1. Implement FedLine Advantage on a personal computer ("PC") that is dedicated to supporting critical business functions. Critical business functions comprise activities that provide business value to your organization and are performed with heightened vigilance and scrutiny to ensure their accuracy and integrity. In accordance with your organization's risk management practices, you may dedicate one or more PCs solely for Fedline Advantage use.
    - *Fedline Advantage is installed only on approved devices within the Bank. Since the Fedline Advantage users are working in the hybrid environment (on-site and remote work), the Bank decided to not provide dedicated devices solely for Fedline Advantage use, as this would require individuals to have 2 devices. The Bank has determined the control environment is sufficient for Fedline Advantage to be used on devices that perform other bank functions.*
2. Ensure that personal firewall software is properly installed, configured and regularly updated. Adjust the software settings as appropriate to ensure that network traffic using the https protocol (e.g., port 443) is permitted to flow between Subscriber PCs and the VPN device.
    - *The Bank leverages Crowdstrike Endpoint Detection and Response (EDR) software that prevents malicious software from executing on the end points. Although this is not considered "personal firewall software", the solution does mitigate similar risks. Additionally, the Bank's primary Internet firewall is tightly configured to only allow HTTPS (SSL encrypted) traffic to the Fedline Advantage site.*
3. Implement physical and logical access controls to help ensure that only authorized users can access Subscriber PCs. This may include allocating one or more Subscriber PCs that are physically and logically dedicated to conducting Fedline transactions.
    - *The Bank is operating in a hybrid environment due to the COVID-19 Pandemic and it might be possible that an employee without access to Fedline Advantage will use a computer with Fedline Advantage software installed. Although the Bank has given the majority of its staff laptop devices, in rare cases there might be a computer with Fedline Advantage installed that might be used by an employee who is not a user of Fedline Advantage. The Bank does require Fedline Advantage users to keep tight control of their access tokens.*
4. Where passwords are used for Subscriber PC authentication, use complex, alphanumeric passwords in accordance with your organization's security policies. For Fedline Advantage authentication, employ passwords that are different than those used to authenticate to the Subscriber PC and which comply with the Federal Reserve Banks' Password Practice Statement.
    - *The Bank enforces complex, alphanumeric passwords for logging in to the Network. Complex passwords are also mandated for login to the Fedline Advantage software. We believe that the use of the token is equivalent to having a distinct password. We will add the requirement for using a different password to the Fedline users guide because there is no systemic way to mandate the use of different passwords.*
5. Ensure that Subscriber PCs will automatically lock after 10 minutes of inactivity.
    - *The Bank and industry standard is to lock all workstations/laptops after 15 minutes of inactivity. We do not believe that a setting of 10 minutes will significantly lessen the risk.*

6. Where technically feasible, use multi-factor authentication for interactive login to Subscriber PCs. The form of such multi-factor authentication is in addition to and independent of the Fedline credentials used to authenticate to Fedline Advantage.
    - *The Bank requires logical multi-factor authentication for remote access to the Bank's network (through VPN). Multi-factor authentication is not required for on premise users. The physically segregated space employed for on premise users serves as a second level of authentication. Nevertheless the Bank will be evaluating additional authentication controls for interactive logins in 2022.*
7. Implement policy and, where feasible, technical controls to limit the accounts on Subscriber PCs to only those necessary for critical business functions. Furthermore:

    a. Where technically feasible, unmanaged (e.g. local) accounts should be avoided.

    b. Implement policy and, where feasible, technical controls to restrict administrative, network, middleware and/or operating system privileges for accounts defined on Subscriber PCs to the minimum period of time necessary. Limiting the use of administrative accounts may, among other benefits, minimize the risk of system compromise by contemporary malware and related cyber threats.

    c. Implement policy and, where feasible, technical controls to enforce least-privilege access for login accounts with access to Subscribers PCs. Enforcing least-privilege access may, among other benefits, reduce the extent of system compromise by contemporary malware and related cyber threats.

    d. Accounts used on Subscriber PCs for interacting with Fedline must be different accounts than those used for other business activity. This may, among other benefits, reduce the risk that a successful compromise of accounts not used for accessing Fedline will adversely affect Fedline Advantage security and functionality.
    - *At this time, the Bank is fully compliant with the controls in this section with the exception of, "Accounts used on Subscriber PCs for interacting with Fedline must be different than those used for other business activity." Bank employees use the same Active Directory credentials when they are connecting to Fedline Advantage and when performing other business activities. It would be impractical and require increased management to use a different set of network credentials for connecting to Fedline advantage and switch to a different set of credentials for performing other business functions.*
8. Assign a static IP address to Subscriber PCs to provide a means of uniquely identifying Subscriber PCs on the network and building access controls around communication with the VPN device(s) or Dedicated WAN device(s).
    - *The Bank does not leverage static IP addresses for its end-points that communicate to the FED. Since the start of the Pandemic, Fedline Advantage users access it via remote access VPN, and assigning static IP addresses in the VPN environment is very challenging. The Bank is considering leveraging Active Directory groups to further control access to the Fedline Advantage application in 2022.*
9. Implement technical controls to identify/flag/categorize external inbound emails targeted for Subscriber PCs. When feasible, implement controls to prohibit Subscriber PCs from receiving emails that originate from outside of your organization.
    - *The Bank currently flags emails received by our employees sourced from an external (non-Bank domain) address and provides employee awareness and*

handling training to ensure diligence in the review of such emails. At this time, it would be impractical to prohibit Subscriber workstations from receiving external emails, as the users of Subscribers workstations also use the same computers for other business processes to include sending/receiving external emails.

10. Implement policy and, where feasible, technical controls to ensure that Fedline traffic is appropriately restricted to authorized Subscriber PCs and transactions are monitored to identify anomalous activity.
    - *The Bank is in the process of implementing enhanced network segmentation. Once the project is complete, the Fedline application traffic will be segmented with the help of an Active Directory Group used within the firewall configuration. The target date for completion is Q1, 2022.*
11. Conduct periodic control validation testing of your Fedline Advantage implementation and ensure the timely correction of any identified variances.
    - *The Bank conducts regular testing of the Fedline Advantage implementation (at least once a year) via various risk assessments and audits. We believe the frequency of testing is sufficient to satisfy this control objective, but we would like to get clarity on what the FED means by "periodic control validation".*