

**Federal Reserve Banks  
Operating Circular No. 5**

**ELECTRONIC ACCESS**

**Effective February 1, 2023**

**FEDERAL RESERVE BANKS  
OPERATING CIRCULAR NO. 5  
Effective February 1, 2023**

**ELECTRONIC ACCESS**

(Click CTRL + section or page number to go directly to the section)

<b>1.0</b>	<b>GENERAL</b> .....	<b>1</b>
1.1	INTRODUCTION .....	1
1.2	SERVICES ACCESSIBLE VIA ELECTRONIC CONNECTIONS.....	2
1.3	OTHER CIRCULARS; INSTITUTION'S AGREEMENT .....	2
1.4	INSTITUTION'S SECURITY OBLIGATIONS .....	3
1.5	PRIOR APPROVAL OR NOTICE REQUIREMENTS FOR ELECTRONIC CONNECTIONS.....	4
1.6	SERVICE PROVIDERS .....	4
<b>2.0</b>	<b>INSTITUTION'S EQUIPMENT AND SOFTWARE</b> .....	<b>5</b>
<b>3.0</b>	<b>AVAILABLE ELECTRONIC CONNECTIONS</b> .....	<b>5</b>
<b>4.0</b>	<b>RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT AND SOFTWARE; WARRANTIES; DISCLAIMER OF WARRANTY</b> .....	<b>6</b>
4.1	EQUIPMENT DELIVERY, INSTALLATION, AND ALTERATIONS.....	6
4.2	ELECTRONIC CONNECTION TO NETWORK; SOFTWARE .....	6
4.3	SOFTWARE LICENSE.....	6
4.4	ELECTRONIC CONNECTION RESTRICTIONS.....	7
4.5	DISCLAIMER OF WARRANTY.....	7
4.6	UNAUTHORIZED DISCLOSURE OR USE OF SOFTWARE .....	8
4.7	RESERVE BANK'S MALWARE PROTECTION.....	8
4.8	INSTITUTION'S AND SERVICE PROVIDER'S MALWARE PROTECTION .....	9

<b>5.0 RISK AND LIABILITY IN USE OF ELECTRONIC CONNECTIONS.....</b>	<b>9</b>
<b>5.1 RESPONSIBILITY FOR ACCESS CONTROL FEATURES .....</b>	<b>9</b>
<b>5.2 RESERVE BANK LIABILITY .....</b>	<b>10</b>
<b>5.3 COMPLIANCE WITH RESERVE BANK STANDARDS.....</b>	<b>11</b>
<b>5.4 CONFIDENTIALITY OF RESERVE BANK PROPRIETARY AND SECURITY-         RELATED INFORMATION .....</b>	<b>11</b>
<b>5.5 MANAGEMENT OF ELECTRONIC CONNECTIONS .....</b>	<b>12</b>
<b>5.6 CONTINGENCY PLANS FOR DISRUPTION OF ELECTRONIC CONNECTIONS.</b>	<b>13</b>
<b>6.0 FEES AND TAXES .....</b>	<b>13</b>
<b>6.1 ELECTRONIC CONNECTION FEES .....</b>	<b>13</b>
<b>6.2 OFF-LINE FEES DUE TO EQUIPMENT FAILURE.....</b>	<b>13</b>
<b>6.3 LIABILITY FOR TAXES .....</b>	<b>13</b>
<b>7.0 TERMINATION AND AMENDMENT.....</b>	<b>14</b>
<b>7.1 TERMINATING THE ELECTRONIC ACCESS AGREEMENT.....</b>	<b>14</b>
<b>7.2 RETURN OF RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT AND         SOFTWARE; SURVIVAL OF OBLIGATIONS .....</b>	<b>14</b>
<b>7.3 AMENDMENT OF CIRCULAR.....</b>	<b>15</b>
<b>8.0 FORUM, GOVERNING LAW AND TIME FOR ACTIONS .....</b>	<b>15</b>
<b>9.0 EFFECT OF THIS CIRCULAR ON PREVIOUS CIRCULAR .....</b>	<b>15</b>
<b>Appendix A.....</b>	<b>16</b>
<b>Appendix B.....</b>	<b>26</b>

## 1.0 GENERAL

### 1.1 INTRODUCTION

This operating circular (“Circular”) sets forth the terms under which an Institution may access certain services and applications provided by a Reserve Bank, and under which an Institution or its Service Provider may send certain data to or receive certain data from a Reserve Bank, by means of electronic connection(s).

For purposes of this Circular:

- (a) **Access Control Feature** means the Software, encryption keys, logon identifications (“logon IDs”), passwords, pass phrases, digital certificates, Virtual Private Network (“VPN”) devices, routers, removable certificate storage devices (“tokens”), personal identification numbers (“PINs”), encryption technology, workstation configurations, workstation or network access restrictions (physical or logical), and other security measures used for access, authentication or authorization with regard to an Electronic Connection.
- (b) **Electronic Connection** refers to a communication facility used to exchange data between a Reserve Bank and an Institution or its Service Provider. The term includes but is not limited to an Internet, extranet, wireless, wide area network (“WAN”), local area network (“LAN”), or other data connection, and a connection for which access, authentication, or authorization is controlled by use of one or more Access Control Features.
- (c) **Institution** means (i) a depository institution as defined in Section 19(b) of the Federal Reserve Act (12 U.S.C. § 461(b)); (ii) a branch or agency of a foreign bank maintaining reserves under Section 7 of the International Banking Act of 1978 (12 U.S.C. § 347d, 3105); (iii) a department, agency, instrumentality, independent establishment, or office of the United States, or a wholly owned or controlled Government corporation; (iv) another entity for which a Reserve Bank directly provides financial services or (v) any entity or individual authorized by any Federal Reserve Bank to use an Electronic Connection for submitting regulatory reports, applications and information or for software testing.
- (d) **Reserve Bank** means any Federal Reserve Bank.
- (e) **Service Provider** means a person or entity, other than a Reserve Bank, that uses an Electronic Connection on behalf of an Institution.
- (f) **Software** means all software, including upgrades, modifications, applets and hypertext markup language (“HTML”), as well as any other code that resides on the Federal Reserve Banks' servers and/or equipment required by the Federal Reserve Banks to be deployed (i.e. firmware) that permits transactions to occur or data to be transferred between an Institution and a Reserve Bank and third party software that a Reserve

Bank provides to an Institution for the purpose of accessing a Reserve Bank's services and/or applications.

## **1.2 SERVICES ACCESSIBLE VIA ELECTRONIC CONNECTIONS**

Services which may be accessed using an Electronic Connection include, for example:

- a transfer of funds and/or securities;
- multilateral settlement service;
- commercial and/or governmental automated clearing house transactions;
- electronic presentment of checks;
- notification of nonpayment of checks;
- an order for cash and/or savings bonds;
- a bid for Treasury securities or Treasury investments;
- receipt of data related to services (such as check information, federal tax payment advices, and statements of account) sent by a Reserve Bank; and
- transmission of data related to services (such as check information and Treasury Tax and Loan ("TT&L") reports) to a Reserve Bank.

The Reserve Banks also permit Institutions to use Electronic Connections to submit certain statistical, regulatory and financial reports and to receive data related to those reports. Use of an Electronic Connection for these purposes does not in any way alter or modify the requirements governing the completion and submission of such reports, including any requirements to sign and retain copies of the reports.

A Reserve Bank may from time to time offer other services and/or applications using an Electronic Connection.

## **1.3 OTHER CIRCULARS; INSTITUTION'S AGREEMENT**

Each Reserve Bank has issued a Circular identical to this one. In the event of any inconsistency between this Circular and any other Reserve Bank operating circular, agreement, or instruction governing particular types of transactions, such other operating circular, agreement or instruction controls. By accessing any services and/or applications from a Reserve Bank (including, for example, the E-Payments Routing Directory Service described in Appendix B), or by sending data to or receiving data from a Reserve Bank, by means of any Electronic Connection, directly or through a Service Provider, an Institution agrees to the provisions of this Circular, including the terms of Appendix A, *Information Security Program*, and any Certification Practice Statement ("CPS"), as each may be amended from time to time, applicable to the Electronic Connection(s) that the Institution uses. The Institution also agrees to the

provisions of any separate agreement governing the use of a service, and agrees that any such agreement, including modifications and amendments thereto, may be posted and agreed to purely in electronic form. The current version of any CPS may be accessed at the Federal Reserve Bank Services Web site at [www.FRBservices.org](http://www.FRBservices.org), or such other location as a Reserve Bank may designate.

#### 1.4 INSTITUTION'S SECURITY OBLIGATIONS

The Institution agrees that complying with the security measures required by a Reserve Bank shall not relieve the Institution of its obligation and responsibility to exercise its own independent judgments about security and additional steps or procedures needed to prevent fraud, unauthorized access or other unauthorized use of an Electronic Connection. Accordingly, an Institution agrees to take all additional commercially reasonable security measures in establishing an Electronic Connection as circumstances may dictate over time; and further agrees to take all commercially reasonable security measures necessary to prevent fraud, unauthorized access or other unauthorized use of an Electronic Connection or necessary to prevent disruption to the operations of any Reserve Bank's, and other Institutions', computers, networks, systems and software.

The Institution or its Service Provider must immediately notify the Reserve Banks by telephone at (888) 333-7010, with written confirmation via email at [ccc.technical.support@kc.frb.org](mailto:ccc.technical.support@kc.frb.org), of any suspected, threatened or known cyber event, fraud, malware detection, compromise, or other security incident or breach, that relates to or has the potential to impact an Electronic Connection, Access Control Feature, or the use of a Reserve Bank financial service, including (but not limited to) circumstances in which the Institution or the Service Provider have a reasonable basis to know or suspect that such event:

- impacts or may impact software or hardware that the Institution or Service Provider use to engage or interface with an Electronic Connection or an Access Control Feature;
- impacts or may impact software or data stored on servers or other electronic media shared with Reserve Bank data or applications;
- impacts or may impact hardware, software or data that are used to generate transactions, messages, or other information that will be transmitted through an Electronic Connection;
- caused or may have caused the Institution or its Service Provider to generate an unauthorized transaction;
- causes or may cause the Institution or Service Provider to modify its operations while investigating or mitigating the impact of the event;
- requires notification by the Institution or its Service Provider to its prudential regulator, or by a Service Provider to the Institution, pursuant to any law, regulation, or supervisory requirement;

- resulted in or may have resulted in the loss of, unauthorized access to, compromise of, or tampering with an Access Control Feature; or
- resulted or may have resulted in the unauthorized disclosure or use of Confidential Information or the Security Procedures described in Appendix A.

## **1.5 PRIOR APPROVAL OR NOTICE REQUIREMENTS FOR ELECTRONIC CONNECTIONS**

A Reserve Bank's prior approval may be required before an Institution or a Service Provider uses an Electronic Connection to access any of the Reserve Bank's services and applications or to send any data to or receive any data from the Reserve Bank.

Additionally, an Institution must provide written notice before it uses a Service Provider, and an Institution or a Service Provider must provide prior written notice to the Reserve Bank before it:

- (a) shares the use of an Electronic Connection with another Institution or entity or,
- (b) sublicenses, assigns, delegates or transfers to a third party any of its rights, duties or obligations under this Circular.

The Reserve Bank reserves the right to reject any of the arrangements described in (a) or (b) above, and use of any such arrangements does not in any way affect or diminish any obligation or duty of the Institution to a Reserve Bank under this Circular.

## **1.6 SERVICE PROVIDERS**

By accessing any services and/or applications from a Reserve Bank, or by sending data to or receiving data from a Reserve Bank, by means of any Electronic Connection, a Service Provider agrees to the provisions of this Circular applicable to Service Providers. For purposes of the CPS, a Service Provider may be a Participant and/or a Subscriber, depending on its relationship with the Institution. The Reserve Bank reserves the right to require any Service Provider to agree in writing to additional terms and conditions, depending on the type of Electronic Connection and/or service the Service Provider is accessing on behalf of the Institution.

The provision of services by a Service Provider to an Institution shall in no way affect or diminish any obligation or duty of the Institution under this Circular or the provisions of any separate agreement governing the use of a particular Reserve Bank service. The Institution agrees that: (i) its Service Provider may be granted certain Access Control Features authorizing such Service Provider to use an Electronic Connection; (ii) its Service Provider will use those Access Control Features to act on behalf of the Institution; and (iii) its Service Provider may use the same Access Control Features to act on behalf of other Institutions that use the same Service Provider to access a Reserve Bank's computer systems. It is the responsibility of the Institution and its Service Provider to establish controls sufficient to ensure that the Service Provider properly segregates the data of the

Institution from any data of other Institutions. The Reserve Banks are not required to take, and will not take, any measures to ensure that the Institution's data are properly segregated by its Service Provider. The Institution authorizes each Reserve Bank to rely on its Service Provider's identification of data as having been originated or authorized by the Institution. The sending or receiving of data by means of any Electronic Connection by a Service Provider purportedly on behalf of an Institution constitutes the sending or receiving of the data by the Institution for purposes of the Reserve Bank acting on such data.

Except to the extent prohibited by law or regulation, the Institution and the Service Provider shall defend, indemnify, and hold the Reserve Banks harmless against any liability, claim, loss, cost or expense, including, but not limited to, attorneys' fees and expenses of litigation, resulting from the Service Provider agency relationship or the acts or omissions of either the Institution or the Service Provider or their agents except, however, for any liability, claim, loss, cost or expense arising solely out of a Reserve Bank's failure to exercise ordinary care.

The Reserve Bank reserves the right, without prior notice, to terminate any Service Provider arrangement.

## **2.0 INSTITUTION'S EQUIPMENT AND SOFTWARE**

An Institution is responsible for ensuring that its and its Service Provider's, if any, computer(s) and associated equipment and software comply with Reserve Bank requirements (which a Reserve Bank may change from time to time) and for maintaining its own equipment. The Reserve Banks reserve the right to approve or disapprove the use of an Institution's or its Service Provider's equipment and software, and/or to make recommendations regarding the equipment and software that the Institution uses. The Reserve Bank's knowledge of any noncompliance with its requirements for computer(s) and associated equipment and software used to establish an Electronic Connection does not constitute the Reserve Bank's approval of such noncompliance. Any such noncompliance shall be solely at the risk of the Institution and its Service Provider, where applicable. THE RESERVE BANKS DO NOT HAVE ANY OBLIGATION FOR, AND DO NOT MAKE ANY WARRANTY OR REPRESENTATION OF ANY KIND WITH RESPECT TO, ANY COMMUNICATION FACILITY, NETWORK, BROWSER, OPERATING SYSTEM, SERVER, OR ANY OTHER EQUIPMENT OR SOFTWARE NOT SUPPLIED, OWNED OR OPERATED BY A RESERVE BANK.

A Reserve Bank may, at its option, also specify third party vendors through which an Institution or its Service Provider must obtain equipment or software necessary for establishing and maintaining an Electronic Connection.

## **3.0 AVAILABLE ELECTRONIC CONNECTIONS**

An Institution or its Service Provider may choose from certain Electronic Connections that a Reserve Bank makes available and/or that a Reserve Bank permits to be used to connect to a Reserve Bank's services. A Reserve Bank reserves the right to specify the type of Electronic Connection necessary to support the volume and type of an Institution's transactions.



## **4.0 RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT AND SOFTWARE; WARRANTIES; DISCLAIMER OF WARRANTY**

### **4.1 EQUIPMENT DELIVERY, INSTALLATION, AND ALTERATIONS**

A Reserve Bank may, at its option, arrange for the delivery and/or installation of Reserve Bank supplied or designated equipment necessary for establishing an Electronic Connection.

Reserve Bank supplied or designated equipment may not be altered, encumbered, relocated, removed or transferred to a third party, except with the Reserve Bank's prior written approval. The Institution and its Service Provider, if any, are liable for any loss of and damage to Reserve Bank supplied or designated equipment, ordinary wear and tear excepted.

Unless otherwise agreed in writing, a Reserve Bank is not responsible for the delivery, installation, repair or alteration of any non-Reserve Bank supplied equipment, even if the Reserve Bank required that such equipment be used in order to establish an Electronic Connection to the Reserve Bank's computers.

### **4.2 ELECTRONIC CONNECTION TO NETWORK; SOFTWARE**

The Reserve Banks require the use of specified Access Control Features to establish an Electronic Connection, and/or to permit access to certain services or applications over the connection. A Reserve Bank may provide, on request and where appropriate, either Computer Interface Protocol Specifications, product specifications, or Software (including documentation) to enable a connection to the Reserve Banks' network.

### **4.3 SOFTWARE LICENSE**

In the event a Reserve Bank provides Software or access to Software, except as otherwise provided in a written agreement specifically referencing the Software, the Reserve Bank grants the Institution or its Service Provider, if any, a personal, nontransferable, nonexclusive license to use the Software solely for the purposes stated in this Circular and in compliance with applicable security procedures. The Reserve Bank warrants that it owns or has the right to license or sublicense the Software, and the Reserve Bank shall indemnify and hold the Institution and its Service Provider, if any, harmless from any loss or expense arising from any claim that the Software alone, and not in combination with any other party's products, software or activities, infringes a patent, copyright, trademark or other proprietary right of any third party, provided the Reserve Bank is given prompt written notice of the claim, has sole control of the defense of the claim and of any settlement negotiations, and the Institution and its Service Provider, if any, cooperate fully with the Reserve Bank in the defense and negotiations. In the event of a claim that the Software infringes any third party proprietary right, the Reserve Bank reserves the right in its sole discretion to (a) replace the Software with a noninfringing product, (b) modify the Software to avoid the infringement, (c) obtain a license for the Institution to continue use of the Software, or (d) terminate the use of the Software.

#### **4.4 ELECTRONIC CONNECTION RESTRICTIONS**

In addition to restrictions contained in Paragraph 4.1, an Institution or its Service Provider may not, except with a Reserve Bank's prior written consent:

- (a) situate any VPN device used in conjunction with an Electronic Connection in any location other than the Institution's or its Service Provider's premises within the United States or its territories\*;
- (b) modify, add to, translate, reverse assemble, reverse compile, decompile or otherwise attempt to derive the source code from any Software;
- (c) copy, sublicense or transfer the Software for any reason except that Software may be copied for back-up, testing or archival purposes, and all such copies shall include the Reserve Bank's and any third party's copyright, trademark and proprietary notices externally in the distribution medium and internally in machine-readable form; or,
- (d) remove any copyright or trademark notice contained in the Software.

Use of an Electronic Connection from outside of the U.S. and its territories is permissible only in accordance with the Reserve Banks' policies and procedures pertaining to foreign access. Institution acknowledges and understands that it and its Service Provider, if any, will be required to agree to additional terms and conditions governing any regular and on-going foreign access (including contingency arrangements) prior to such use of an Electronic Connection.

#### **4.5 DISCLAIMER OF WARRANTY**

RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT AND SOFTWARE (INCLUDING DOCUMENTATION), AND ANY ACCESS CONTROL FEATURE, ELECTRONIC CONNECTION, RECOMMENDATION, SECURITY PROCEDURE, OPERATING INSTRUCTION, USER MANUAL, GUIDELINE AND SPECIFICATION FOR AN ELECTRONIC CONNECTION THAT A RESERVE BANK SPECIFIES, ARE FURNISHED STRICTLY ON AN "AS-IS" BASIS. THE RESERVE BANKS DO NOT WARRANT OR REPRESENT THAT OPERATION OF ANY RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT OR SOFTWARE OR USE OF AN ELECTRONIC CONNECTION OR ACCESS CONTROL FEATURE WILL MEET AN INSTITUTION'S OR ITS SERVICE PROVIDER'S PLANNED APPLICATIONS, THAT RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT OR SOFTWARE WILL BE COMPATIBLE WITH AN INSTITUTION'S OR ITS SERVICE PROVIDER'S EQUIPMENT, OR THAT ANY DEFECT IN RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT OR SOFTWARE CAN BE CORRECTED. THE RESERVE BANKS DO NOT WARRANT OR REPRESENT THAT USE OF AN ELECTRONIC CONNECTION, REGARDLESS OF WHETHER USED IN CONJUNCTION WITH ANY ACCESS CONTROL FEATURES AND/OR IN COMPLIANCE WITH ANY RECOMMENDATIONS, SECURITY PROCEDURES, OPERATING INSTRUCTIONS, USER MANUALS, GUIDELINES, OTHER DOCUMENTATION, AND SPECIFICATIONS FOR AN ELECTRONIC

---

\* Puerto Rico, the U.S. Virgin Islands, American Samoa, Guam and the Northern Mariana Islands.

CONNECTION THAT A RESERVE BANK SPECIFIES, WILL BE UNINTERRUPTED, FREE FROM INTERCEPTION, TIMELY, SECURE, OR ERROR FREE.

A RESERVE BANK'S SOLE OBLIGATION IN THE EVENT OF A MALFUNCTION IN RESERVE BANK SUPPLIED EQUIPMENT OR SOFTWARE IS TO PROVIDE A REMEDY IN THE FORM OF EITHER PROVIDING REASONABLE ASSISTANCE IN RESOLVING PROBLEMS OR REPLACING DEFECTIVE OR DAMAGED EQUIPMENT OR SOFTWARE: (1) THAT AN INSTITUTION OR ITS SERVICE PROVIDER RETURNS TO THE RESERVE BANK OR (2) ABOUT WHICH AN INSTITUTION OR ITS SERVICE PROVIDER INFORMS THE RESERVE BANK. THE RESERVE BANK SHALL HAVE SOLE AUTHORITY TO SELECT THE FORM OF THE REMEDY TO SATISFY THAT OBLIGATION, IF ANY.

A RESERVE BANK SHALL HAVE NO OBLIGATION FOR EQUIPMENT OR SOFTWARE THAT IS PURCHASED BY THE INSTITUTION OR ITS SERVICE PROVIDER FROM A THIRD PARTY VENDOR, EVEN IF THE RESERVE BANK REQUIRES THE USE OF THAT EQUIPMENT OR SOFTWARE OR ARRANGES FOR THE PURCHASE FROM SAID VENDOR.

THE OBLIGATIONS AND THE WARRANTY SET FORTH IN THIS PARAGRAPH AND IN PARAGRAPH 4.3 ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY OTHER WARRANTY ARISING BY STATUTE OR FROM A COURSE OF DEALING OR USAGE OF TRADE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY A RESERVE BANK SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THE RESERVE BANKS' OBLIGATIONS.

#### **4.6 UNAUTHORIZED DISCLOSURE OR USE OF SOFTWARE**

Software includes trade secrets and proprietary information of the Reserve Banks and others, which may be copyrighted or patented, and must be handled in accordance with the requirements applicable to Confidential Information as set forth in Paragraph 5.4.

#### **4.7 RESERVE BANK'S MALWARE PROTECTION**

The Reserve Banks provide Software either on optical disks or other electronic media or through data transmission facilities. The Reserve Banks use commercially reasonable efforts to provide Software that is free of known malicious code such as computer viruses, trojans, worms or other defects that might disrupt the operations of computers or software ("Malware") The Reserve Banks test random samples of electronic media obtained from vendors, using malicious code-detection software that the Reserve Banks believe is commercially reasonable. However, it is not commercially feasible for the Reserve Banks to test all such electronic media, and the malicious code-detection software may not detect all Malware. Reserve Bank data transmission facilities also are protected by what the Reserve Banks believe is commercially reasonable technology to prevent the introduction of Malware.

#### **4.8 INSTITUTION'S AND SERVICE PROVIDER'S MALWARE PROTECTION**

The Institution and its Service Provider, if any, agree to take all commercially reasonable precautions and protections to prevent the introduction of Malware that might disrupt the operations of a Reserve Bank's, or other Institutions' or Service Providers', computers or software, including the installation, operation and proper configuration of commercially reasonable anti-Malware software. Certain Software that a Reserve Bank supplies may not be compatible with all types of commercial anti-Malware software. Accordingly, an Institution or its Service Provider may need to use an alternative type of commercial anti-Malware software on certain computers that contain Access Control Feature(s) or that are otherwise engaged in Electronic Connection(s) with a Reserve Bank. The Institution and its Service Provider, if any, shall institute and/or reinforce procedural controls, such as the timely patching of software (including, but not limited to, operating systems, applications, and firmware), and regular scanning/assessment of the enterprise environment for vulnerabilities and other exposures.

### **5.0 RISK AND LIABILITY IN USE OF ELECTRONIC CONNECTIONS**

#### **5.1 RESPONSIBILITY FOR ACCESS CONTROL FEATURES**

An Institution and its Service Provider, if any:

- (a) must use all Access Control Features specified by a Reserve Bank, but may use any Access Control Features supplied by a Reserve Bank or by a vendor specified by a Reserve Bank only for authorized access to a Reserve Bank's services and/or applications;
- (b) acknowledge that their Electronic Connection(s) and the Access Control Features can be used to originate funds transfer messages, other value transfer messages and non-value messages and should be appropriately restricted to ensure access is logically and physically limited to authorized staff;
- (c) except as otherwise provided in this Circular, assume sole responsibility and the entire risk of use and operation of their Electronic Connection(s) and the Access Control Features;
- (d) are responsible for unauthorized physical and network access to their Electronic Connection(s) and applicable Access Control Features and for implementing additional preventative and detective controls necessary to mitigate the risk of unauthorized physical and network access to their Electronic Connection(s) and applicable Access Control Features; and
- (e) are responsible for (i) establishing, instituting and enforcing policies and procedures for controlling, detecting and preventing unauthorized physical and network access to all applicable Access Control Features; (ii) immediately contacting the Reserve Bank in accordance with Section 1.4 herein if they have a reasonable basis to know or suspect that any applicable Access Control Feature is missing, has been compromised or shows evidence of tampering, and (iii) documenting within such policies

and procedures the requirement to immediately contact the Reserve Banks by telephone at (888) 333-7010, with written confirmation via email to [ccc.technical.support@kc.frb.org](mailto:ccc.technical.support@kc.frb.org).

Any Reserve Bank may act on any message that it receives through an Electronic Connection that the Reserve Bank authenticates as an Institution's directly (or an Institution's through its Service Provider, where applicable), using such technical protocols and procedures as the Reserve Bank shall establish in its sole discretion, as if the message consisted of a written instruction bearing the manual signature of one of the Institution's duly authorized officers.

## **5.2 RESERVE BANK LIABILITY**

The Reserve Banks are not liable for loss or damage resulting from a problem beyond their reasonable control. This includes, but is not limited to, (a) loss or damage resulting from any delay, error or omission in the transmission of any message to or from an Institution or its Service Provider; (b) alteration of any data, instruction or notice sent to or from a Reserve Bank through an Electronic Connection; (c) any third party's interception and/or use of any data conveyed using an Electronic Connection; (d) the services provided by an internet service provider; (e) Malware received from or introduced by any entity other than a Reserve Bank; (f) or technology provided by a Reserve Bank if the technology was not developed by a Reserve Bank, even if the Reserve Bank requires the use of such technology. Additionally, Reserve Banks are not liable for loss or damage resulting from unavailability of an Electronic Connection due to security or other concerns which the Reserve Banks, in their sole discretion, may conclude justify making such Electronic Connection unavailable, or from strikes, labor disputes or civil unrest, acts of war, riots, acts of terrorism, acts of God or acts of nature.

Further, the Reserve Banks are not liable for any loss or damage arising from an Institution's or its Service Provider's use of any Access Control Feature, or from a third party's reliance on any Access Control Feature, for any purposes other than those expressly authorized by a Reserve Bank. The Reserve Banks are not liable for any loss or damage arising from the theft or compromise of a private key or the password that protects a private key, whether detected or undetected, the storage of any private keys on an Institution's or its Service Provider's computer hard drive(s) or other storage device, or any loss caused by a third party's use or duplication of a private key.

Except as provided in Paragraph 4.3 of this Circular, a Reserve Bank shall be liable only to the Institution, only for losses that result from failure by the Reserve Bank or its employees to exercise ordinary care or act in good faith in providing the Electronic Connection, and only up to the amount of any fees paid to the Reserve Bank for the relevant Electronic Connection during the one month period immediately prior to the transaction or occurrence giving rise to the liability. In no event shall the Reserve Bank be liable for special, incidental, or consequential damages, even if such damages were foreseeable at the time of the Reserve Bank's failure to exercise ordinary care or act in good faith.

Except for a liability, claim or loss arising exclusively from the Reserve Bank's failure to exercise ordinary care or act in good faith in providing an Electronic Connection, and except to the extent prohibited by law or regulation, the

Institution shall indemnify, defend, and hold harmless the Reserve Bank with respect to any liability, claim or loss, whether alleged by the Institution, any customer of the Institution, its Service Provider or any third party, arising in connection with the use by the Institution (or its Service Provider or other agents) of the Electronic Connection. This indemnification shall survive the termination of access provided under this Agreement.

### **5.3 COMPLIANCE WITH RESERVE BANK STANDARDS**

An Institution and its Service Providers, if any, agree to use the Access Control Features, and agree to conform to the security procedures, operating instructions, guidelines, and specifications applicable to an Electronic Connection that a Reserve Bank specifies from time to time, including the need for the Institution and its Service Provider, if any, to exercise their own independent judgment about the adequacy of existing security measures and to implement additional security measures as necessary with respect to their own operating environments. Notwithstanding the above, the Institution and its Service Providers, if any, are required and agree to implement appropriate physical and logical security to protect the Access Control Features, Software, computer(s) and any associated equipment that are used to exchange data with a Reserve Bank from unauthorized use. THE RESERVE BANKS MAKE NO WARRANTIES WITH RESPECT TO THE FOREGOING OR OTHERWISE IN CONNECTION WITH THE USE OF AN ELECTRONIC CONNECTION, EXCEPT AS EXPRESSLY SET FORTH IN THIS CIRCULAR.

As further described in Section 3 of Appendix A, the Institution and its Service Providers, if any, shall (i) conduct, at least annually, a self-assessment of its adherence to the security procedures, operating instructions, guidelines, and specifications applicable to an Electronic Connection that a Reserve Bank specifies from time to time, as well as any additional security measures established by the Institution or Service Provider, and (ii) upon the request of the Reserve Bank, attest to its completion of such self-assessment in a form and manner acceptable to the Reserve Bank.

### **5.4 CONFIDENTIALITY OF RESERVE BANK PROPRIETARY AND SECURITY-RELATED INFORMATION**

“Confidential Information” shall include all information, provided in writing, electronically or orally, which is designated by Reserve Bank herein or by other means as “Confidential.” All security-related information, including information regarding Access Control Features and security procedures, whether or not it is labeled as “Confidential,” is hereby designated as “Confidential,” unless a Reserve Bank makes any such information generally available to the public (i.e., places it on its unrestricted public Web site or otherwise publishes it to the general public). Confidential Information contains trade secrets, proprietary information or security information of Reserve Banks or others. Unauthorized disclosure of Confidential Information likely would cause a Reserve Bank immediate and irreparable damage for which there may be no adequate remedy at law.

The Institution and its Service Provider, if any, agree to take all reasonable measures to protect and ensure the secrecy of and affirmatively avoid unauthorized disclosure and use of Confidential Information. Without limiting the

foregoing, the Institution and its Service Provider, if any, shall protect the Confidential Information with at least the same degree of care that the Institution uses to protect its own highly confidential information and comply with all handling instructions that are provided with the Confidential Information. The Institution and its Service Provider, if any, are responsible for destroying or returning any Confidential Information to Reserve Bank upon the request of Reserve Bank or when the Confidential Information is no longer needed.

The Institution and its Service Provider, if any, shall disclose the Confidential Information to their employees or third parties only on a “need to know” basis. The Institution and its Service Provider, if any, shall maintain a written record of all third parties to whom Confidential Information is disclosed (indicating the recipient, date and description of content of the disclosure), and shall provide such record to the Reserve Bank upon request. The Institution and its Service Provider must take all necessary steps to enforce the obligations of Paragraph 5.4 with their employees. Before disclosure to any third party, the Institution and its Service Provider, if any, must have a written agreement with such party sufficient to require that party to treat the Confidential Information in accordance with Paragraph 5.4. The Institution and its Service Provider, if any, are liable for any unauthorized disclosure of Confidential Information by any of their employees or third parties to whom they have disclosed Confidential Information.

In the event the Institution or its Service Provider become aware of any suspected or confirmed unauthorized disclosure or use of the Confidential Information, the Institution or Service Provider must immediately notify Reserve Bank in accordance with Section 1.4 herein of the suspected or confirmed unauthorized disclosure or use, and must take all reasonable efforts necessary to prevent further unauthorized disclosure or use.

## **5.5 MANAGEMENT OF ELECTRONIC CONNECTIONS**

- (a) An Institution or its Service Provider must manage its Electronic Connection(s) so as to permit the Reserve Banks to send data to the Institution or the Service Provider, and to permit the Institution or the Service Provider to receive data from the Reserve Banks, on a timely basis throughout the day. A Reserve Bank is not responsible for any delay in sending data (or for notifying any party of such a delay), if the delay results from the Institution's or its Service Provider's failure to so manage its connection(s), or from any cause other than the Reserve Bank's failure to exercise ordinary care or to act in good faith. The Reserve Bank's records shall be determinative of when data has been received by a Reserve Bank or when a Reserve Bank sends data to, or makes it retrievable by, the Institution or its Service Provider.
- (b) An Institution and its Service Provider, if any, are responsible for reviewing the current Reserve Bank hardware, software and connection requirements (“System Requirements”) on a regular basis and updating their operating systems accordingly. A Reserve Bank shall make best efforts to provide notice (which may be in electronic form) of changes to the System Requirements. An Institution or its Service Provider must also update in a timely manner all applicable workstation operating systems, anti-Malware software and any other software used in connection with or comprising the Institution's or its Service Provider's

Electronic Connections. The Reserve Banks shall not be responsible or liable in any manner for any loss or damage to an Institution or its Service Provider that could have been prevented had an update been installed when such update was made available by the applicable vendor. The Reserve Banks shall also not be responsible or liable in any manner for any loss or damage caused directly or indirectly by the installation of any such update whether or not the update was directly provided by a Reserve Bank.

## **5.6 CONTINGENCY PLANS FOR DISRUPTION OF ELECTRONIC CONNECTIONS**

Problems with hardware, software, or data transmission may on occasion delay or prevent a Reserve Bank from sending or receiving payments or other data electronically. Accordingly, an Institution and its Service Provider, if any, should be prepared to send or receive payments or other data by other means.

An Institution and its Service Provider agree to establish and regularly test business continuity and disaster recovery plans for use in the event of loss of a single or group of Electronic Connections to a Reserve Bank.

## **6.0 FEES AND TAXES**

### **6.1 ELECTRONIC CONNECTION FEES**

A Reserve Bank's fees relating to Electronic Connections (including, for example, installation support and training) are published separately and are subject to change on thirty (30) calendar days' prior notice. A Reserve Bank charges these fees to the Institution's (or its correspondent's) account on a Reserve Bank's books. By designating a Service Provider, an Institution agrees that the Service Provider may be billed directly by the Reserve Bank for any fees related to the Service Provider's Electronic Connection. Notwithstanding any such direct billing, the Institution shall remain liable for any unpaid fees.

### **6.2 OFF-LINE FEES DUE TO EQUIPMENT FAILURE**

If, because of a failure of an Institution's or its Service Provider's equipment, either a Reserve Bank or the Institution reverts to an off-line procedure, the Reserve Bank may charge off-line fees to the Institution.

### **6.3 LIABILITY FOR TAXES**

An Institution and its Service Provider, if any, are liable for the payment of any taxes, however designated, levied on its possession or use of equipment, services and/or applications or Software a Reserve Bank has supplied, including, without limitation, state and local sales, use, value-added and property taxes.



## **7.0 TERMINATION AND AMENDMENT**

### **7.1 TERMINATING THE ELECTRONIC ACCESS AGREEMENT**

An Institution may terminate its agreement to use Reserve Bank services and/or applications through an Electronic Connection and its agreement to the terms of this Circular by giving not less than thirty (30) calendar days' prior written notice to the Reserve Bank(s) with which it has Electronic Connections. A Reserve Bank may terminate an Institution's or its Service Provider's authority to use an Electronic Connection on similar notice. In addition, a Reserve Bank immediately may terminate an Institution's or its Service Provider's Electronic Connection if the Reserve Bank, in its sole discretion, determines that continued use of the Electronic Connection poses a risk to the Reserve Bank or others, or the Reserve Bank believes that the Institution or its Service Provider is in violation of this Circular.

The Reserve Bank, in its discretion, may restore the Electronic Connection when the Reserve Bank deems appropriate.

An Institution and its Service Provider, if any, are solely responsible for the proper operation of their electronic information systems. A Reserve Bank in its discretion may suspend or disconnect an Electronic Connection in the event that such access to the Reserve Bank's systems generates error conditions, causes denials or disruptions of the Reserve Bank's systems, or appears to have been compromised with respect to information security or integrity. In the event of any such suspension or disconnection, the Reserve Bank and the Institution and its Service Provider, if any, will cooperate to investigate, identify, and correct the problem or problems affecting access to the Reserve Bank's systems.

### **7.2 RETURN OF RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT AND SOFTWARE; SURVIVAL OF OBLIGATIONS**

Upon termination, an Institution and its Service Provider, if any, promptly must: (a) disable (by removing the battery or otherwise) any encryption card, or other card that supports encryption and communication, but only after the workstation has been disconnected from production network connections; (b) return all Reserve Bank supplied or designated equipment (or properly dispose of it, if a Reserve Bank authorizes it to do so); (c) destroy or return, as required herein any Software and Confidential information provided to the Institution and its Service Provider, if any; (d) delete as required herein any installed copies of such Software or saved copies of Confidential information; and (e) upon request of a Reserve Bank, provide written certification that all relevant Software and Confidential information has been destroyed and deleted. Notwithstanding the foregoing, the Reserve Bank retains the right to require that an Institution and its Service Provider, if any, promptly return all relevant Software, hardware and Confidential information upon termination. The Institution's and its Service Provider's obligations pertaining to confidentiality, nondisclosure and cooperation with a Reserve Bank's defense of any Software infringement claim survive any termination of the Institution's and its Service Provider's agreement to this Circular.

### **7.3 AMENDMENT OF CIRCULAR**

The Reserve Banks may amend this Circular at any time without prior notice. Any amendment applies immediately upon the effective date of the amendment.

### **8.0 FORUM, GOVERNING LAW AND TIME FOR ACTIONS**

The exclusive forum for any action involving a Reserve Bank for that Reserve Bank's acts or omissions arising under this Circular is in the United States District Court and Division where the head office of the Reserve Bank that committed the alleged act or omission is located and the Institution and its Service Provider, if any, hereby submit to the exclusive jurisdiction of such court. No action or claim relating to this Circular may be instituted more than one year after the event giving rise to such action or claim. This Circular is governed by Federal law and, to the extent not inconsistent therewith, the law of the State in which said Reserve Bank's head office is located, excluding that State's law regarding conflicts of law.

### **9.0 EFFECT OF THIS CIRCULAR ON PREVIOUS CIRCULAR**

This Circular amends and restates the Reserve Banks' Operating Circular 5 on Electronic Access dated June 30, 2021 and shall be effective on February 1, 2023.

# Operating Circular 5 Appendix A

## INFORMATION SECURITY PROGRAM

This Appendix sets forth the obligations of the Reserve Banks to Institutions and of Institutions to the Reserve Banks for implementation and ongoing operation of information security programs supporting the exchange of data between the Reserve Banks and Institutions according to the Reserve Bank Operating Circulars. By sending or receiving data to or from a Reserve Bank in accordance with an Operating Circular, Institutions agree to the terms of this Appendix A.

Section 1 of this Appendix states the general expectations and obligations of the Reserve Banks and Institutions with respect to information security. Section 2 describes the specific security procedures offered by the Reserve Banks to Institutions in order to detect unauthorized transactions. Section 3 describes the requirement that an Institution conduct a self-assessment with respect to its compliance with the Security Requirements (as defined therein) and the ability of the Reserve Banks to require the Institution deliver an attestation with respect to such self-assessment. Section 4 sets forth the liability of an Institution and a Reserve Bank with respect to this Appendix A. Section 5 describes the consequences to an Institution for failure to comply with this Appendix A. Terms not defined in this Appendix have the same meaning as defined in Operating Circular 5. For purposes of this Appendix A, references to “Institution” shall include any Service Providers for that Institution, although on occasion both an Institution and a Service Provider may be separately referenced for emphasis or clarity.

### 1.0 INFORMATION SECURITY

#### 1.1 Reserve Bank Program

The Reserve Banks have in place information security measures designed to protect the security of sensitive information, such as personally identifiable information and transaction records. These measures are intended to protect against threats or hazards to the security of such information and to protect against unauthorized access to or unauthorized use of such information that could result in substantial harm to Institutions. These measures are collectively referred to in this Appendix as the “Reserve Bank Program”.

The Reserve Bank Program is risk-based and informed by industry best practices, federal standards (including National Institute of Standards and Technology (“NIST”) standards), and relevant supervisory guidance (including Federal Financial Institutions Examination Council (“FFIEC”) guidance). The Reserve Bank Program is implemented in a manner consistent with the supervised nature of most Reserve Bank customers and the size and complexity of Reserve Bank operations. The Reserve Bank Program includes, among other things, technical, operational and/or procedural controls addressing:

- Access control
- Telecommunications and network security
- Governance and risk management
- Software development
- Cryptography
- Information security architecture and design
- Operations security
- Business continuity and disaster recovery planning
- Physical (environmental) security

THE RESERVE BANKS DO NOT MAKE ANY PROMISES, REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, THAT THE RESERVE BANK PROGRAM IS ABLE TO PREVENT UNAUTHORIZED TRANSACTIONS OR OTHER HARM TO INSTITUTIONS.

## 1.2 Institution Program

- (a) Each Institution agrees for itself and any Service Provider to implement technical, operational, managerial, and procedural controls designed to protect the security of the information technology (“IT”) environment, including systems (physical or virtual), and processes of or for the Institution and that are:
  - (i) used to access Reserve Bank services and applications (as described in section 1.2 of Operating Circular 5) or to send or receive data over an Electronic Connection; or
  - (ii) used to process, store, retransmit, or modify information received from those IT systems that use an Electronic Connection to exchange data or access Reserve Bank services and applications, including hardware, software, and access controls the Institution uses with its customers.
- (b) At a minimum, such technical, operational, managerial, and procedural controls shall not conflict with any part of the Reserve Bank Security Procedure selected for use by the Institution (see section 2.1(c) through 2.1(g) below), must be consistent with the controls described in section 4.1 below, and shall be consistent with guidance provided by the FFIEC, including its guidance regarding Authentication in an Internet Banking Environment.
- (c) Each Institution and any Service Provider shall include within its security breach related notification procedures and processes (e.g., within disaster recovery, hazard, business continuity, cyber security, and other appropriate procedures and processes) the obligation to immediately notify Federal Reserve Financial Services by telephone at (888) 333-7010, with

written confirmation via email at [ccc.technical.support@kc.frb.org](mailto:ccc.technical.support@kc.frb.org), in the event of a known, suspected, or threatened compromise, cyber event, fraud, malware detection, or other security incident or breach that would render the Electronic Connection vulnerable to misconduct.

## 2.0 SECURITY PROCEDURES RELATING TO UNAUTHORIZED TRANSACTIONS

### 2.1 Reserve Bank Security Procedures Generally

- (a) The Reserve Banks offer Institutions security procedures for the purpose of verifying the authenticity of transaction instructions that a Reserve Bank receives from the Institution (“Security Procedures”). The Security Procedures are designed for the purpose of verifying only that the instruction is that of the sender, i.e. the party identified in the transaction message as the party that sends the instruction to the Reserve Bank. The Security Procedures are not used to detect an error in the transmission or the content of an instruction. The Reserve Banks offer at least two Security Procedures for each Reserve Bank service but do not offer all Security Procedures for every service. A Security Procedure may be either On-Line or Off-Line.
- (b) The Institution is responsible for choosing a Security Procedure that is appropriate for the Institution taking into account, among other things, the nature and scale of the Institution’s business and the nature of its technical environment and information security policies and procedures.
- (c) The Reserve Banks have no obligation to verify, and expressly disclaim any responsibility for verifying, the authenticity of any party identified in a transaction instruction other than the party identified in the transaction instruction as the party that sends the instruction to the Reserve Bank.
- (d) Each On-Line Security Procedure is identified by the name of the Electronic Connection associated with the On-Line Security Procedure. Each of the On-Line Security Procedures consists of the following:
  - Security protocols embedded in the hardware and software associated with the equipment used by the Reserve Banks and by the Institution to initiate, transmit, and receive instructions;
  - Access controls that grant the Institution access to Reserve Bank services, such as identification codes, confidential passwords, and digital certificates;
  - Access controls that manage access rights of Reserve Bank employees and vendors to critical systems and infrastructure supporting Reserve Bank services; and
  - Encryption of instructions during the transmission process over a private network or virtual private network connection.

- (e) In addition, as part of each of the On-Line Security Procedures, the Reserve Banks (i) provide implementation guides and technical documents that prescribe policies, procedures, and controls that the Institution must follow and (ii) issue and manage access credentials in accordance with Operating Circular 5, including the applicable Certification Practice Statement. Each Institution is responsible for implementing the policies, procedures, and controls set forth in the applicable documentation provided to it by the Reserve Banks, as well as any subsequent modification to the policies, procedures and controls that are designed to strengthen the Security Procedures. If the Institution changes a default setting without prior written authorization from its Administrative Reserve Bank (as defined in Operating Circular 1) or fails to implement any other requirement in the documentation provided by the Reserve Banks, then the Institution is regarded as having unilaterally altered the Security Procedure and solely bears any resulting loss.
- (f) In addition, each Institution issuing or receiving instructions over an Electronic Connection must, as part of any On-Line Security Procedure, implement its own physical and logical security, as well as management controls, that appropriately protects the hardware, software, and access controls used in the transaction process from unauthorized access and use. An Institution that is sending instructions to a Reserve Bank must have controls in place to (i) ensure that initiation of instructions occurs only from locations authorized by the Institution and (ii) require action by more than one of its employees or authorized personnel of a Service Provider, using separate devices, to initiate any Fedwire® or National Settlement Service instruction.
- (g) Each Institution shall also prevent any disclosure, except on a “need to know” basis, of any aspects of the Security Procedure agreed to by it with the Reserve Bank holding its Master Account (as defined in Operating Circular 1). The Institution shall notify the Reserve Banks immediately in accordance with Section 1.4 of Operating Circular 5, if the confidentiality of the Security Procedures is compromised, and shall act to prevent the Security Procedure from being further compromised.
- (h) The Institution shall adopt policies and procedures that are designed to ensure the prompt management of compromised devices or fraudulent transactions.

## 2.2 Institution Verification Responsibility

Nothing in the Reserve Bank Security Procedures is intended to relieve an Institution from its responsibility to implement procedures for the purpose of verifying that a transaction instruction that the Institution receives is authorized, whether that responsibility stems from applicable law or is imposed by the Institution’s supervisor.

## 2.3 Security Procedures for Credit Transfers

- (a) In addition to the provisions set forth in section 2.1 above, with respect to funds transfers governed by Regulation J of the Board of Governors of the Federal Reserve System or Article 4A of the Uniform Commercial Code:

Before issuing a payment order to or receiving a payment order from a Reserve Bank, a sender or receiving bank, or its Service Provider, must execute a security procedure agreement with the Reserve Bank holding its Master Account in the form prescribed by the Reserve Bank. See, for example, Appendix A-1 to Operating Circular 6 if the payment order is a Fedwire® funds transfer; Appendix A-1 to Operating Circular 4 if the payment order is an ACH credit item; and Appendix A to Operating Circular 8 if the payment order is a FedNow<sup>SM</sup> Service transfer.

In addition, before sending a National Settlement Service settlement file to a Reserve Bank, a Settlement Agent must execute a security procedure agreement with the Host Reserve Bank (as defined in Operating Circular 12) in the form attached as Appendix B-1 to Operating Circular 12.

Before selecting a Security Procedure, a sender or a receiving bank may discuss with its Reserve Bank the various options offered by the Reserve Banks to determine which option best satisfies the sender's or receiving bank's business needs given the size, type, and frequency of payment orders normally issued by the sender to the Reserve Banks or received by the receiving bank from the Reserve Banks. Nothing in this Appendix requires a Reserve Bank to agree to a security procedure other than the standard Security Procedures offered by the Reserve Banks and described herein. If a Reserve Bank decides in its sole discretion to accept a nonstandard security procedure, then the Reserve Bank will only do so by executing a written agreement that has been previously signed by an authorized representative of the sender or receiving bank describing in detail the agreed upon Security Procedure.

- (b) Notwithstanding any other provision of this Appendix, when a sender or a receiving bank (or a Service Provider) chooses to use one of the Security Procedures, it rejects other Security Procedures, and if any one of the rejected Security Procedures is commercially reasonable for such sender or receiving bank, the sender or receiving bank agrees to be bound by any payment order, whether or not authorized, if it was issued in the sender's or the receiving bank's name and accepted by a Reserve Bank in compliance with the Security Procedure selected, subject to Section 4A-203 of Article 4A of the Uniform Commercial Code.
- (c) Off-Line Security Procedure

Fedwire® Funds Service: An Off-Line Security Procedure is available to any bank that issues or receives a payment order over the Fedwire Funds Service orally by telephone. An Off-Line Security Procedure may also be used when a bank that normally issues or receives a payment order over the Fedwire Funds Service by means of an encrypted communication using an On-Line Security Procedure is unable to do so because of an equipment or communications failure or other similar circumstances.

When a payment order is issued, the Off-Line Security Procedure involves the use of an identification code by an employee of the sender and may include a call-back or listen-back procedure by a Reserve Bank. When the Institution is acting as a receiving bank, the Off-Line Security Procedure involves the use of an identification code provided by a Reserve Bank to an employee of the receiving bank, and the receiving bank is required to call the Reserve Bank back to authenticate the payment order before making the proceeds available to its customer or otherwise acting with respect to the payment order.

The names of the employees of the sender or receiving bank who are authorized to issue or authenticate an Off-Line payment order must be provided to the Appropriate Reserve Bank (as defined in Operating Circular 6) by the sender or receiving bank desiring to set up an Off-Line Security Procedure. The list of authorized employees must be in writing and must be signed by an individual vested with authority to conduct business on behalf of the respective sender or receiving bank.

National Settlement Service: An Off-Line Security Procedure is available when a Settlement Agent (as defined in Operating Circular 12) that normally issues a Settlement Instruction (as defined in Operating Circular 12) by means of an encrypted communication using one of the On-Line Security Procedures is unable to do so because of an equipment or communications failure or other similar circumstances.

When a Settlement Instruction is issued, the Off-Line Security Procedure involves a telephone call initiated by an authorized employee of the Settlement Agent followed by the transmission by e-mail or facsimile of a Settlement Instruction signed (in the case of a facsimile) by an authorized employee of the Settlement Agent or sent from the e-mail address of an authorized employee of the Settlement Agent.

The names and e-mail addresses of the employees of the Settlement Agent who are authorized to issue a Settlement Instruction must be provided by the Settlement Agent to the Processing Reserve Bank (as defined in Operating Circular 12). The list of authorized employees must be in writing and must be signed by an individual vested with authority to conduct business on behalf of the Settlement Agent.



### 3. INFORMATION SECURITY PROGRAM ASSURANCE

#### 3.1 Self-assessment Requirements

Each Institution must at all times comply with the measures, protections, and requirements established under the Reserve Bank Program described in Section 1.1 of this Appendix A, the Institution Program described in Section 1.2 of this Appendix A, and any applicable Security Procedures (collectively, the “Security Requirements”).

Each Institution and, if applicable, any Service Provider, shall at least annually conduct a self-assessment of its compliance with the Security Requirements (“Self-Assessment”). The Self-Assessment may be calibrated based on an Institution’s analysis of the risks it faces. However, the Reserve Banks may in their discretion require that the Self-Assessment be conducted or reviewed by an independent third party, an internal audit function, or an internal compliance function.

#### 3.2 Attestation Requirements

Upon the request of the Reserve Banks which shall not exceed more than once during any consecutive 12-month period, each Institution and, if applicable, any Service Provider, shall attest to having completed a Self-Assessment by submitting an attestation in a form and manner acceptable to the Reserve Banks (“Attestation”). The Attestation sought by the Reserve Banks will generally include the following:

- (i) An acknowledgement of the Institution’s responsibility to adhere to the Security Requirements;
- (ii) A confirmation that the Institution has conducted a Self-Assessment within the time period requested by the Reserve Banks;
- (iii) If applicable, a confirmation 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 Requirements;
- (iv) If applicable, an acknowledgement that the Institution is responsible for its Service Provider’s compliance with the Security Requirements;
- (v) A statement that the Institution has remediation plans in place, including procedures to escalate concerns to the appropriate leaders within the

- Institution, to promptly address any areas of noncompliance with the Security Requirements; and
- (vi) An acknowledgement that the Institution must immediately notify the Federal Reserve Banks of any suspected or confirmed fraud, infringement, or security breach relating to any Electronic Connection.

### 3.3 Additional Assurance Requirements

In addition to the foregoing, the Reserve Banks may require one or more supplemental Self-Assessments and Attestations within any 12-month period if the Reserve Banks suspect that an Electronic Connection may be subject to compromise, attack, unauthorized use, or other circumstance that would render the Electronic Connection vulnerable to misconduct.

Each Institution shall maintain, consistent with its records management policy, the records of the Self-Assessment, the appropriate documentation supporting the results of the Self-Assessment, and a copy of the Attestation itself.

## 4. LIABILITY

### 4.1 Liability of Institution Relating to the Institution's Information Security Program and Assurance Requirements

Unless applicable law specifically requires otherwise, the Institution assumes all risk of loss, claim, or damage that results from the Institution's failure to adopt and implement an information security program consistent with section 1.2(a) and (b) above or that results from the failure to include any one or more of the below described technical, operational, managerial, and procedural controls, and the Institution shall indemnify, hold harmless, and defend the Reserve Banks for and against any such loss, claim, or damage (including reasonable attorneys' fees):

- Fraud detection and monitoring systems, processes or tools that take into account customer history and behavior and enable detection of suspicious transfers and procedures for responding in a timeframe that allows the Institution to eliminate or significantly reduce the risk of repeated fraudulent transactions or occurrences;
- Information security breach monitoring systems that detect anomalous events in the Institution's IT environment and/or in the data that is exchanged between the Institution and a Reserve Bank, and systems and procedures for responding to exceptions or anomalies in near real time;
- Controls, including limitations, prohibitions, or in-house multiple verification of any transactions that exceed risk tolerances established by the Institution with respect to dollar amounts of transactions, number or frequency of transactions,

destination of transfers, dates of transactions, time of day of transactions, or the risk profile that the Institution associates with the originator or receiver of a financial transaction;

- Customer education regarding fraud risk and mitigation techniques;
- Enhanced controls over account maintenance and configuration, particularly with respect to system administrators making access or application changes;
- Network and system controls to safeguard against the introduction of malicious code, including timely installation of all critical software patches and updates consistent with the requirements of section 4.8 of Operating Circular 5;
- Information retention procedures that handle backup media according to security practices no less secure than those applied to the Institution's production systems and connectivity;
- Disaster recovery and business continuity procedures that facilitate the timely recovery from a physical or cyber event;
- Network, system, and application segregation based on the criticality of such network, system, or application;
- Documented processes and procedures that govern the testing, validation, signoff, and implementation associated with changes to an information system before those changes are applied to critical software, systems, and networks; and
- Identity and access management practices that use appropriate forms of authentication based on the sensitivity of information accessed, adhere to need-to-know principles of information management, and are audited on a periodic basis.

In addition to any other losses borne by the Institution under this Circular (including this Appendix A), an Institution that fails to comply with the Security Requirements or to complete a Self-Assessment or submit an Attestation in accordance with the assurance requirements of Section 3 above agrees that it shall bear any loss to the Institution that directly or indirectly results from the Institution's failure to comply with these requirements or that could have been avoided had the Institution complied with these requirements.

#### 4.2 Liability of a Reserve Bank Relating to the Reserve Banks' Information Security Program

Unless applicable law specifically requires otherwise, a Reserve Bank shall be liable only to the Institution and only for losses that result solely and directly from the failure by the Reserve Banks to adopt and implement an information security program consistent with section 1.1 above. Unless applicable law specifically

requires otherwise, in no event shall a Reserve Bank be liable for any losses that result in whole or in part from an Institution's failure to adopt and implement an information security program consistent with sections 1.2(a) and (b) above and the controls in section 3.1 above.

## **5. FAILURE TO COMPLY WITH THIS APPENDIX A**

Failure of an Institution to comply with any part of this Appendix A, including but not limited to its obligations with respect to the Institution Program described in section 1.2 above, the Security Procedures described in section 2 above, and the Security Requirements, Self-Assessment requirements, and Attestation requirements described in section 3 above, is a violation of Operating Circular 5 that may result in the Reserve Banks taking any of the actions set out in section 7.1 of Operating Circular 5. At their discretion, the Reserve Banks may take other actions that they deem appropriate under the circumstances in response to the failure of an Institution to comply with any part of this Appendix A, including but not limited to disclosing the circumstances of noncompliance to the Institution's prudential regulator or other supervisory body in accordance with section 7.3 of Operating Circular 1, as well as executing limitations on user access and authentications, services, and reporting. Although the Reserve Banks will endeavor to provide advance notice to the Institution of taking any of these other actions, it has no obligation to do so and each Institution waives any and all rights to advance notice.

# Operating Circular 5

## Appendix B

### E-PAYMENTS ROUTING DIRECTORY SERVICE

This Appendix B sets forth the obligations of the Reserve Banks to Institutions, and of Institutions to the Reserve Banks, related to access through an Electronic Connection to the E-Payments Routing Directory Service as described in section 2.0 of this Appendix B. The E-Payments Routing Directory Service is an information service offered to Institutions through an Electronic Connection for the purpose of facilitating the processing and settling of Institutions' payment transactions. This Appendix B does not apply to access to the Directory through any publicly available search capabilities offered via a Reserve Bank's public website.

By using the E-Payments Routing Directory Service through an Electronic Connection, or by downloading or obtaining an Authorization Code for downloading the Directory through the E-Payments Routing Directory Service, Institutions (including their Service Providers) agree to the terms of this Appendix B. Terms not defined in this Appendix B have the same meaning as set forth in Operating Circular 5.

#### 1.0 DEFINITIONS

**Authorization Code** means an alpha-numeric code that can be inserted into a script or program, or other Access Control Feature established by the Reserve Banks from time to time, to allow Institutions and Authorized Users an automated, unattended electronic transfer of the Directory through an Electronic Connection.

**Authorized User** means a customer of an Institution that is authorized by the Institution to obtain access to the Directory through an Electronic Connection for the purpose of facilitating the Institution's processing and settling of payment transactions and that agrees to the Authorized User Terms in connection with receiving an Authorization Code from the Institution. An Authorized User may only obtain access to the Directory through utilization of an Authorization Code.

**Authorized User Terms** means the terms of an agreement between an Institution and an Authorized User, which shall require, at a minimum, that the Authorized User: (i) use the Directory solely for the purpose of facilitating the Institution's processing and settling of payment transactions; (ii) keep the Authorization Code confidential and not distribute the Authorization Code to any third party; (iii) terminate use of the Authorization Code as soon as the Authorized User no longer facilitates the Institution's processing and settling of payment transactions; (iv) acknowledge that the Authorization Code may expire or terminate at any time, with or without cause; (v) acknowledge that the Reserve Banks are not liable for any losses or damages of any kind arising in connection with the Authorized User's use, or inability to use, the Authorization Code or the E-Payments Routing Directory Service, (vi) not sell, relicense or distribute an Authorization Code or the Directory; and (vii) implement and maintain the controls and security measures, procedures, protocols and requirements as established from time to time in the operational documentation associated with the E-Payments Routing Directory Service.

**Directory** means the E-Payments Routing Directory that is maintained by the Federal Reserve Banks and containing routing information for the Fedwire® Funds Service, Fedwire Securities Service, and FedACH® transactions such as bank names, routing

and transit numbers, contact information, and other information determined by the Reserve Banks from time to time.

**E-Payments Routing Directory Service** means the service, as further described in Section 2.0 of this Appendix B, which provides access to the Directory through an Electronic Connection.

**Institution** means an Institution as defined in Operating Circular 5 together with any of its Service Providers (as defined in Operating Circular 5).

## **2.0 THE E-PAYMENTS ROUTING DIRECTORY SERVICE**

The E-Payments Routing Directory Service is a Reserve Bank information service which provides access to the Directory through an Electronic Connection. The E-Payments Routing Directory Service makes the Directory available to Institutions via a manual electronic transfer (i.e., download), or by utilization of an Authorization Code for an automated and unattended electronic transfer of the Directory. The Directory is available to Authorized Users only through utilization of an Authorization Code.

## **3.0 OBTAINING AND DISTRIBUTING AN AUTHORIZATION CODE**

An Authorization Code is needed in order to automate access to the Directory with a script or program. Only an Institution with an Electronic Connection is permitted to request and obtain an Authorization Code from a Reserve Bank. A Service Provider obtaining an Authorization Code from a Reserve Bank on behalf of an Institution agrees to the terms herein, as amended from time to time.

An Institution may distribute an Authorization Code to an Authorized User, provided that (i) the Authorized User agrees to terms of use consistent with the Authorized User Terms, (ii) the Authorization Code is distributed in a manner designed to prevent access to the Authorization Code by anyone not an Authorized User, and (iii) the Authorization Code is only distributed to those customers of the Institution that require access to the Directory for the purpose of facilitating the Institution's processing and settling of payment transactions.

A Reserve Bank may limit the number of Authorization Codes that it provides to any Institution or Service Provider, and may terminate any Authorization Codes or access to the E-Payments Routing Directory Service at any time in its absolute discretion and without notice, either generally or with respect to a specific Institution or Authorized User.

## **4.0 LIMITATIONS ON USE OF DIRECTORY**

An Institution may use the E-Payments Routing Directory Service solely for the purpose of facilitating the Institution's processing and settling of payment transactions.

An Institution is responsible for any use or misuse of the E-Payments Routing Directory Service by its Authorized Users, and it is responsible for ensuring that each Authorized User agrees to and complies with Authorized User Terms. An Institution that distributes an Authorization Code to an Authorized User remains responsible for all of the obligations of an Institution under this Appendix B for the Authorized User's use of the Authorization Code.

## **5.0 DISCLAIMER OF WARRANTIES; INDEMNIFICATION; LIMITATIONS OF LIABILITY**

- (A) THE RESERVE BANKS PROVIDE NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, TITLE, QUALITY, OR NONINFRINGEMENT OF THE E-PAYMENTS ROUTING DIRECTORY SERVICE OR ANY DATA OR INFORMATION CONTAINED IN THE DIRECTORY. THE E-PAYMENTS ROUTING DIRECTORY SERVICE, AND ALL INFORMATION, DATA, AND MATERIALS IN THE DIRECTORY, ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS WITHOUT WARRANTY OF ANY KIND.
- (B) THE RESERVE BANKS ARE NOT LIABLE FOR ANY DIRECT OR INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR FOR ANY OTHER KIND OF DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF REVENUES, BUSINESS INTERRUPTION, LOSS OF INFORMATION AND ATTORNEYS' FEES) THAT ARE IN ANY WAY DUE TO, RESULTING FROM, OR ARISING IN CONNECTION WITH THE USE OR PERFORMANCE OF, OR INABILITY TO USE FOR ANY REASON (INCLUDING AS A RESULT OF TERMINATION OF ACCESS), THE E-PAYMENTS ROUTING DIRECTORY SERVICE, REGARDLESS OF WHETHER THE RESERVE BANKS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, INCLUDING LIABILITY FOR ANY VIRUSES THAT MIGHT INFECT A USER'S COMPUTER SYSTEM.
- (C) To the maximum extent permitted by law, Institutions (which includes their Service Providers) release from any and all liability, and waive all claims against, the Reserve Banks and their officers, directors, employees, and agents for claims, losses, damages (whether actual and/or consequential), costs, and expenses (including litigation costs and reasonable attorneys' fees) arising from or in any way related to their use of (or inability to use) the E-Payments Routing Directory Service, any use or distribution of an Authorization Code, the use of (or inability to use) the E-Payments Routing Directory Service by their Authorized User, or any use (whether authorized or unauthorized) of the E-Payments Routing Directory Service by a third party where such usage derives from the Institution's distribution of an Authorization Code. Institutions agree to indemnify and hold harmless the Reserve Banks and their officers, directors, employees, and agents from and against any and all liability for claims, losses, damages (whether actual and/or consequential), costs, and expenses (including litigation costs and reasonable attorneys' fees) arising from or in any way related to their use of (or inability to use) the E-Payments Routing Directory Service or an Authorization Code, distribution of the Authorization Code to an Authorized User, and/or the use of (or inability to use) the E-Payments Routing Directory Service by the Institution's Authorized User, including any violation of this Appendix B by an Institution, by its Authorized User, or by any third party where such violation derives from the Institution's distribution of the Authorization Code.

## **6.0 FEES**

A Reserve Bank's fees relating to the issuance of an Authorization Code or the ability to receive, view or download the Directory through the E-Payments Routing Directory Service are published separately (together with other information about Reserve Bank financial services) and are subject to change from time to time.

## **7.0 AMENDMENTS AND TERMINATION**

In addition to the amendment and termination provisions relating to Electronic Access set forth in Operating Circular 5, the Reserve Banks may amend or terminate the E-Payments Routing Directory Service, including any Authorization Code, at any time without prior notice, either generally or with respect to a specific Institution, Service Provider or Authorized User.