THE FEDERAL RESERVE
Financial Services

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

# GENERAL FINANCIAL SERVICE PROVISIONS*

**Effective December 11, 2026**

Deleted: May15

* Operating Circular 5, previously titled *Electronic Access*, was renamed *General Financial Service Provisions*, effective January 5, 2026. All references in Federal Reserve Bank materials to Operating Circular 5 regardless of the title referenced shall be deemed a reference to this Operating Circular 5, as retitled.

**FEDERAL RESERVE BANKS**
**OPERATING CIRCULAR NO. 5**

**TABLE OF CONTENTS**


**1.0 INTRODUCTION ---- 4**

PART A – GENERAL TERMS

**2.0 GENERAL TERMS FOR ALL FINANCIAL SERVICES ---- 4**

*2.1 DEFINITIONS ---- 4*

*2.2 GOVERNING LAW; FORUM AND TIME FOR ACTIONS ---- 6*

*2.3 SERVICE PROVIDERS ---- 6*

*2.4 USE, DISCLOSURE, AND SHARING OF INFORMATION THROUGH FINANCIAL SERVICES ---- 7*

*2.5 RISK MANAGEMENT FOR SUPPORTING SERVICES ---- 8*

*2.6 TERMINATING USE OF A FINANCIAL SERVICE ---- 8*

*2.7 RECOVERY, RESILIENCE, AND TESTING ---- 10*

*2.8 FEES ---- 12*

*2.9 LIABILITY FOR TAXES ---- 12*

*2.10 CONFIDENTIALITY OF RESERVE BANK PROPRIETARY AND SECURITY-RELATED INFORMATION ---- 12*

*2.11 AMENDMENT OF CIRULARS; EFFECT OF PRIOR OPERATING CIRCULARS ---- 13*

***PART B – SUPPORTING SERVICES***

**3.0 SUPPORTING SERVICE – ELECTRONIC ACCESS ---- 14**

*3.1 SERVICES ACCESSIBLE VIA ELECTRONIC CONNECTIONS ---- 14*

*3.2 INSTITUTION'S SECURITY OBLIGATIONS ---- 14*

*3.3 PRIOR APPROVAL OR NOTICE REQUIREMENTS FOR ELECTRONIC CONNECTIONS ---- 15*

*3.4 INSTITUTION'S EQUIPMENT AND SOFTWARE ---- 16*

*3.5 AVAILABLE ELECTRONIC CONNECTIONS ---- 16*

*3.6 EQUIPMENT DELIVERY, INSTALLATION, AND ALTERATIONS ---- 16*

*3.7 ELECTRONIC CONNECTION TO NETWORK; SOFTWARE ---- 17*

*3.8 SOFTWARE LICENSE ---- 17*

*3.9 ELECTRONIC CONNECTION RESTRICTIONS ---- 17*

*3.10 DISCLAIMER OF WARRANTY ---- 18*

*3.11 UNAUTHORIZED DISCLOSURE OR USE OF SOFTWARE ---- 19*

*3.12 RESERVE BANK'S MALWARE PROTECTION ---------- 19*
*3.13 INSTITUTION'S AND SERVICE PROVIDER'S MALWARE PROTECTION ---------- 19*
*3.14 RESPONSIBILITY FOR ACCESS CONTROL FEATURES ---------- 20*
*3.15 RESERVE BANK LIABILITY ---------- 21*
*3.16 COMPLIANCE WITH RESERVE BANK STANDARDS ---------- 21*
*3.17 MANAGEMENT OF ELECTRONIC CONNECTIONS ---------- 22*
*3.18 DESTRUCTION, DELETION, OR RETURN OF RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT AND SOFTWARE; SURVIVAL OF OBLIGATIONS --- 23*

**4.0 SUPPORTING SERVICE – E-PAYMENTS ROUTING DIRECTORY ---------- 23**
*4.1 DEFINITIONS ---------- 23*
*4.2 THE E-PAYMENTS ROUTING DIRECTORY SERVICE ---------- 24*
*4.3 OBTAINING AND DISTRIBUTING AN AUTHORIZATION CODE ---------- 24*
*4.4 LIMITATIONS ON USE OF DIRECTORY ---------- 25*
*4.5 DISCLAIMER OF WARRANTIES; INDEMNIFICATION; LIMITATIONS OF LIABILITY ---------- 25*

**5.0 SUPPORTING SERVICE – EXCEPTION RESOLUTION SERVICE ---------- 26**
*5.1 DEFINITIONS ---------- 26*
*5.2 ERS GENERALLY ---------- 27*
*5.3 ENROLLMENT; TYPES OF PARTICIPANTS ---------- 27*
*5.4 EXCEPTION CASES; REPORTS PROVIDED BY THE RESERVE BANKS ---------- 27*
*5.5 USE AND STORAGE OF INFORMATION BY THE RESERVE BANKS ---------- 28*
*5.6 DESIGNATION OF AUTHORIZED USERS, EMAIL ADDRESSES, AND SERVICE PROVIDERS ---------- 28*
*5.7 UNENROLLMENT ---------- 28*
*5.8 USE AND DISCLOSURE OF INFORMATION ---------- 29*
*5.9 LIABILITY ---------- 29*

**6.0 SUPPORTING SERVICE – PAYEE NAME VERIFICATION SERVICE ---------- 30**
*6.1 DEFINITIONS ---------- 30*
*6.2 PNV GENERALLY ---------- 30*
*6.3 TRANSMISSION OF INFORMATION; SERVICE PROVIDERS; INACCURATE INFORMATION ---------- 31*
*6.4 RELATION TO THE RESERVE BANKS' SECURITY PROCEDURES AND OTHER INFORMATION SECURITY REQUIREMENTS ---------- 31*
*6.5 LICENSE GRANT, CUSTOMER USE AND NONDISCLOSURE OF INFORMATION 31*
*6.6 LIABILITY ---------- 32*

**7.0 SUPPORTING SERVICE – API SERVICE ---------- 33**

*7.1 DEFINITIONS ---- 33*
*7.2 REGISTRATION ---- 34*
*7.3 LICENSES AND OWNERSHIP ---- 34*
*7.4 POLICIES AND RESTRICTIONS ---- 35*
*7.5 USE OF MARKS ---- 39*
*7.6 ADDITIONAL RESPONSIBILITIES ---- 39*
*7.7 FEES ---- 41*
*7.8 REPRESENTATIONS AND WARRANTIES ---- 41*
*7.9 YOUR FEEDBACK ---- 41*
*7.10 TERM AND TERMINATION ---- 42*
*7.11 CONFIDENTIALITY ---- 42*
*7.12 DISCLAIMERS ---- 43*
*7.13 LIMITATION OF LIABILITY ---- 43*
*7.14 INDEMNIFICATION ---- 44*
*7.15 GOVERNMENT USE ---- 44*
*7.16 ASSIGNMENT ---- 44*
*7.17 NO AGENCY, PARTNERSHIP, OR JOINT VENTURE ---- 44*
*7.18 GOVERNING LAW AND FORUM FOR LEGAL DISPUTES ---- 44*
*7.19 WAIVER AND SEVERABILITY ---- 45*
*7.20 PUBLICITY ---- 45*
*7.21 UPDATES TO API TERMS ---- 45*
*7.22 EMAIL NOTICE ---- 45*
*7.23 EXPORT RESTRICTIONS ---- 45*

**APPENDIX A – INFORMATION SECURITY PROGRAM ---- *47***

## 1.0 INTRODUCTION

This Operating Circular 5 sets forth (i) the terms under which the Reserve Banks provide Institutions and their Service Providers with access to certain services and applications provided by a Reserve Bank, including electronic connections under which an Institution or its Service Provider may send certain data to or receive certain data from a Reserve Bank; and (ii) other general terms applicable across all financial services provided by a Reserve Bank. Each Reserve Bank has issued an Operating Circular 5 identical to this one.

By obtaining, participating, or accessing a Financial Service or Supporting Service (as defined below), Institutions and their Service Providers or other agents agree to the terms set forth in this Operating Circular 5, any applicable CPS, and all applicable Financial Service Operating Circulars or other separate agreements governing the use of such applications or services, as each may be amended from time to time. In the event of any inconsistency between this operating circular and any other Financial Service Operating Circular, agreement, or instruction governing a particular Financial Service (other than an Electronic Connection or other Supporting Service described in this operating circular), such other Financial Service Operating Circular, agreement or instruction controls.

The Institution and its Service Provider, if any, agrees that the Financial Service Operating Circulars and other agreements referenced in this Section, including any modifications and amendments thereto, may be agreed to in electronic form.

Each reference in a Financial Service Operating Circular to another Reserve Bank operating circular or other agreement, technical and operational requirements, procedures, rules, regulations, guides, schedules, or the like shall mean such item including all of its appendices, and as amended from time to time.

# PART A – GENERAL TERMS

## 2.0 GENERAL TERMS FOR ALL FINANCIAL SERVICES

### 2.1 DEFINITIONS

**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.

**Administrative Reserve Bank** means the Reserve Bank in whose Federal Reserve district an entity is located, as determined under the procedure described in 12 CFR Part 204, even if the entity is not otherwise subject to that chapter, or if the entity maintains an account on the books of a different Reserve Bank, the Reserve Bank at which the entity maintains an account.

**Appropriate Reserve Bank Staff** means Reserve Bank staff identified by the Reserve Banks as the staff with which an Institution should communicate on particular matters related to a Financial Service or any other Reserve Bank services or applications.

**Business Day** means, with respect to each Financial Service, a day on which the Financial Service is open for business, as set forth in the relevant Financial Service Operating Circular for that Financial Service. For the purpose of the FedNow Service, a Business Day is a Standard Business Day as defined in Operating Circular 8.

**CPS** means any Certification Practice Statement applicable to the Electronic Connection used by the Institution as published on the FRBservices.org® website or such other location designated by the Federal Reserve Banks.

**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.

**Financial Service** means the FedACH® Services, Federal Reserve Check Services, Fedwire® Funds Service, Fedwire Securities Service, FedNow® Service, FedCash® Services, National Settlement Service, or any Supporting Service.

**Financial Service Operating Circular** means Operating Circular 2, 3, 4, 5, 6, 7, 8, or 12.

**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 authorized by any Federal Reserve Bank to use an Electronic Connection for submitting regulatory reports, applications and information or for software testing.

**Malware** means malicious code such as computer viruses, trojans, worms, or other defects that might disrupt the operations of computers or software.

**Master Account** means a means a "Master Account" as defined in Operating Circular 1.

**Message** means each item, value or nonvalue message, advice, acknowledgement, payment order, entitlement order, notice or other communication sent, received, processed, or otherwise transmitted to or from a Reserve Bank through or in connection with a Financial Service.

**Reserve Bank** means any Federal Reserve Bank.

**Service Provider** means any entity, other than a Reserve Bank, that uses an Electronic Connection on behalf of an Institution.

**Software** means all software, including upgrades, modifications, applets and hypertext markup language ("HTML"), as well as any other code required by the Federal Reserve Banks to be deployed (regardless of where located) 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.

**Supporting Service** means any service performed by a Reserve Bank under a Financial Service Operating Circular that is incidental or ancillary to one or more Financial Services that is a payment, clearing, or settlement service. An Electronic Connection is a Supporting Service, but a Master Account or other account maintained with a Reserve Bank is not.

## 2.2 GOVERNING LAW; FORUM AND TIME FOR ACTIONS

**2.2.1** This operating circular shall be governed by federal law and, to the extent not inconsistent therewith, the law of the state in which head office of the Institution or Service Provider's Administrative Reserve Bank is located, excluding that state's law regarding conflicts of law.

**2.2.2** An Institution or Service Provider may bring legal action against a Reserve Bank only for an act or omission in providing a Financial Service. An Institution or Service Provider must bring such legal action in the U.S. District Court with jurisdiction over the main office of the Administrative Reserve Bank within one calendar year from the date of the transaction or occurrence that gives rise to the claim. Each Institution or Service Provider hereby submits to the exclusive jurisdiction of such court.

## 2.3 SERVICE PROVIDERS

By accessing any services 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 operating circular applicable to Service Providers. For purposes of the CPS, a Service Provider may be a Participant 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 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 operating circular or the provisions of any separate agreement governing the use of a particular Financial 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; (iii) its Service Provider may issue instructions and transact business with a Reserve Bank, including the provision of new or modified services, and the Reserve Bank may rely on such instructions and actions as fully authorized by the Institution; and (iv) 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. The Institution authorizes a Reserve Bank to share all data and information with an Institution's Service Provider to the same extent such data and information may be shared directly with the Institution, and the Institution's Service Provider authorizes a Reserve Bank to share all data and information with the Institution to the same extent such data and information may be shared directly with the Service Provider.

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.

## 2.4 USE, DISCLOSURE, AND SHARING OF INFORMATION THROUGH FINANCIAL SERVICES

**2.4.1** Each Institution that uses or accesses a Financial Service acknowledges that the Reserve Banks may use, disclose, or share information collected by the Reserve Banks in providing the Financial Service as prescribed in the Reserve Banks' Operating Circular 1 and as may be further prescribed in the Financial Service Operating Circulars.

**2.4.2** Each Institution that enables, uses, or accesses a Financial Service acknowledges that in connection with providing the Financial Service, the

Reserve Banks will use and disclose information collected in operating the Financial Service consistent with the exceptions to consumer notice and optout rights outlined in the Consumer Financial Protection Bureau's Regulation P (12 CFR part 1016). This includes but is not limited to using and sharing information in:

(a) Accepting or rejecting any Messages sent through the Financial Service;

(b) Remediating, investigating, and preventing exceptions that might arise, such as actual or potential errors or fraudulent activity, including by providing notifications or transaction-related reports to the Institution;

(c) Developing data models, analytical reports, and controls that may be used in operating any Financial Service; and

(d) Otherwise operating the Financial Services.

**2.4.3** Each Institution that uses or accesses a Financial Service shall obtain consent from its customers and make related customer disclosures in connection with the use and disclosure of information by it, a Reserve Bank, or another Institution through the Financial Service in accordance with the terms applicable to the Financial Service.

**2.4.4** Each Institution that shares information with the Reserve Banks through a Financial Service warrants that it is authorized to share such information with the Reserve Banks and the Reserve Banks are authorized to use and disclose such information in accordance with the terms applicable to the Financial Service, in each case without further consent of or disclosure to any person.

## 2.5 RISK MANAGEMENT FOR SUPPORTING SERVICES

Each Institution that uses a Supporting Service as part of its own risk management processes and procedures is responsible for determining how best to use such Supporting Service in accordance with its own risk tolerance and any requirements applicable to it.

## 2.6 TERMINATING USE OF A FINANCIAL SERVICE

**2.6.1** An Institution or Service Provider may terminate its use of or access to a Financial Service or other Reserve Bank service or application, unless otherwise required or agreed to in another Financial Service Operating Circular or other Reserve Bank agreement. Termination shall not be effective until after Appropriate Reserve Bank Staff have received a written request and the later of (i) a reasonable opportunity for the Reserve Banks to act on the termination request, or (ii) ten Business Days' after receiving the written request.

**2.6.2** A Reserve Bank may terminate or restrict an Institution's or Service Provider's use of or Electronic Connection to a Financial Service or other Reserve Bank application or service at any time upon notice to the

Institution and its Service Provider. A Reserve Bank is not obliged to but will endeavor to give such notice at least five Business Days' in advance of terminating or restricting the Institution's or Service Provider's use of or access to the Financial Service or other Reserve Bank application or service.

**2.6.3** In addition, unless specifically provided otherwise with respect to a particular Financial Service, a Reserve Bank may terminate, suspend, or restrict an Institution or Service Provider's use of or access to a Financial Service or other Reserve Bank application or service at any time without notice if the Reserve Bank has reason to believe that the Institution or Service Provider's use of or access to the Financial Service or other Reserve Bank application or service does not comply with any Reserve Bank agreement, including this operating circular or any other applicable Financial Service Operating Circular, or applicable law, or otherwise poses risk to a Reserve Bank, any Institution, or the security or proper functioning of any Financial Service or other Reserve Bank service or application.

**2.6.4** Actions by a Reserve Bank under this Section 2.6 to restrict an Institution or Service Provider's use of or access to a Financial Service or other Reserve Bank application or service may include, among others, restricting the ability to send or receive Messages or other information through a Financial Service; restricting access through or use of one or more Electronic Connections; delaying the release to a Financial Service application of Messages or other information sent through an Electronic Connection; restricting access by one or more individuals authorized to use a Financial Service on an Institution's behalf; and imposing, modifying, or restricting modifications to one or more of the profile settings or processing options described in a Financial Service Operating Circular or in Reserve Bank operating procedures.

**2.6.5** In the event of any termination, suspension, or restriction under this Section 2.6, the Reserve Bank and the Institution or its Service Provider will cooperate to investigate, identify, and correct the problem or problems affecting the Institution or Service Provider's use of or access to a Financial Service or other Reserve Bank applications or services. The Reserve Banks may, in their discretion, impose conditions before restoring the Institution or Service Provider's use of or access to the Financial Service or other Reserve Bank application or service after the correction of such problem or problems.

**2.6.6** Termination of a Financial Service or feature by the Reserve Banks or termination of an Institution or Service Provider's use of or access to a Financial Service or other Reserve Bank service or application under this Section 2.6 terminates its agreements with the Reserve Banks with respect to that Financial Service or other Reserve Bank application or service, including any applicable Financial Service Operating Circulars. The provisions of such agreements pertaining to confidentiality, nondisclosure, cooperation with a Reserve Bank's defense of any claim (including any Software infringement claim), intellectual property, indemnification, warranties, exclusions and limitations of damages and liability, governing law, legal actions, and any other obligation that, by its

nature, cannot be fully performed prior to termination, survive termination of such agreements. Termination of an Institution's use of or access to a Financial Service or other Reserve Bank service or application or its agreements with respect to such Financial Service or other Reserve Bank service or application does not affect an Institution's responsibility for any liability or obligation to the Reserve Banks or another party arising under the agreements or applicable law, even if the liability or obligation is contingent or unmatured at the time of termination.

## 2.7 RECOVERY, RESILIENCE, AND TESTING

**2.7.1** Each Institution shall develop, implement, and maintain its own business contingency and recovery plans, such as back-up hardware, software, data transmission capabilities, and operations facilities, to ensure its ability to continue its operations for each Financial Service that it accesses in the event of equipment failure or other operational interruption. At a minimum, these contingency and recovery plans shall meet applicable regulatory and supervisory standards, and shall be designed to help ensure an Institution meets the Reserve Banks' availability expectations even in a contingency event. The Reserve Banks assume no responsibility for providing any back-up access facilities.

**2.7.2** Each Institution, or its Service Provider, must notify the Reserve Banks promptly of any disruption of the Institution's Electronic Connection that prevents the Institution from using a Financial Service.

**2.7.3** In the event of an emergency or failure of Reserve Bank hardware, software, data transmission capabilities, or operational facilities, Messages or other information may be delayed until the emergency or failure is resolved. During a disruption, applications or operations related to a Financial Service may be relocated to alternate production sites and certain services or features may be unavailable. The Reserve Banks will endeavor to provide Institutions and their Service Providers with information about such emergency or failure, and any related disruption, through FRBservices.org or otherwise. Institutions and their Service Providers and agents must be prepared to obtain instructions from the Reserve Banks under such circumstances as well as follow any applicable Reserve Bank instructions set forth in operating procedures for the Financial Service, through FRBservices.org, or otherwise. Institutions and their Service Providers and agents must refer to the Reserve Banks' business continuity guides, operating procedures, and this operating circular regarding actions to take to prepare for, and their requirements and responsibilities during, contingency operations.

**2.7.4** Each Institution shall be prepared to reconcile its activities over a Financial Service up to the point of the emergency or failure.

**2.7.5** The Reserve Banks process Messages in accordance with their processing schedules and as set forth in the relevant Financial Service Operating Circular. If, because of circumstances beyond a Reserve Bank's control, a Reserve Bank is delayed beyond the applicable time limit in acting on a Message, the time for acting is extended to the extent

permitted under applicable law.

**2.7.6** The Reserve Banks may require an Institution to (i) test its ability to continue to access and use any Financial Service following Reserve Bank prescribed contingency scenarios and (ii) establish and periodically test an additional Electronic Connection through which the Institution may send or receive Messages or other information. In determining whether an Institution is subject to these requirements, the Reserve Banks may consider, among other factors, the aggregate value, aggregate volume, or purpose of Messages sent and received by that Institution or the Financial Services the Institution uses.

**2.7.7** Unless otherwise permitted by the Reserve Banks, each Institution shall test its ability to access or use a Financial Service before it first accesses or uses the Financial Service or the Institution or its Service Provider, if any, makes changes to their hardware, software, data transmission capabilities, or operations that might affect the Institution's ability to continue to access and use the Financial Service. Each Institution shall, as directed by the Reserve Banks, test its ability to continue to access and use the Financial Service (i) in advance of changes the Reserve Banks make to hardware, software, data transmission capabilities, or operations that may affect the Financial Service or (ii) if the Reserve Banks believe that such testing is necessary to ensure that the Institution is properly accessing or using the Financial Service.

**2.7.8** An Institution that sends Messages in connection with testing its ability to use or access a Financial Service, including Messages sent in a test environment offered by the Reserve Banks, shall comply with Reserve Bank instructions on identifying such Messages as test Messages. An Institution that receives test Messages shall handle them as test Messages. Unless otherwise permitted by the Reserve Banks, Institutions shall not introduce any sensitive or personally identifiable information in any test environment. Any data shared by an Institution or its Service Provider into a test environment may be shared with other Institutions, Service Providers, and agents.

**2.7.9** The obligations in this Section apply to all Institutions regardless of whether an Institution accesses the Financial Service directly or by using a Service Provider. The Reserve Banks may require an Institution's Service Provider to participate in any testing required under this Section.

**2.7.10** The Reserve Banks are not liable for any loss or damage that might arise because an Institution or its Service Provider fails to perform its obligations under this Section or any recovery, resiliency, and testing obligations applicable to a particular Financial Service as set forth in another Financial Service Operating Circular. Except to the extent prohibited by law, each Institution and Service Provider and other agent of an Institution shall indemnify and hold the Reserve Banks harmless against any claim, loss, cost, or expense (including but not limited to attorneys' fees and expenses of litigation) that arise because the Institution or its Service Provider fails to perform its obligations as specified in this Section.

## 2.8 FEES

The fees imposed for any Financial Service are listed in the Reserve Banks' fee schedules published on the FRBservices.org website. The Reserve Banks may change the published fees from time to time, provided that written notice of any such changes will be published before the effective date thereof.

To settle Financial Service fees, a Reserve Bank may debit, on a schedule determined by the Reserve Banks, (i) the Institution's Master Account or (ii) the Master Account of the Institution's Correspondent (as defined in Operating Circular 1) if the Institution has completed the Reserve Banks' forms to establish such a relationship.

An Institution that designates a Service Provider to operate or manage an Electronic Connection on its behalf agrees that the Service Provider may be billed directly by the Reserve Bank for any fees related to the Service Provider's Electronic Connection, which may be settled in a Master Account designated by the Service Provider. Notwithstanding any such direct billing, the Institution shall remain liable for any unpaid fees.

If, because of a failure of an Institution's or its Service Provider's equipment, the Reserve Bank offers an alternative procedure to the Institution for sending or receiving Messages or other information, the Reserve Bank may charge fees to the Institution to recover costs incurred by the Reserve Banks in providing such alternative procedure to the Institution.

## 2.9 LIABILITY FOR TAXES

All fees and charges quoted are exclusive of applicable taxes and duties. An Institution and its Service Provider, if any, are liable for the payment of any taxes assessed in connection with a Financial Service, however designated, including any taxes levied on its possession or use of equipment, services or applications, or Software a Reserve Bank has supplied, including, without limitation, state and local sales, use, value-added, and property taxes.

## 2.10 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 this Section 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 this Section. 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 becomes 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 3.2 herein of the suspected or confirmed unauthorized disclosure or use, and must take all reasonable efforts necessary to prevent further unauthorized disclosure or use.

### 2.11 AMENDMENT OF CIRULARS; EFFECT OF PRIOR OPERATING CIRCULARS

The Reserve Banks may amend the Operating Circulars at any time without prior notice. Revisions to Operating Circulars shall take effect on the date indicated as the effective date of the revision, at which time any earlier version of the Operating Circular shall no longer be in effect.

*[Part B begins on next page]*

## PART B – SUPPORTING SERVICES

## 3.0 SUPPORTING SERVICE – ELECTRONIC ACCESS

This Section 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).

### 3.1 SERVICES ACCESSIBLE VIA ELECTRONIC CONNECTIONS

The Reserve Banks offer a variety of financial services which may be accessed using an Electronic Connection, including, for example, transfers of funds and securities, settlement services, check and automated clearing house transactions, cash and savings bond services, Treasury securities services, and others. The transmission of data to or from a Reserve Bank and an Institution or its Service Provider in connection with these services, including the transmission of any data through an application programming interface, occurs through an Electronic Connection.

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 or applications using an Electronic Connection.

### 3.2 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. An Institution and its Service Provider, if any, are solely responsible for the proper operation of their electronic information systems.

The Institution or its Service Provider must immediately notify the Support Center by telephone at 833-FRS-SVCS (833-377-7827), with written confirmation via email at 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:

(a) 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;

(b) impacts or may impact software or data stored on servers or other electronic media shared with Reserve Bank data or applications;

(c) 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;

(d) caused or may have caused the Institution or its Service Provider to generate an unauthorized transaction;

(e) causes or may cause the Institution or Service Provider to modify its operations while investigating or mitigating the impact of the event;

(f) 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;

(g) resulted in or may have resulted in the loss of, unauthorized access to, compromise of, or tampering with an Access Control Feature; or

(h) resulted or may have resulted in the unauthorized disclosure or use of Confidential Information or the Security Procedures described in Appendix A.

A Reserve Bank may share any data and information regarding a cyber event, fraud, malware detection, compromise, or other security incident or breach with (i) a governmental, administrative, or regulatory organization, and (ii) to the extent the Reserve Bank determines in its discretion that such event manifests the potential for contagion among financial institutions, a security/resiliency industry organization.

### 3.3 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 operating 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 operating circular.

### 3.4 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 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.

### 3.5 AVAILABLE ELECTRONIC CONNECTIONS

An Institution or its Service Provider may choose from certain Electronic Connections that a Reserve Bank makes available 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.

### 3.6 EQUIPMENT DELIVERY, INSTALLATION, AND ALTERATIONS

A Reserve Bank may, at its option, arrange for the delivery and 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.

### 3.7 ELECTRONIC CONNECTION TO NETWORK; SOFTWARE

The Reserve Banks require the use of specified Access Control Features to establish an Electronic Connection, and 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.

### 3.8 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 operating 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.

### 3.9 ELECTRONIC CONNECTION RESTRICTIONS

In addition to restrictions contained in Section 3.6, an Institution or its Service Provider may not, except with a Reserve Bank's prior written consent:

(a) situate any network communication device (e.g., VPN or WAN device) used in conjunction with an Electronic Connection in any location other than the Institution's or its Service Provider's premises. However, a network communication device may be located off premises in a secure facility designed specifically for the sole purpose of housing and supporting servers and other physical electronic equipment, provided that (i) all security obligations required by a Reserve Bank with respect to the network communication device are met, (ii) the Institution or its Service Provider will give the Reserve Bank physical access to the device upon request; (iii) the Reserve Bank is at all times informed of the exact location of the device, and (iv) the Reserve Bank in its discretion is satisfied that the facility adequately secures and protects the device, or is otherwise generally acceptable as an off premises facility;

(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.

**3.10 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 OR IN COMPLIANCE WITH ANY RECOMMENDATIONS, SECURITY PROCEDURES, OPERATING INSTRUCTIONS, USER MANUALS, GUIDELINES, OTHER DOCUMENTATION, AND SPECIFICATIONS FOR AN ELECTRONIC 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

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

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 SECTION AND IN SECTION 3.8 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.

### 3.11 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 Section 2.10.

### 3.12 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 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.

### 3.13 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 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.

### 3.14 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 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 operating 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, regardless of where located, 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 3.2 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 Support Center by telephone at 833-FRS-SVCS (833-377-7827), with written confirmation via email to 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.

### 3.15 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 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; or (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 Section 3.8 of this operating 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.

### 3.16 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 OPERATING 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.

## 3.17 MANAGEMENT OF ELECTRONIC CONNECTIONS

**3.17.1** 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.

**3.17.2** 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.

### 3.18 DESTRUCTION, DELETION, OR RETURN OF RESERVE BANK SUPPLIED OR DESIGNATED EQUIPMENT AND SOFTWARE; SURVIVAL OF OBLIGATIONS

Upon termination under Section 2.6, 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.

## 4.0 SUPPORTING SERVICE – E-PAYMENTS ROUTING DIRECTORY

This Section 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. 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 Section 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 Section.

### 4.1 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 contains 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 this Section, which provides access to the Directory through an Electronic Connection.

**Institution** for purposes of this Section means an Institution together with any of its Service Providers, although on occasion both an Institution and a Service Provider may be separately referenced for emphasis or clarity.

### 4.2 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.

### 4.3 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.

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.

## 4.4 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 Section for the Authorized User's use of the Authorization Code.

## 4.5 DISCLAIMER OF WARRANTIES; INDEMNIFICATION; LIMITATIONS OF LIABILITY

**4.5.1** 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.

**4.5.2** 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.

**4.5.3** 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 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 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 the use of (or inability to use) the E-Payments Routing Directory Service by the Institution's Authorized User, including any violation of this Section 4 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.

### 4.6 AMENDMENTS AND TERMINATION

In addition to the amendment and termination provisions set forth in this 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.

## 5.0 SUPPORTING SERVICE – EXCEPTION RESOLUTION SERVICE

This Section sets forth the terms under which the Reserve Banks provide the Exception Resolution Service. The Exception Resolution Service is designed to aid Institutions in handling certain kinds of exceptions that arise with respect to their payment messages or items by facilitating Institutions' exchange of information related to such exceptions.

### 5.1 DEFINITIONS

**ERS Participant** means an Institution that has enrolled in the Exception Resolution Service.

**ERS Guide** means the guide made available to Institutions by the Reserve Banks setting forth information on the features and use of the Exception Resolution Service.

**Exception Resolution Service** means the service provided by the Reserve Banks in accordance with this Section.

**Exception Case** means a case that an Institution may initiate through the Exception Resolution Service related to an exception that arises with respect to a payment message or item, as set forth in the ERS Guide.

**Requesting ERS Participant** means an ERS Participant that initiates an Exception Case in accordance with the procedures set forth in the ERS Guide.

**Responding ERS Participant** means an ERS Participant that receives an Exception Case in accordance with the procedures set forth in the ERS Guide.

## 5.2 ERS GENERALLY

Each ERS Participant is responsible for determining how best to use the Exception Resolution Service as part of its own risk management processes and procedures, in accordance with its own risk tolerance and any requirements applicable to it.

The Exception Resolution Service is not a means through which an ERS Participant or any other Institution may notify the Reserve Banks of an unauthorized debit to its Master Account.

## 5.3 ENROLLMENT; TYPES OF PARTICIPANTS

An Institution may become an ERS Participant by enrolling in the Exception Resolution Service as set forth in the ERS Guide.

An Institution must enroll as either a full ERS Participant or a partial ERS Participant as set forth in the ERS Guide. A full ERS Participant may act as a Requesting ERS Participant or a Responding ERS Participant. A partial ERS Participant may act as a Responding ERS Participant only.

## 5.4 EXCEPTION CASES; REPORTS PROVIDED BY THE RESERVE BANKS

The ERS Guide sets forth procedures for, and any limitations on, (i) the initiation, resolution, and cancellation of Exception Cases by Requesting ERS Participants,

(ii) the Reserve Banks' processing, cancellation, and closure of Exception Cases, including email messages and other notifications regarding Exception Cases sent to ERS Participants, and (iii) responses to Exception Cases by Responding ERS Participants.

The ERS Guide may specify times by which an ERS Participant is expected to act with respect to an Exception Case. The Reserve Banks are not responsible for monitoring or enforcing an ERS Participant's compliance with such expectations.

This Section does not impose any obligation on a Responding ERS Participant to respond to an Exception Case. A Responding ERS Participant is responsible for complying with any independent obligation it may have to respond to an Exception Case.

The Reserve Banks may from time to time make reports available to ERS Participants regarding Exception Cases for which they are the Requesting ERS Participant or Responding ERS Participant, as set forth in the ERS Guide.

## 5.5 USE AND STORAGE OF INFORMATION BY THE RESERVE BANKS

Each ERS Participant agrees that the Reserve Banks may receive, store, and transmit information related to each Exception Case for which the ERS Participant is the Requesting ERS Participant or Responding ERS Participant. Such information may include personally identifiable financial information or other sensitive information provided by the ERS Participant.

The Reserve Banks manage an Exception Resolution Service data repository that contains all information related to each Exception Case for the period specified in the ERS Guide. An ERS Participant may view and retrieve information from the Exception Resolution Service data repository related to Exception Cases for which it was the Requesting ERS Participant or Responding ERS Participant as set forth in the ERS Guide.

## 5.6 DESIGNATION OF AUTHORIZED USERS, EMAIL ADDRESSES, AND SERVICE PROVIDERS

When an ERS Participant enrolls in the Exception Resolution Service, the ERS Participant (i) must designate authorized users for the Exception Resolution Service and (ii) may be required to designate email addresses to which Exception Cases and any reports or notifications regarding the Exception Resolution Service may be sent, in each case in accordance with the ERS Guide.

By designating email addresses to which Exception Cases and any reports or notifications may be sent, an ERS Participant authorizes the Reserve Banks to

send information via secure email, including any personally identifiable or other sensitive information, utilizing the email security mechanism selected by the Reserve Banks in their discretion. ERS Participants agree not to designate an email address of a person other than an employee or other authorized individual of the ERS Participant. The Reserve Banks have no responsibility to ensure that the email addresses designated by an ERS Participant belong to employees or other authorized individuals of the ERS Participant.

An ERS Participant may designate an agent, including an ACH operator (other than a Reserve Bank), as a Service Provider that may access or use the Exception Resolution Service on behalf of the ERS Participant in accordance with the ERS Guide and Section 2.3. The Reserve Banks may rely on the Service Provider designation until it is revoked in accordance with the ERS Guide and the Reserve Banks have had a reasonable time to act on the revocation.

An ERS Participant may designate a Reserve Bank to access and use the Exception Resolution Service on the ERS Participant's behalf in accordance with the ERS Guide.

### 5.7 UNENROLLMENT

An ERS Participant may unenroll from the Exception Resolution Service by following the procedures set forth in the ERS Guide.

### 5.8 USE AND DISCLOSURE OF INFORMATION

Each ERS Participant is responsible for protecting the security, integrity, and confidentiality of nonpublic, personally identifiable or other sensitive information contained in an Exception Case, report, or notification or otherwise made available to it through the Exception Resolution Service.

Each ERS Participant may use the information contained in an Exception Case, report, or notification or otherwise made available to it only in connection with its use of the Exception Resolution Service or processing of payment messages or items, and may disclose the information to third parties directly interested in the payment message or item to which the Exception Case relates, or otherwise as permitted by law.

### 5.9 LIABILITY

The Reserve Banks are not liable for any loss or damage resulting from the Exception Resolution Service being unavailable for any reason.

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, loss or damage resulting from (i) any delay, error, or omission in the transmission of an Exception Case, (ii) information submitted by an ERS Participant with respect to an Exception Case or contained in any files attached to such an Exception Case, (iii) an ERS Participant's failure to take any action with respect to an Exception Case, or (iv) acts or omissions of internet service providers. The Reserve Banks are also not liable for loss or damage resulting from acts of war, riots, civil unrest, strikes, labor disputes, acts of terrorism, acts of God, pandemics, or acts of nature.

The Reserve Banks shall have no liability with respect to the Exception Resolution Service to any party other than an ERS Participant. A Reserve Bank may be liable to an ERS Participant only for the Reserve Bank's failure to exercise ordinary care or act in good faith in providing the Exception Resolution Service. The amount of a Reserve Bank's liability to an ERS Participant under this Section is strictly limited to the greater of any fees for the Reserve Bank financial service for which the Exception Resolution Service is provided or fees for the Exception Resolution Service, in each case paid to the Reserve Banks by the ERS Participant during the month in which the Exception Case or occurrence giving rise to the liability is alleged to have occurred. In no event shall the Reserve Bank be liable for lost profits, claims by third parties, or consequential or incidental 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. Any legal action against a Reserve Bank with respect to the Exception Resolution Service must be initiated within one year from the date of the Exception Case or occurrence that gives rise to the claim.

Each ERS Participant will indemnify, defend, and hold the Reserve Banks harmless against any claim, loss, harm, or cost (including reasonable attorneys' fees and expenses of litigation) resulting from the acts or omissions of the ERS Participant or its Service Provider in connection with the ERS Participant's use of the Exception Resolution Service, or a Reserve Bank's acts or omissions in carrying out the instructions of the ERS Participant or its Service Provider within the scope of its agency appointment, except for any claim, loss, cost, or expense arising solely out of a Reserve Bank's failure to exercise ordinary care or to act in good faith.

## 6.0 SUPPORTING SERVICE – PAYEE NAME VERIFICATION SERVICE

This Section sets forth the terms under which the Reserve Banks provide the Payee Name Verification Service. The Payee Name Verification Service is an information service offered through an Electronic Connection for the purpose of aiding Institutions in evaluating whether the Payee's name is consistent with the title of the Payee Account, in relation to the routing of a payment transaction.

### 6.1 DEFINITIONS

**Institution** for purposes of this Section means an Institution together with any of its Service Providers, although on occasion both an Institution and a Service Provider may be separately referenced for emphasis or clarity.

**Payee Account** means an account to which an Institution intends to send a payment, as identified by account number and routing number in Payee Input Information provided by the Institution.

**Payee** means the person or entity to which an Institution intends to send a payment, as identified by name in Payee Input Information provided by the Institution.

**Payee Input Information** means information provided by an Institution to the Reserve Banks through the Payee Name Verification Service. The Payee Input Information generally contains the name of the Payee, the routing number and account number of the Payee Account, and any other information as set forth in the PNV Guide.

**Payee Output Information** means information that the Reserve Banks provide to an Institution through the Payee Name Verification Service.

**PNV Guide** means the guide made available to Institutions by the Reserve Banks setting forth information on the features and use of the Payee Name Verification Service.

### 6.2 PNV GENERALLY

The Payee Name Verification Service is designed only to provide an Institution with Payee Output Information regarding a Payee Account that the Institution may find useful in evaluating whether the Payee's name is consistent with the title of the Payee Account in relation to the routing of a payment transaction, as set forth in the PNV Guide. The Payee Name Verification Service does not stop payment transactions or other Messages from processing or settling through a Financial Service.

Payee Output Information reflects only the Reserve Banks' observations of their transaction records associated with the Payee Account identified by the Institution. Payee Output Information includes (i) a proprietary algorithmic scoring mechanism that reflects an estimated statistical match between the name of the Payee provided by the Institution against the payee names that the Reserve Banks have observed in payment transactions sent to the Payee Account through a Financial Service, and (ii) other information observed by the Reserve Banks as set forth in the PNV Guide.

To the extent that the information and data exchanged through the Payee Name Verification Service is made available by the Reserve Banks through an API Service, the terms of Section 7 (governing API Services) shall also apply.

### 6.3 TRANSMISSION OF INFORMATION; SERVICE PROVIDERS; INACCURATE INFORMATION

A Service Provider designated by an Institution to access or use a Financial Service on its behalf under any of the Reserve Banks' operating circulars may access or use the Payee Name Verification Service on behalf of the Institution in accordance with the PNV Guide and Section 2.3. Each time a Service Provider provides Payee Input Information to the Reserve Banks on behalf of an Institution, the Service Provider represents and warrants that it is authorized by the Institution to use the Payee Name Verification Service on the Institution's behalf.

An Institution shall notify Appropriate Reserve Bank Staff if it becomes aware of any inaccurate information reflected in the Payee Output Information. An Institution shall use reasonable efforts to investigate the circumstances regarding such inaccurate information and assist with the remediation of any inaccuracies.

### 6.4 RELATION TO THE RESERVE BANKS' SECURITY PROCEDURES AND OTHER INFORMATION SECURITY REQUIREMENTS

The Payee Name Verification Service does not (i) vary the Reserve Banks' security procedures described in the Reserve Banks' operating circulars; (ii) establish any agreement or instruction restricting a Reserve Bank's acceptance of payment orders, as described in Section 4A-202(b) of the Uniform Commercial Code; or (iii) relieve an Institution from its responsibility for developing controls to manage risks associated with sending or receiving Messages through a Financial Service or for complying with any information security or risk management requirements applicable to it.

### 6.5 LICENSE GRANT, CUSTOMER USE AND NONDISCLOSURE OF INFORMATION

**6.5.1** The Reserve Banks grant a limited, non-exclusive, non-transferable, non-assignable, non-sublicensable and revocable worldwide license to use the Payee Output Information subject to the terms set forth in this Section.

**6.5.2** The Payee Output Information is hereby designated as Confidential Information, whether or not it is labeled as "Confidential," and is proprietary information of the Reserve Banks. The Payee Output Information may not be used or shared with any other party including the Payee, except as outlined in this Section.

**6.5.3** Payee Output Information may be used by an Institution only as an input into an evaluation of whether the Payee's name is consistent with the title of the Payee Account, in relation to the routing of a payment transaction. The Payee Output Information shall not be used to ascertain other information about the Payee Account, Payee, or any other person or entity.

**6.5.4** The Institution may incorporate the Payee Output Information as an input into derivative services offered by the Institution, provided the input is only used to evaluate whether the Payee's name is consistent with the title of the Payee Account in relation to the routing of a payment transaction.

**6.5.5** The Reserve Banks may from time to time (i) require an Institution to provide confirmation that it is in compliance with the requirements set forth in this Section, and (ii) implement further controls with respect to Payee Output Information as set forth in the PNV Guide.

### 6.6 LIABILITY

**6.6.1** The Reserve Banks are not liable for any loss or damage resulting from the Payee Name Verification Service being unavailable for any reason.

**6.6.2** The Reserve Banks shall have no liability with respect to the Payee Name Verification Service to any party other than an Institution. A Reserve Bank may be liable to an Institution only for the Reserve Bank's failure to exercise ordinary care or act in good faith in providing the Payee Name Verification Service. The Reserve Banks are not liable to an Institution for any loss or damage resulting from any decision on whether to make or how to route a payment transaction for which it has received information through the Payee Name Verification Service, and such decision does not affect whether the Reserve Banks have exercised ordinary care and acted in good faith in providing the Payee Name Verification Service. The amount of a Reserve Bank's liability to an Institution under this Section is strictly limited to the fees for the Payee Name Verification Service paid to the Reserve Banks by the Institution during the month in which the occurrence giving rise to the liability is alleged to have occurred. In no event shall the Reserve Bank be liable for lost profits, claims by third parties, or consequential or incidental 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. Any legal action against a Reserve Bank with respect to the Payee Name Verification Service must be initiated within one year from the date of the occurrence that gives rise to the claim.

**6.6.3** Each Institution will indemnify, defend, and hold the Reserve Banks harmless against any claim, loss, harm, or cost (including reasonable attorneys' fees and expenses of litigation) resulting from the acts or omissions of the Institution in connection with the Institution's use of the Payee Name Verification Service, or a Reserve Bank's acts or omissions in carrying out the instructions of the Institution, except for any claim, loss, cost, or expense arising solely out of a Reserve Bank's failure to exercise ordinary care or to act in good faith.

## 7.0 SUPPORTING SERVICE – API SERVICE

This Section sets forth the obligations of the Reserve Banks to Institutions or Service Providers (often referred to in this Section as "you"), and of you to the Reserve Banks, related to access and use of various APIs through an Electronic Connection. The Reserve Banks offer an Electronic Connection that makes certain APIs available to Institutions and their Service Providers for the purpose of transmitting information and

data between them and a Reserve Bank on an unattended, systematic basis through an API.

Additional terms and requirements may apply to specific APIs that are established and agreed upon (by electronic click through acceptance or another means acceptable to the Reserve Banks) by you in connection with accessing or using a specific API.

**7.1 DEFINITIONS**

**API Service** means the services and functions, and data including any Reserve Bank Data, provided by a Reserve Bank which are accessible through or performed by a particular Reserve Bank API.

**API Service Provider** means a person or entity that is acknowledged by a Reserve Bank as authorized to act on behalf of an Institution, has agreed to the terms of this Operating Circular 5, and has obtained from a Reserve Bank the necessary Credentials to access a Reserve Bank API on behalf of an Institution.

**Application** means any software application, website, product, or service, developed or used by you that interacts with any aspect of a Reserve Bank API or that is intended for use on or with an API Service.

**Credentials** means the credentials that allow you to make authenticated requests to a Reserve Bank API.

**Developer Portal** means the marketplace accessible via website through which Institutions and API Service Providers may access and use the Reserve Bank APIs, including any mocking service that the Reserve Banks provide.

**API Terms** means the terms and conditions expressed in this Section 7, any terms and requirements applicable to a specific Reserve Bank API (if any), and any security, data, code and technical information regarding the use of the Reserve Bank APIs.

**End User** means a person or entity that uses an Application.

**Reserve Bank API** means an application programming interface made available via an Electronic Connection and comprising a set of programming instructions and standards, including any related code and API Terms, as updated from time to time, through which your Application(s) access and integrate with API Services.

**Reserve Bank Data** means data or content made available to you hereunder by a Reserve Bank through a Reserve Bank API.

**Reserve Bank Marks** means a Reserve Bank's proprietary trademarks, trade names, branding, or logos, related to the financial services that are offered to financial institutions by the Reserve Banks.

**Term** shall have the meaning assigned to it in Provision 7.10 hereof.

**7.2 REGISTRATION**

To access and use Reserve Bank APIs, you must first register on the Developer Portal or otherwise sign up for the API Service as directed by a Reserve Bank. A Reserve Bank may at its discretion approve or reject any registration without providing any reason. If you are permitted to register, you will create an account with the Reserve Banks and will obtain access credentials. You must keep your access credentials secret and take all appropriate measures to ensure their security. Any personalized login credentials may not be shared between individuals. You must ensure that any information you provide in connection with your registration is correct and complete, and you are solely responsible for keeping such information up-to-date and accurate as long as you maintain an account. You shall be responsible for all results of any access to a Reserve Bank API or API Service, using your account, whether authorized by you or not.

### 7.3 LICENSES AND OWNERSHIP

**7.3.1** Subject to your full compliance with these Terms and Conditions, the Reserve Banks grants you a nonexclusive, revocable, non-sublicensable, non-transferable, limited license, during the Term, to (i) use the Reserve Bank APIs for the sole purpose of enabling your Application to access or interface with an API Service; (ii) display Reserve Bank Data associated with such API Service within such Application; and (iii) distribute such Application to End Users. You have no right to distribute or allow access to any Reserve Bank API on a stand-alone basis.

**7.3.2** Your use of Reserve Bank APIs and API Services must comply with the security access requirements, other security requirements, API Terms, usage guidelines, call volume limits, rate limits or throttling limits, and other documentation provided through the Developer Portal or otherwise provided by a Reserve Bank in connection with your use of Reserve Bank APIs. If a Reserve Bank believes that you have attempted to exceed or circumvent these limitations, the Reserve Banks may temporarily or permanently block your ability to use Reserve Bank APIs or API Services. If you would like to use any Reserve Bank API beyond these limits, you must obtain a Reserve Bank's express written consent (and a Reserve Bank may decline such request or condition acceptance on your agreement to additional terms or charges for that use in its sole discretion).

**7.3.3** As between the parties, the Reserve Banks own all rights, title, and interest in and to the Reserve Bank APIs, API Services, and the Reserve Bank Marks, and subject to the foregoing, you own all rights, title, and interest in and to the Applications. The API Terms in no way convey any ownership right to you in any Reserve Bank API, API Service, or any component thereof, including any Reserve Bank Data within any Application. You agree to display any attribution(s) required by a Reserve Bank as described in the API Terms. Except to the limited extent expressly provided in the API Terms, neither party grants, and the other party shall not acquire, any right, title or interest (including any implied license) in or to any property of the first party under the API Terms or as a result of the use of an API Service. All rights not expressly granted herein are deemed withheld.

**7.3.4** You grant the Reserve Banks a perpetual, irrevocable, worldwide, sublicenseable, royalty free license to use, host, store, modify and publish, any content provided or posted to the Reserve Bank APIs through an Application, for the purpose of enabling a Reserve Bank to provide, update, and improve the Reserve Bank APIs and API Services. You shall not transmit content to the Reserve Bank APIs through any Application unless and until you have obtained all rights (including those from any End Users) required to grant the license set forth in the preceding sentence.

**7.3.5** If any Application includes any Open Source Software, you agree to comply with all applicable Open Source Software licensing terms, including by providing the notices and passing through the relevant licenses. You also agree not to use any Open Source Software in any Application in such a way that would cause any portion of any Reserve Bank API or any other software of a Reserve Bank to be subject to any Open Source Software licensing terms or obligations. "Open Source Software" means any software that requires as a condition of use, modification or distribution of such software that such software or other software incorporated into, derived from or distributed with such software (i) be disclosed or distributed in source code form, (ii) be licensed for the purpose of making derivative works, or (iii) be redistributable at no charge.

### 7.4 POLICIES AND RESTRICTIONS

**7.4.1** Under the API Terms, a Reserve Bank has no obligation to provide any type of support for the Reserve Bank APIs, the API Services, or any services or content related thereto (except as otherwise provided herein or in published specifications relating to a Reserve Bank API). You agree and acknowledge that a Reserve Bank may make changes or updates to any Reserve Bank API or API Service from time to time, and at its sole discretion and with or without notice. Changes or updates to a Reserve Bank API or API Service may adversely affect the manner in which your Application accesses or communicates with a Reserve Bank API or API Service. You must implement and use the most current version of the Reserve Bank APIs and make any changes to your Application that are required as a result of any such change or update by a Reserve Bank, at your sole cost and expense. In addition, a Reserve Bank may discontinue the availability of some or all Reserve Bank APIs at any time for any reason with or without notice. Such action may include removal of features, or requiring the payment of fees for previously free features. In addition to any other limitations of a Reserve Bank's liability set forth in these API Terms, the Reserve Banks will have no liability resulting from the actions described in this Provision 7.4.1.

**7.4.2** You acknowledge that a Reserve Bank or other developers may independently create applications, content, and other products or services that are similar to or competitive with your Applications. Nothing in these API Terms shall prevent or restrict a Reserve Bank or other developers from creating and fully exploiting any applications, content, and other items they may develop, with no obligation to you.

**7.4.3** Your registration on the Developer Portal does not entitle you to use every Reserve Bank API and API Service that may be offered by the Reserve Banks. The Reserve Banks have the right to restrict the use of certain Reserve Bank APIs or API Services to specially authorized registrants as determined by a Reserve Bank in its sole discretion. A Reserve Bank may suspend access to the Reserve Bank APIs or API Services or any component thereof at any time and from time to time in a Reserve Bank's sole discretion. A Reserve Bank may also take any Reserve Bank API or API Service partially or fully offline on a periodic basis in order to perform maintenance and support on, or implement upgrades or enhancements to, a Reserve Bank API or API Service or to components thereof (although the Reserve Banks shall have no obligation to provide any such maintenance, support or upgrades). Any such downtime may occur with or without notice.

**7.4.4** You shall not place advertisements within or adjacent to any API Service, nor shall you deliver, allow, or enable the delivery of unauthorized or unsolicited advertising, promotional materials, junk mail, or spam through your Applications. You shall ensure that your Application and your use of the Reserve Bank APIs and API Services comply with all laws and regulations, including all privacy and security-related laws, rules, and regulations. In addition, if you offer your Application to End Users outside your organization, you will provide and adhere to a legally compliant privacy policy that clearly and accurately describes to End Users what user information you collect and how you use and share such information with the Reserve Banks and third parties.

**7.4.5** A Reserve Bank may monitor and collect certain usage data and information related to your use of the Reserve Bank APIs and API Services, and may use such usage data and information for any business purpose, internal or external, including providing enhancements to the Reserve Bank APIs or API Services, providing support, or otherwise. In addition, a Reserve Bank may audit your use of the Reserve Bank APIs and your Applications in order to ensure compliance with these API Terms, and you agree to provide the Reserve Banks with the access necessary to reasonably conduct such audit. The Reserve Banks shall provide you with not less than thirty (30) days' advance written notice prior to conducting any such audit, and shall reasonably agree to maintain the confidentiality of any confidential information obtained pursuant to such audit. You further agree to conduct, upon a Reserve Bank's reasonable request, a self-assessment of your adherence to these API Terms and any security measures, instructions, guidelines, or specifications applicable to your usage of the Reserve Bank APIs or API Services, and attest to your completion of such self-assessment to the Reserve Banks. Your failure to comply with our efforts to audit your compliance with these API Terms is a material breach of these API Terms.

**7.4.6** Except as expressly authorized by these API Terms or as otherwise permitted in a separately executed agreement between you and a Reserve Bank, you will not attempt, or permit or encourage others, to:

(a) copy, modify, or create derivative works of any Reserve Bank API or API Service, in whole or in part;

(b) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer, wrap into another API, or otherwise make available any Reserve Bank API or API Service;

(c) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to any software component of any Reserve Bank API or API Service, in whole or in part;

(d) remove any proprietary notices from any Reserve Bank API or API Service;

(e) use any Reserve Bank API or API Service in any manner or for any purpose that infringes, misappropriates, or otherwise violates any intellectual property right or other right of any person, or that violates any applicable law;

(f) integrate, or allow access to, any Reserve Bank API or API Service with or from any software, technology, services, source or materials not managed by you or authorized by a Reserve Bank;

(g) use any Reserve Bank API or API Service in connection with any Application that offers or promotes services that may be damaging to, disparaging of, or otherwise detrimental to a Reserve Bank or our licensors, licensees, supervisors, affiliates, or partners;

(h) design or permit the Applications to disable, override, or otherwise interfere with any Reserve Bank-implemented communications to End Users, consent screens, user settings, alerts, warning, or the like;

(i) use any Reserve Bank API or your Application to create or provide services that replace or provide similar functionality to any Reserve Bank API or API Service or which is intended to migrate users away from an API Service;

(j) build databases from, store, or otherwise create permanent copies of, any Reserve Bank Data (except if you are an Institution, in which event this restriction does not apply to data separately shared between you and a Reserve Bank);

(k) pre-fetch or cache any Reserve Bank Data in or through an Application, except temporarily and only for the purpose of operating or improving the performance of an Application;

(l) use or access any Reserve Bank API for the purpose of testing or monitoring the performance or functionality of any Reserve Bank API or API Service or for any other benchmarking or competitive purposes;

(m) use a Reserve Bank's name or trademarks as part of your name or the name of any Application you offer or in any manner that creates a false sense of endorsement or sponsorship by a Reserve Bank;

(n) use a Reserve Bank API in an Application that directly or indirectly promotes criminal activity or violates any applicable federal or state law;

(o) upload or otherwise transmit any material that contains software viruses or any other computer code, files, or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

(p) use any Reserve Bank API in a manner that, as determined by a Reserve Bank in its sole discretion, is abusive or exceeds reasonable request volume or otherwise fails to comply with the API Terms;

(q) request more than the minimum amount of data from the Reserve Bank API needed by an Application to provide the intended Application functionality, or any data outside any permissions granted by the End User;

(r) include code in any Application which performs any operations not related to the services provided by the Application, including embedding or incorporating code into any Application which utilizes the resources (e.g., CPU resources) of another computer, such as for the purpose of cryptocurrency mining;

(s) interfere with or disrupt servers or other computer systems; or

(t) access or attempt to access any Reserve Bank server, computer system, service or content (including by probing, scanning or testing their vulnerability), except as expressly authorized by a Reserve Bank.

**7.4.7** Notwithstanding the restrictions set forth in Provision 7.4.6 above, an API Service Provider may, for the sole purpose of delivering or otherwise making available an API Service to an Institution for which it acts as an API Service Provider:

(a) copy, modify, or create derivative works of any Reserve Bank API or API Service, in whole or in part;

(b) rent, lease, lend, distribute, transfer, wrap into another API, or otherwise make available any Reserve Bank API or API Service;

(c) use any Reserve Bank API or your Application to create or provide services that replace or provide similar functionality to any Reserve Bank API or API Service; and

(d) build databases from, or otherwise create permanent copies of, any Reserve Bank Data to the extent such data reflects data that an Institution previously shared with a Reserve Bank.

### 7.5 USE OF MARKS

Subject to these API Terms, you may use the Reserve Bank Marks during the Term, to identify your Applications as compatible with the API Service. Your use of the Reserve Bank Marks must comply with the usage guidelines that a Reserve Bank may specify from time to time and (without limiting a Reserve Bank's other termination rights) you shall promptly cease any use of any Reserve Bank Marks that a Reserve Bank determines, in its sole discretion, to be non-compliant with Reserve Bank usage guidelines or otherwise detrimental to a Reserve Bank. You may not register any domain name containing the Reserve Bank Marks, the word "Federal Reserve Bank" or the name of any API Service (or anything confusingly similar). You also agree not to contest the validity of ownership of any Reserve Bank Marks. You receive no other rights to the Reserve Bank Marks under these API Terms. All goodwill arising from use of the Reserve Bank Marks belongs to a Reserve Bank.

### 7.6 ADDITIONAL RESPONSIBILITIES

**7.6.1** You are solely responsible, at your own expense, for (i) your Applications and their distribution and operation; and (ii) all customer and technical support and maintenance for the Applications. If you offer your Application for use by any End User outside of your organization, the End User may enable you or an Application, via a Reserve Bank API, to access certain of its data, content or information from a Reserve Bank database ("End User Data"). You must have in place an agreement with each End User outside your organization that: (x) contains all of the restrictions on use, limitations of liability and warranty disclaimers with respect to the Reserve Bank APIs and API Services as those contained herein; and (y) provides that you are solely responsible for the Applications including for any liability that may arise from the End User's use of the Application. You may not use any End User Data (or other Reserve Bank Data) in promotions or to target advertisements, and may not sublicense, lease, sell or otherwise transfer any End User Data or derivatives of End User Data to any third party (including to any ad networks, ad exchanges or data brokers). You will ensure that all End User Data is collected, processed, transmitted, maintained and used in accordance with (1) your agreement with the End User, (2) a legally adequate privacy policy and appropriate notices to and consents from End Users, and (3) all laws and regulations. As between you and a Reserve Bank, the Reserve Bank shall own all right, title and interest in any data that the Reserve Bank receives as a result of an End User's installation or use of an Application.

**7.6.2** Your networks, operating system and software of your web servers, routers, databases, and computer systems must be properly configured to industry standards so as to securely operate your Application and protect against unauthorized access to, disclosure or use of any information you receive from a Reserve Bank. Not in limitation of the preceding sentence, you must: (i) comply with the Reserve Banks Information Security Program set forth in Appendix A to Operating Circular 5 as if you are an "Institution" as defined therein, and (ii) use industry-standard technical, administrative and physical security measures to protect the privacy and

security of Reserve Bank Data and store all Reserve Bank Data using strong encryption. If you make your Application available for use by an End User outside of your organization, you may not store or use End User Data except as expressly permitted by the End User; and, subject to any legal data retention requirements, you must delete End User Data (i) upon the End User's request; (ii) when such data is no longer required to provide the services of your Application to the End User to whom the data relates, (iii) when the End User closes his or her account with, or otherwise deactivates, your applicable Application and (iv) if a Reserve Bank terminates your or your applicable Application's access to the applicable Reserve Bank API.

**7.6.3** You must promptly notify the Reserve Banks by telephone at 833-FRS-SVCS (833-377-7827), with written confirmation via email at 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 your Application, an API Service, any Reserve Bank Data or the Developer Portal (a "Security Event"). In addition, upon learning of the Security Event, at your own cost, you will: (A) promptly remedy the Security Event to prevent any further loss of data or other harm; (B) investigate the Security Event; (C) take reasonable actions to mitigate any future anticipated harm; and (D) provide the Reserve Banks with any requested information and assistance in a timely manner, including bearing the Reserve Banks' costs associated with remediating such Security Event (including any costs resulting from compliance with any notification or other regulatory requirements and costs for the provision of credit monitoring services to affected individuals). Any notification to End Users or others outside your organization relating to a Security Event shall not contain any reference to a Reserve Bank unless (i) the Reserve Bank approves of the reference, (ii) the notification is required by applicable law and the Reserve Bank fails to timely respond to a request for approval, or (iii) the Reserve Bank seeks to modify the reference in a manner that your counsel reasonably determines is inaccurate or inconsistent with applicable law.

**7.6.4** You are not permitted to use a service provider in connection with hosting, distributing or supporting any Application or otherwise providing an Application's service unless they agree to limit their use of the Reserve Bank API and API Service solely for the purpose of providing their services to your Application (and not for their own purpose or any other purpose), and keep the Reserve Bank API, API Service, and any Reserve Bank Data secure and confidential. You must ensure that any service provider complies with the API Terms, and you acknowledge and agree that any act or omission by a service provider which constitutes a breach of the API Terms will be deemed to be a breach by you.

### 7.7 FEES

Except for those Reserve Bank APIs made available by a Reserve Bank free of charge, the Reserve Bank APIs are priced in accordance with the API Fee Schedule published by the Reserve Banks. Unless otherwise provided on such Fee Schedule or such other notice as may be published by the Reserve Banks,

all fees are payable in United States currency and are non-refundable. All fees and charges quoted are exclusive of applicable taxes and duties, including any applicable sales and use tax. You are responsible for paying any taxes assessed based on your use of Reserve Bank APIs and API Services under the API Terms. If you fail to pay any fees due by the due date, a Reserve Bank may suspend your access to any Reserve Bank API or API Service. The Reserve Banks may change the published fees for Reserve Bank APIs from time to time; provided, that the Reserve Banks shall publish written notice of any such change prior to the effectiveness thereof.

You may not directly or indirectly charge End Users for use of, or access to, the functionality of any API Service or Reserve Bank APIs. You may charge fees for your Applications; provided, that, if you choose to charge any fees for your Applications, then you are solely responsible for collecting those fees.

**7.8 REPRESENTATIONS AND WARRANTIES**

You represent and warrant that (a) you have full power and authority to enter into and perform the API Terms; and (b) you have or will obtain effective consent, to the extent legally required, from the applicable individual before you provide a Reserve Bank with, or obtain from a Reserve Bank, information of or pertaining to such person in connection with your use of Reserve Bank APIs. You further represent and warrant that you have the right to use, reproduce, transmit, copy, publicly display, publicly perform, and distribute your Applications, and that use of your Application by you, your users (including any End Users), a Reserve Bank, or its users, will not violate the rights of any third party (e.g., copyright, patent, trademark, privacy, publicity or other proprietary right of any person or entity), or any applicable regulation or law.

**7.9 YOUR FEEDBACK**

Any feedback, suggestions and ideas ("Feedback") that you provide to a Reserve Bank regarding any Reserve Bank API or API Service, or content or services related thereto may be treated by a Reserve Bank as non-confidential, and a Reserve Bank may, in its sole discretion, use the Feedback in any way, including in future modifications of the Reserve Bank APIs, API Services, or content or services related thereto, or advertising and promotional materials relating thereto. You hereby grant the Reserve Banks a perpetual, worldwide, fully transferable, irrevocable, royalty-free license to make, use, sell, offer for sale, reproduce, modify, create derivative works from, distribute, and display the Feedback in any manner and for any purpose.

**7.10 TERM AND TERMINATION**

The term of license granted to you under these API Terms shall be coterminous with the expiration of your login credentials established at the registration or renewal of your credentialed electronic access to any Reserve Bank API, unless earlier terminated as hereinafter provided (the "Term").

You may terminate the API Terms at any time by ceasing all use of the Reserve Bank APIs and any relevant credentials. The Reserve Banks may immediately suspend or terminate any license granted to you hereunder and your access to and use of any Reserve Bank API or API Service or any portion thereof, or

terminate the API Terms, in part or in their entirety, at any time for any reason and with or without notice. The Reserve Banks may discontinue the availability of some or all of the Reserve Bank APIs or Reserve Bank Data at any time for any reason, with or without notice. The Reserve Banks will not be liable for any costs, expenses, or damages that may result from any such suspension or termination.

The following provisions of these API Terms shall survive any termination or expiration: Provisions 7.4 through 7.23, and any other terms that may reasonably be assumed to be intended to survive expiration or termination.

Upon any termination of the API Terms: (a) you will immediately stop using the Reserve Bank APIs, Reserve Bank Marks and API Services; (b) you must permanently destroy any Confidential Information; and (c) all licenses granted to you by the Reserve Banks will cease. If your Application makes use of a Reserve Bank API, your Application may no longer function as intended after expiration or termination of the license granted to you under the API Terms, and you are responsible for ensuring that all End Users are aware of this risk. You understand that after termination, you will have no access to any data or content that you or any End Users submitted to a Reserve Bank in connection with use of the Reserve Bank APIs. A Reserve Bank may independently communicate with any End User whose account(s) are associated with your Application and credentials to provide notice of the termination of your right to use a Reserve Bank API.

**7.11 CONFIDENTIALITY**

You may be given access to certain non-public proprietary information, software, and specifications related to the Reserve Bank APIs and API Services (the "Confidential Information"). A Reserve Bank's Confidential Information includes the Reserve Bank APIs, Reserve Bank Data, any Credentials, keys, or passwords, and any non-public aspects of the API Services. You shall use a Reserve Bank's Confidential Information only as necessary for the purpose of exercising the rights granted to you by the API Terms. You agree to protect the Confidential Information from unauthorized use, access, or disclosure in the same manner that you would use to protect your own confidential and proprietary information of a similar nature and in any event with no less than a reasonable degree of care. You shall not disclose any Confidential Information to any third party without our prior written consent; provided, however, that you may disclose the Confidential Information to your personnel or agents engaged in a use permitted by the API Terms who have a need to know and who are subject to an obligation to maintain the confidentiality thereof. You may not embed Credentials in open source projects. If you are compelled by law to disclose Confidential Information, you must provide FRB with (i) prior notice of such compelled disclosure (to the extent legally permitted) in a manner that provides a Reserve Bank with sufficient time to allow the Reserve Bank an opportunity to contest the disclosure, and (ii) reasonable assistance if a Reserve Bank wishes to contest the disclosure. You acknowledge that any breach of this Section may cause immediate and irreparable injury to a Reserve Bank, and in the event of such breach, the Reserve Bank shall be entitled to seek injunctive relief in addition to any and all other remedies available at law or in equity.

**7.12 DISCLAIMERS**

THE RESERVE BANKS DO NOT MAKE ANY SPECIFIC PROMISES REGARDING ANY RESERVE BANK API, API SERVICE, OR ANY COMPONENT THEREOF. FOR EXAMPLE, THE RESERVE BANKS DO NOT MAKE ANY COMMITMENTS ABOUT ANY RESERVE BANK DATA ACCESSED THROUGH THE RESERVE BANK API, YOUR ABILITY TO UTILIZE THE RESERVE BANK API IN CONNECTION WITH YOUR APPLICATIONS, OR THE SPECIFIC FUNCTIONS OF ANY RESERVE BANK API OR API SERVICES OR ITS OR THEIR RELIABILITY, AVAILABILITY, OR ABILITY TO MEET YOUR NEEDS. THE API SERVICES AND THE RESERVE BANK APIS, ALONG WITH ANY OTHER DATA OR MATERIALS PROVIDED BY THE RESERVE BANKS IN CONNECTION WITH YOUR USE OF THE RESERVE BANK API ARE PROVIDED ON AN "AS-IS" AND AS AVAILABLE BASIS, WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, TITLE, ACCURACY OF DATA, AND ANY WARRANTIES OR CONDITIONS ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. THE RESERVE BANKS DO NOT WARRANT THAT THE API SERVICES, RESERVE BANK APIS OR ANY OTHER DATA OR MATERIALS PROVIDED HEREUNDER WILL MEET YOUR REQUIREMENTS, BE ERROR FREE, UNINTERRUPTED, VIRUS FREE, OR SECURE.

### 7.13 LIMITATION OF LIABILITY

UNLESS OTHERWISE PROHIBITED BY LAW, THE RESERVE BANKS WILL NOT BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY SPECIAL, INCIDENTAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, BUSINESS, REVENUES, OR PROFITS) ARISING OUT OF OR IN CONNECTION WITH THE API TERMS OR YOUR USE OF ANY RESERVE BANK API OR API SERVICE, WHETHER ARISING FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, AND REGARDLESS OF WHETHER YOU HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. THE FOREGOING LIMITATIONS WILL SURVIVE AND APPLY EVEN IF ANY LIMITED REMEDY SPECIFIED IN THE API TERMS IS FOUND TO HAVE FAILED ITS ESSENTIAL PURPOSE. IN ANY CASE, THE RESERVE BANKS' AGGREGATE LIABILITY UNDER THE API TERMS WILL NOT EXCEED THE GREATER OF ONE HUNDRED DOLLARS ($100.00) OR THE AGGREGATE FEES YOU PAID FOR ACCESS TO THE RESERVE BANK API DURING THE 6 MONTHS PRIOR TO THE EVENT GIVING RISE TO THE LIABILITY.

### 7.14 INDEMNIFICATION

You will indemnify, defend and hold the Reserve Banks, their affiliates and their directors, officers, employees, contractors, agents, and users harmless from and against any and all claims, damages, losses, liabilities, actions, judgments, costs, and expenses (including reasonable attorneys' fees) arising out of or in connection with: (a) your use of any Reserve Bank API, API Service, or any component thereof; (b) your negligence, willful misconduct or breach of the API Terms; (c) any agreement or relationship between you and an End User; (d) any content or data routed into or used with a Reserve Bank API by you, or those acting on your behalf; (e) any Security Event; or (f) your Application, including

claims of intellectual property infringement. You will not settle any such claim without a Reserve Bank's prior written consent.

### 7.15 GOVERNMENT USE

The API Services and Reserve Bank APIs and each component thereof constitute a "commercial item," "commercial computer software," and "commercial computer software documentation."

### 7.16 ASSIGNMENT

You shall not assign the API Terms or any rights or obligations hereunder without the prior written consent of a Reserve Bank which may be given or withheld in its sole discretion. Any attempted assignment without such prior written consent shall be void. The Reserve Banks may assign the API Terms without restriction.

### 7.17 NO AGENCY, PARTNERSHIP, OR JOINT VENTURE

The API Terms do not create or imply any partnership, agency, or joint venture between the parties hereto.

### 7.18 GOVERNING LAW AND FORUM FOR LEGAL DISPUTES

The API Terms will be governed by the laws of the United States of America and, in the absence of controlling law, the laws of the State of Illinois, without regard to or application of conflicts of law rules or principles. All claims arising out of or relating to the API Terms will be brought exclusively in the U.S. District Court for the Northern District of Illinois and you consent to personal jurisdiction in those courts. Your breach of the API Terms relating to the licenses the Reserve Banks grant to you and your use of the Reserve Bank APIs and API Services may result in irreparable harm and permanent injury to the Reserve Banks for which monetary damages would be an inadequate remedy. In such circumstances, the Reserve Banks will be entitled to seek and obtain, without the posting of a bond, in addition to all other remedies available to them, at law or in equity, immediate injunctive relief to prevent or stop any breach of those provisions.

### 7.19 WAIVER AND SEVERABILITY

The API Terms constitute the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior proposals, understandings, and communications between the parties with respect to that subject matter. No waiver by either Party of any covenant or right under the API Terms will be effective unless such waiver is in writing and duly authorized by the Party granting the waiver. If any part of the API Terms is determined to be invalid or unenforceable by a court of competent jurisdiction, that provision will be enforced to the maximum extent permissible and the remaining provisions of the API Terms will remain in full force and effect.

### 7.20 PUBLICITY

Except as approved in writing by a Reserve Bank on a case-by-case basis in the Reserve Bank's sole discretion, you may not claim or in any way imply in any advertising that any Application is created, certified, sponsored, or endorsed in any manner by a Reserve Bank. In addition, you may not make any representations, warranties or commitments regarding any Reserve Bank APIs or API Service or on behalf of a Reserve Bank.

### 7.21 UPDATES TO API TERMS

The Reserve Banks may modify the API Terms from time to time. The Reserve Banks will post notice of modifications to the API Terms within the documentation of each applicable Reserve Bank API, to the Developer Portal, or by email notice to you as provided in Section 7.22. Changes will not apply retroactively and will become effective no sooner than 30 days after they are posted, unless the change addresses a new function for a Reserve Bank API or a legally required change, in which case such changes will be effective immediately. If you do not agree to the modified API Terms, you should discontinue your use of the Reserve Bank API. Your continued use of a Reserve Bank API constitutes your acceptance of the modified API Terms.

### 7.22 EMAIL NOTICE

All notices to you in connection with these API Terms may be delivered via email at the email address provided to a Reserve Bank by you, and you agree that these email communications satisfy any legal requirements. You agree that if, during the Term, you update or change your email address from the one that you provided to the Reserve Banks upon your initial registration, you will promptly notify the Reserve Banks in writing of such update or change.

### 7.23 EXPORT RESTRICTIONS

You acknowledge that you will comply with U.S. Export Administration Regulations. You will not export or re-export any API Service, Reserve Bank API or any component thereof, directly or indirectly, to: (1) any countries that are subject to U.S. export restrictions; or (2) any End User who has been prohibited from participating in U.S. export transactions by any federal agency of the U.S. government. In connection with U.S. Export Administration Regulations, a Reserve Bank may, without telling you, furnish any regulator or other governmental authority, both foreign and domestic, with information about your Applications and your use of the Reserve Bank APIs.

*[Appendix A begins on next page]*

# 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 Banks' 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 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 3.1 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 the Support Center by telephone at 833-FRS-SVCS (833-377-7827), with written confirmation via email at 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 Online or Offline.

(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 Online Security Procedure is identified by the name of the Electronic Connection associated with the Online Security Procedure. Each of the Online 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 Online 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 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 Online 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 its Administrative Reserve Bank. The Institution shall notify the Reserve Banks immediately in accordance with Section 3.2 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 its Administrative Reserve Bank 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 Service message; 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® Service message.

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) Offline Security Procedure

Fedwire Funds Service: An Offline Security Procedure is available to any Institution that chooses to send, authenticate, or receive a message, including a payment order, over the Fedwire Funds Service orally by telephone. This includes instances in which an Institution that normally sends, authenticates, or receives a message over the Fedwire Funds Service by means of an encrypted communication using an Online Security Procedure is unable to do so because of an equipment or communications outage or other similar circumstances (regardless of whether such outage or circumstances relate to an issue with Reserve Bank equipment or facilities or equipment or facilities of an Institution or one of its agents).

When an Institution sends a message, including a payment order, to a Reserve Bank, the Offline Security Procedure involves an identity code or other security code sent 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 Offline Security Procedure involves an identity code or other security code sent by a Reserve Bank to an employee of the Institution, and the Institution is required to call the Reserve Bank back to authenticate the message before acting with respect to the message, including, when the messages is a payment order, making proceeds of the funds transfer available to the beneficiary.

An Institution that wishes to use the Offline Security Procedure shall provide to the Appropriate Reserve Bank Staff the names of employees who are authorized to send or authenticate Offline messages, including payment orders. 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 Institution.

National Settlement Service: An Offline 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 Online 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 Offline 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.

Fedwire Securities Service: An Offline Security Procedure is available to any Institution that chooses to send, authenticate, or receive a message, including a securities transfer message, over the Fedwire Securities Service orally by telephone or written by e-mail. This includes instances in which an Institution chooses to conduct this activity offline in the ordinary course of business and those in which an Institution that normally sends, authenticates, or receives a message over the Fedwire Securities Service by means of an encrypted communication using an Online Security Procedure is unable to do so because of an equipment or communications outage or other similar circumstances (regardless of whether such outage or circumstances relate to an issue with Reserve Bank equipment or facilities or equipment or facilities of an Institution or one of its agents).

When an Institution sends a message to a Reserve Bank, the Offline Security Procedure involves an identity code or other security code sent by an employee of the sender and may include a call-back or listen-back procedure by a Reserve Bank. When the Institution is receiving a message, the Offline Security Procedure involves an identity code or other security code sent by a Reserve Bank to an employee of the Institution, and the Institution is required to call the Reserve Bank back to authenticate the message before acting with respect to the message.

An Institution that wishes to use the Offline Security Procedure shall provide to the Appropriate Reserve Bank (as defined in Operating Circular 7) the names of employees who are authorized to send or authenticate

Offline messages, including securities transfer messages. 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 Institution.

## 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 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 3.13 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 Operating Circular 5, 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 2.6 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.