relative to the FedLine Security Controls to ensure they are adequately informed to attest to the attestation provisions.

Assurance Program Requirements:

- Conduct an assessment of your organization's compliance with the Security Requirements
- Implement appropriate risk management steps and support decision making by senior management
- To the extent any deficiencies or gaps were identified in the assessment, develop a remediation plan to address such deficiencies
- 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 assessment was completed by signing the Attestation Letter
  - Attestation Letter must be signed by a senior management official or executive officer in charge of electronic payments operations or payments security

Program Overview

Assurance 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, against growing and highly sophisticated attacks targeting payment systems and payment providers.

IMPORTANT

- **Each Institution must comply with measures, protections and requirements established by the Federal Reserve Banks, in addition to their own independent judgment about appropriate protections to prevent fraud or unauthorized access to an Electronic Connection** (*refer to Operating Circular 5 {Electronic Access}).*
- **Each 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.**

Assurance Program Basics

The Federal Reserve Banks are leveraging an electronic signature solution offered by Adobe Sign, to support the Assurance Program. Instructions on the completion workflow are included in the Assurance Program materials, accessible via a link in the Assurance Program email, sent to organization End User Authorized Contacts (EUACs) in January.

Initial Steps

As primary contact(s) for an organization, all EUACs will receive the Assurance Program communication. In order to successfully begin the process, EUACs must take the following steps:

- Ensure that the Adobe Sign domain (@adobesign.com) is added to your organization's safe senders list and locate the Assurance Program email communication.
- Identify a Primary EUAC to coordinate the assessment and attestation process.
- Closely review the Program Guide and Attestation Letter to ensure familiarity with the Assurance Program requirements.
- Determine if your organization is required to conduct an independent review.
- Identify the senior management official who will electronically sign the Attestation Letter.

If an EUAC cannot locate the annual Assurance Program email, the following steps may be taken:

- Discuss with fellow EUACs if the email can be found and shared (forward) or,
- Reach out to the Customer Contact Center at (888) 333-7010 to request the Assurance Program materials be resent *(all EUACs will receive the new Assurance Program email and the materials link will only work in the new email).*

Assurance Program Basics

Gather Supporting Documentation

The Security Requirements and supporting documentation are not part of the initial Assurance Program communication but are available to EUACs by other means. All materials are referenced on Page 4 of the Program Guide and the designated EUAC should collect the items applicable to their organization.

- **Operating Circular 5:** publicly accessible document, available on FRBServices.org®. The documents in scope are Electronic Access (PDF); Certification Practice Statements (PDF) and Password Practice Statement (PDF).
- **FedLine Web and FedLine Advantage Security and Control Procedures:** available in the EUAC Center, accessible via FedLine Home. The Security documents are restricted to EUACs with proper credentials only.
- **FedLine Command and FedLine Direct Security and Implementation Guides:** available via encrypted, password-protected email. Authorized EUACs must contact the Customer Contact Center via email to request.

Tips for Initiating the Security Assessment

- Determine a primary EUAC to coordinate the assessment and attestation on behalf of your organization
- EUACs may inform the technical team conducting the assessment and provide a package with the relevant security documentation
- Although there is one Attestation Letter for each ABA, an organization need only conduct one assessment so long as all ABA endpoints and services are included in the assessment

Conducting the Security Assessment

Conduct the Security Assessment

Once relevant documentation is gathered and an organization has established a strategy to approach the assessment, the process may be transitioned to the team conducting the assessment.

- Consider expanding the team conducting the assessment to include members of related departments where vulnerabilities could be identified.

Assessment Process and Working Papers

The purpose of the assessment is to ensure organizations are compliant with Federal Reserve Banks Security Requirements and take all commercially reasonable measures necessary to prevent fraud, unauthorized access and use, or disruption to the operations of any FedLine solution.

- The Federal Reserve Banks do not dictate the specific process or format for completing the assessment.
- It is up to the organization to calibrate its assessment based on its risk posture with respect to complying with such policies, procedures, and requirements.

Assessment Results and Next Steps

The overall goal of the assessment is to identify potential security gaps and remediate them. 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.

Conducting the Security Assessment

Independent Assessment Details

As part of the Assurance program, some organizations are required to use an independent party to conduct the assessment or have an independent party review the assessment process and results.

- Indication of this requirement can be found in the body of the annual Assurance Program email received.

Instructions for Independent Assessment

For organizations required to utilize an independent party, the requirement of independence can be satisfied by any one of the items below:

- An independent third party, such as an external audit firm or security consultant, conduct the assessment.
- An independent internal department/function conduct 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.

Completing the Assurance Program

Organizations are required to attest that the assessment was completed by submitting the Attestation Letter to the Federal Reserve Banks. The Attestation Letter must be signed by a senior management official or executive officer in charge of electronic payments operations or payments security.

Once the Attestation Letter is electronically signed, the organization's EUACs and the Federal Reserve Banks will receive a copy of the signed Attestation Letter.

Completing the Assurance Program Attestation Process

The EUAC designated to coordinate the Assurance Program must ensure the Attestation Letter is completed and signed.

- An EUAC must locate and access the Assurance Program email received from the Federal Reserve Banks.
- If the EUAC is not the authorized party to sign the Attestation Letter, it can be delegated by selecting the "Click here to delegate the message" link in the body of the Assurance Program email.
- EUACs for organizations with primary and secondary ABAs may receive multiple Assurance Program emails for completion.

Completing the Assurance Program

The Assurance Program materials consist of, a.) Participant Expectations Cover Page, b.) Program Guide, and c.) Attestation Letter.

Attestation Letter Details

Standard Attestation Letter

- Single page, includes the Institution Name and ABA (ensure information is accurate before signing)
- Attestation provisions outlined in Appendix B (questions regarding those Attestation Provisions can be directed to your Account Executive or the Customer Contact Center)
- Attestation check box
- Attestation signature block with associated information

Independent Attestation Letter

- Two pages in total, includes an additional page requiring information about the independent party involved
- The requested independent party information provides insight into the approach taken for completion of the independent assessment or review, along with information regarding the independent party conducting the review including contact information.

Resources & Documentation

Assurance Program Package (electronically delivered to EUACs annually in January)

Email Body: Contains important information regarding assessment type along with a link to the following:

- Participant Expectations
- Program Guide
- Attestation Letter

Security and Resiliency Assurance Program Resource Center

- Available at FRBservices.org (https://www.frbservices.org/resources/resource-centers/security-resiliency-assurance-program/index.html)
- Resources drop-down
- Resource Centers / Security and Resiliency Assurance Program

FedLine Security and Control Procedures

- Available to your organization's EUACs, for the FedLine Solution applicable to your organization
- FedLine Security and Control Procedures are part of the FedLine documentation provided to your organization during the FedLine implementation process.

Additional Support

For other questions, please contact the CCC at (888) 333-7010. In addition to contacting the CCC with questions, please know that your Account Executive is also available to assist you. To find a list of Federal Reserve Banks contacts specific to your organization, use the Find Your Contacts (https://frbservices.org/contacts/index.jsp) tool.

Q&A

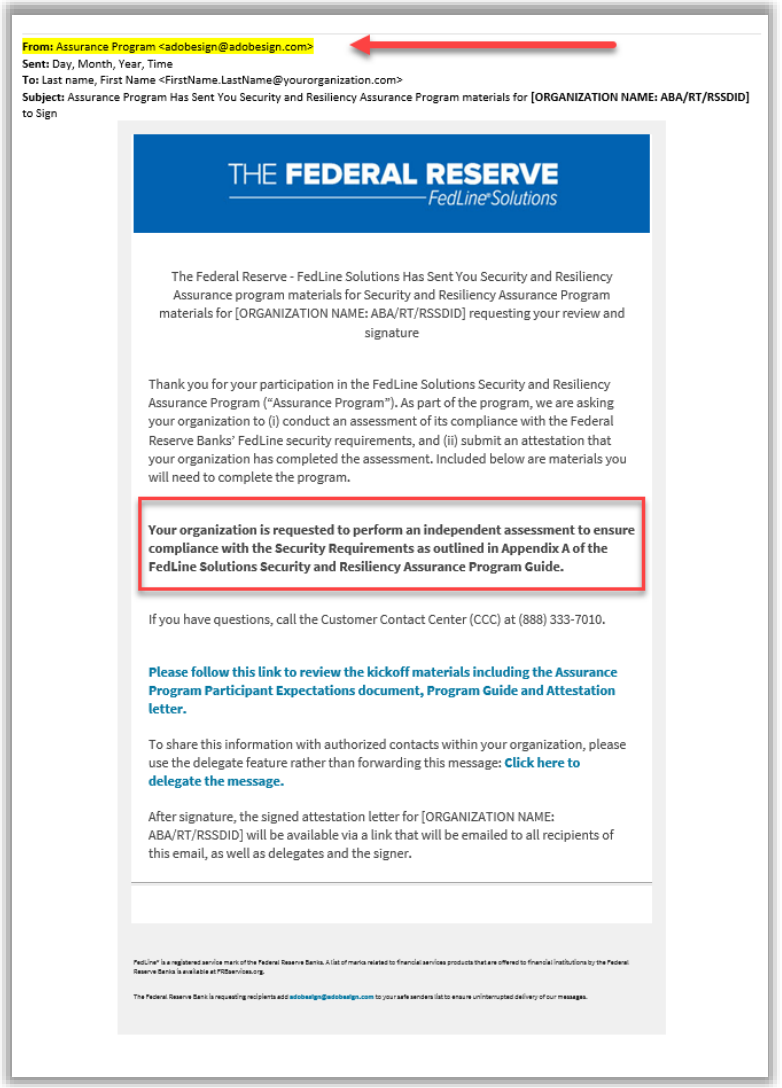
Thank you for taking part in reinforcing the safety, security, resiliency and trust of the Federal Reserve Banks services for all financial institutions and service providers.

Appendix

Assurance Program Materials

Independent Assessment Email

- Delivered via email from **Assurance Program** <adobesign@adobesign.com>
- Independent Assessment/Review Required information can be found in the center of the email body, in bold text *(highlighted here by a red box)*



From: Assurance Program <adobesign@adobesign.com>
Sent: Day, Month, Year, Time
To: Last name, First Name <FirstName.LastName@yourorganization.com>
Subject: Assurance Program Has Sent You Security and Resiliency Assurance Program materials for **[ORGANIZATION NAME: ABA/RT/RSSDID]** to Sign

THE FEDERAL RESERVE
FedLine® Solutions

The Federal Reserve - FedLine Solutions Has Sent You Security and Resiliency Assurance program materials for Security and Resiliency Assurance Program materials for [ORGANIZATION NAME: ABA/RT/RSSDID] requesting your review and signature

Thank you for your participation in the FedLine Solutions Security and Resiliency Assurance Program ("Assurance Program"). As part of the program, we are asking your organization to (i) conduct an assessment of its compliance with the Federal Reserve Banks' FedLine security requirements, and (ii) submit an attestation that your organization has completed the assessment. Included below are materials you will need to complete the program.

Your organization is requested to perform an independent assessment to ensure compliance with the Security Requirements as outlined in Appendix A of the FedLine Solutions Security and Resiliency Assurance Program Guide.

If you have questions, call the Customer Contact Center (CCC) at (888) 333-7010.

Please follow this link to review the kickoff materials including the Assurance Program Participant Expectations document, Program Guide and Attestation letter.

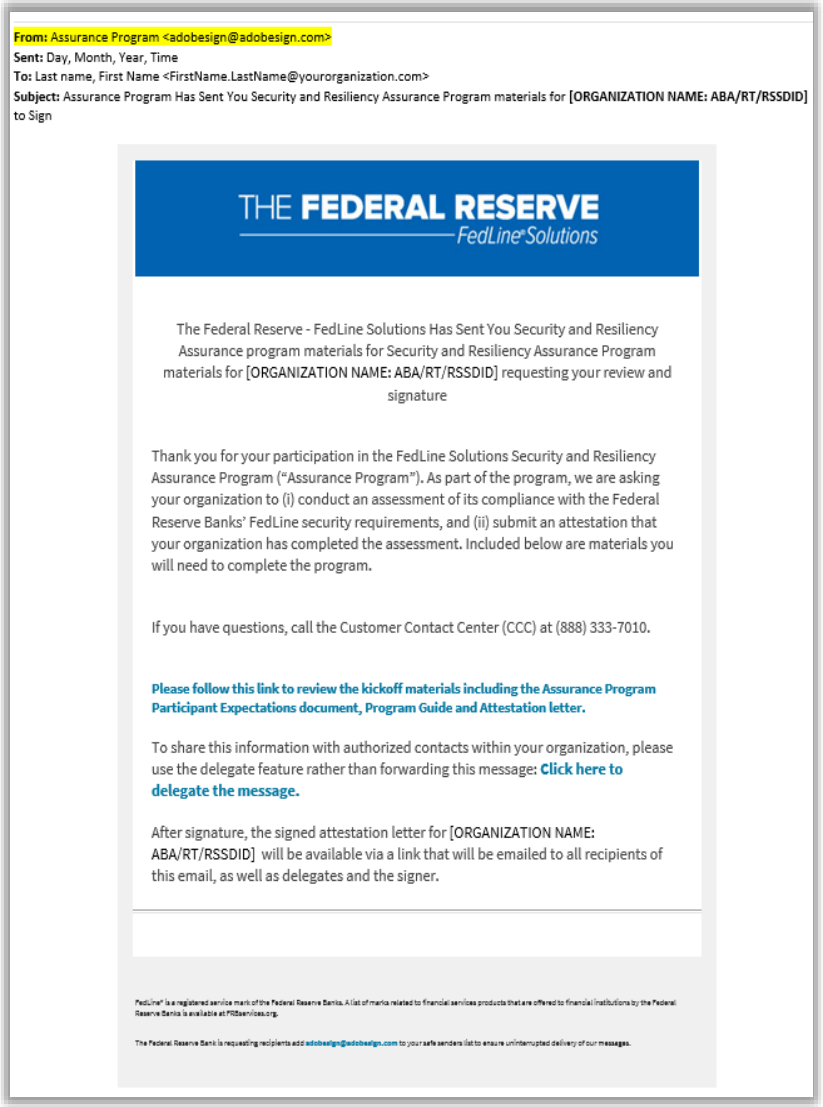
To share this information with authorized contacts within your organization, please use the delegate feature rather than forwarding this message: **Click here to delegate the message.**

After signature, the signed attestation letter for [ORGANIZATION NAME: ABA/RT/RSSDID] will be available via a link that will be emailed to all recipients of this email, as well as delegates and the signer.

Assurance Program Materials

Standard Assessment Email

- Delivered via email from **Assurance Program** <adobesign@adobesign.com>
- Note absence of bold text; no Independent Assessment required



From: Assurance Program <adobesign@adobesign.com>
Sent: Day, Month, Year, Time
To: Last name, First Name <FirstName.LastName@yourorganization.com>
Subject: Assurance Program Has Sent You Security and Resiliency Assurance Program materials for **[ORGANIZATION NAME: ABA/RT/RSSDID]** to Sign

THE FEDERAL RESERVE
FedLine® Solutions

The Federal Reserve - FedLine Solutions Has Sent You Security and Resiliency Assurance program materials for Security and Resiliency Assurance Program materials for [ORGANIZATION NAME: ABA/RT/RSSDID] requesting your review and signature

Thank you for your participation in the FedLine Solutions Security and Resiliency Assurance Program ("Assurance Program"). As part of the program, we are asking your organization to (i) conduct an assessment of its compliance with the Federal Reserve Banks' FedLine security requirements, and (ii) submit an attestation that your organization has completed the assessment. Included below are materials you will need to complete the program.

If you have questions, call the Customer Contact Center (CCC) at (888) 333-7010.

Please follow this link to review the kickoff materials including the Assurance Program Participant Expectations document, Program Guide and Attestation letter.

To share this information with authorized contacts within your organization, please use the delegate feature rather than forwarding this message: **Click here to delegate the message.**

After signature, the signed attestation letter for [ORGANIZATION NAME: ABA/RT/RSSDID] will be available via a link that will be emailed to all recipients of this email, as well as delegates and the signer.

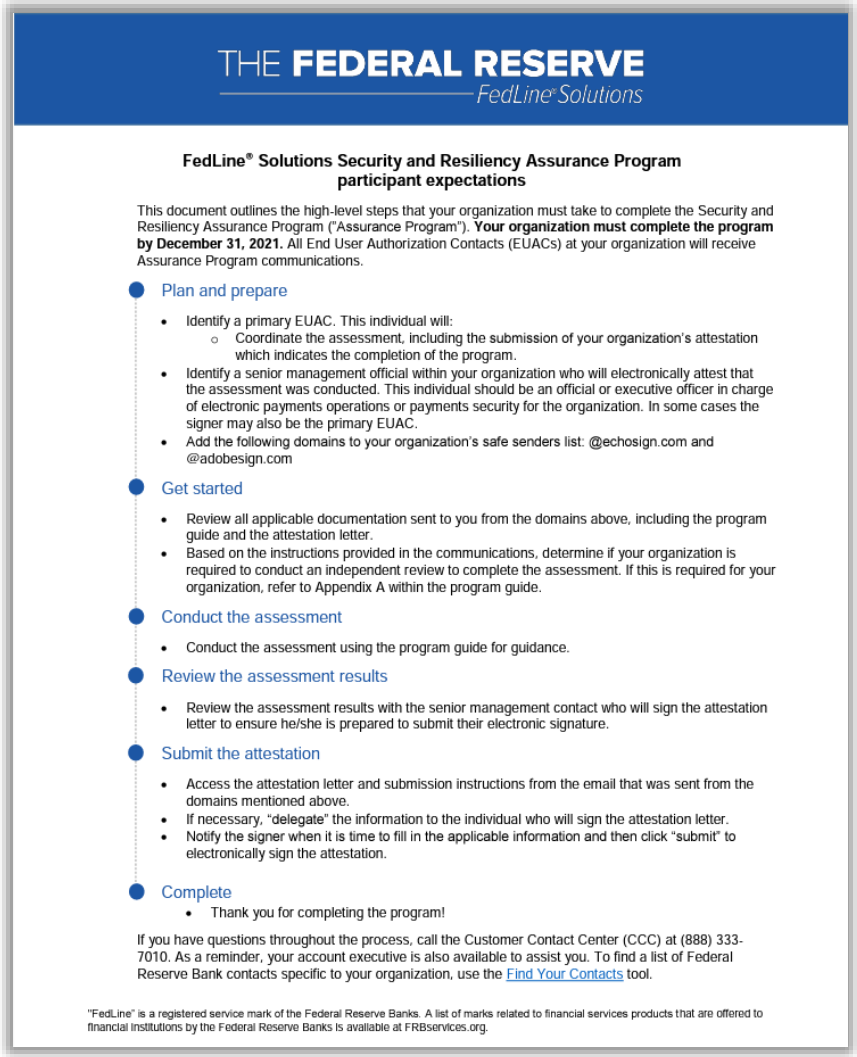
FedLine® is a registered service mark of the Federal Reserve Banks. A list of marks related to financial services products that are offered to financial institutions by the Federal Reserve Banks is available at FRBservices.org.

The Federal Reserve Bank is requesting recipients add adobesign@adobesign.com to your safe senders list to ensure uninterrupted delivery of our messages.

Assurance Program Materials

Participant Expectations

- Will be first document that appears when you click the blue text link in the email body



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

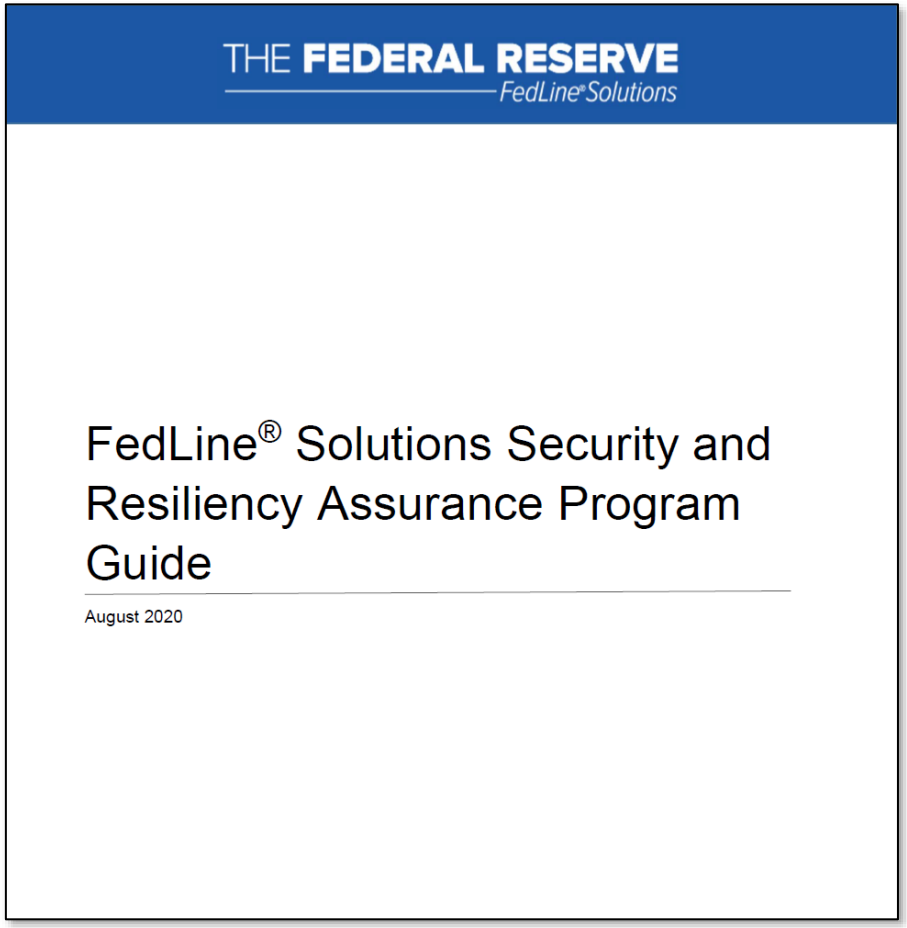
- Thank you for completing the program!

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.

"FedLine" is a registered service mark of the Federal Reserve Banks. A list of marks related to financial services products that are offered to financial institutions by the Federal Reserve Banks is available at FRBservices.org.

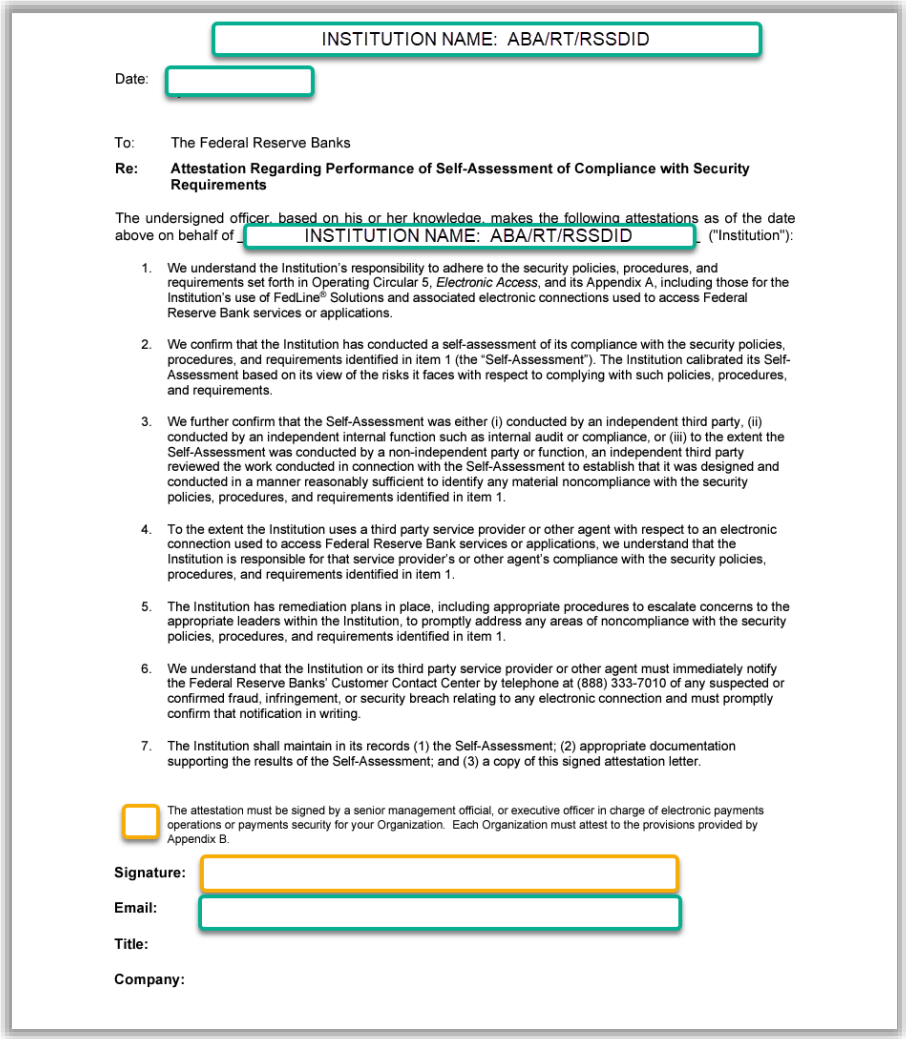
Assurance Program Materials

2021 Program Guide



Assurance Program Materials

Attestation Letters



INSTITUTION NAME: ABA/RT/RSSDID

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 INSTITUTION NAME: ABA/RT/RSSDID ("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.

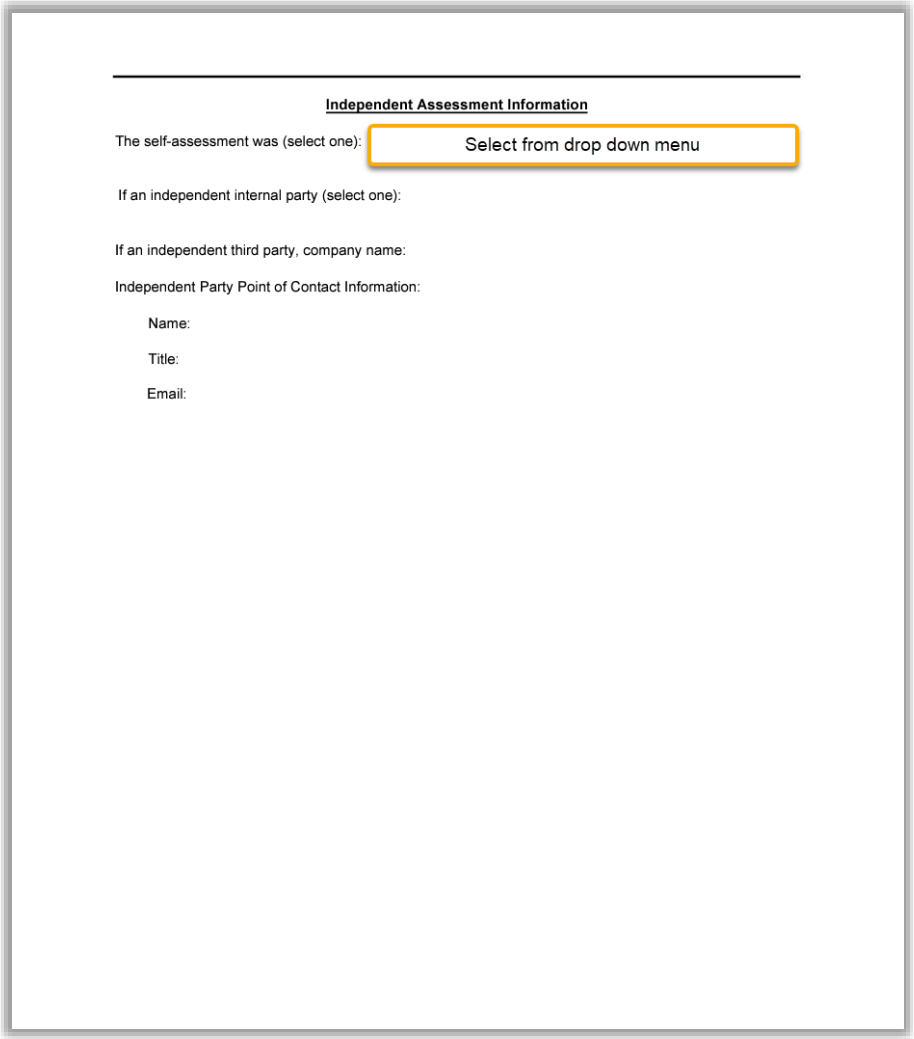
☐ The attestation must be signed by a senior management official, or executive officer in charge of electronic payments operations or payments security for your Organization. Each Organization must attest to the provisions provided by Appendix B.

Signature:

Email:

Title:

Company:



Independent Assessment Information

The self-assessment was (select one): Select from drop down menu

If an independent internal party (select one):

If an independent third party, company name:

Independent Party Point of Contact Information:

Name:

Title:

Email: