Comptroller's Handbook

Safety and Soundness

Capital Adequacy (C) | Asset Quality (A) | Management (M) | Earnings (E) | Liquidity (L) | Sensitivity to Market Risk (S) | Other Activities (O)

Payment Systems

Version 1.0, October 2021

Office of the Comptroller of the Currency

Contents

Introduction

The Office of the Comptroller of the Currency's (OCC) *Comptroller's Handbook* booklet, "Payment Systems," is prepared for use by OCC examiners in connection with their examination and supervision of national banks, federal savings associations, and federal branches and agencies of foreign banking organizations (collectively, banks). Each bank is different and may present specific risks and issues. Accordingly, examiners should apply the information in this booklet consistent with each bank's individual circumstances. When it is necessary to distinguish between them, national banks[1] and federal savings associations are referred to separately.

This booklet provides examiners with information regarding payment systems,[2] types of payments, risks associated with payment systems, and associated risk management practices. For a detailed discussion of the technology aspects of payment systems and associated information technology (IT) risk management, refer to the "Retail Payment Systems" and "Wholesale Payment Systems" booklets of the *Federal Financial Institutions Examination Council (FFIEC) Information Technology Handbook.* Additionally, refer to the "Merchant Processing" booklet of the *Comptroller's Handbook* for more information about merchant processing. For more information on Bank Secrecy Act/anti-money laundering (BSA/AML) related to payment systems, refer to the *FFIEC BSA/AML Examination Manual*.

Examiners should use the information in this booklet when assessing the quantity of risks associated with payment systems and quality of risk management for each associated risk. Examiners should generally expect to see payment systems risk management integrated into the bank's overall risk management system and governance framework. Risk management practices for payment systems should directly correspond with the specific payment channels used, products and services offered, and the complexity of those offerings.

This booklet includes expanded examination procedures for examiners to use when assessing payment products and services. Also included are supplemental procedures for deeper review of certain payment activities.

The OCC's supervisory activities regarding payment systems focus on the risks and associated risk management practices. Effective supervision of a bank's payment system activities includes integrating risk disciplines to provide a holistic supervisory approach.

This booklet references specific services and brand names including those trademarked by their respective companies. These references are informational and should not be construed as an OCC endorsement of a particular product, service, or company.

---

[1] Generally, references to "national banks" throughout this booklet also apply to federal branches and agencies of foreign banking organizations unless otherwise specified. Refer to the "Federal Branches and Agencies Supervision" booklet of the *Comptroller's Handbook* for more information regarding applicability of laws, regulations, and guidance to federal branches and agencies.

[2] Terms that are underscored on first mention in this booklet are defined in appendix B, "Glossary."

Overview

A payment is a transfer of value. Payments are transacted in various ways, such as by check, automated clearing house (ACH), and wire transfer. Payments may also be transacted on a ledger or via distributed ledger technology (DLT),[3] from a digital wallet, and via payment cards (e.g., credit, debit, and prepaid cards (sometimes called stored value cards)).

Payment systems facilitate payments and settle obligations by communicating information about individual payment transactions and settling transactions. Payment systems are critical components of the nation's financial infrastructure and are vital to the financial stability of the U.S. economy. Payment systems facilitate the clearing and settlement of retail and wholesale payments. Retail and wholesale payment systems are operated by public and private sector entities.

Retail payments are primarily made by consumers and between businesses to purchase goods and services. Retail payment systems typically handle a high volume of relatively low-value payments (e.g., ACH, checks, and credit, debit, and prepaid cards).

Wholesale payments are usually made between businesses or governments and are typically large-value payments. Wholesale payments are generally used to purchase, sell, or finance securities transactions; disburse or repay loans; settle real estate transactions; and make large-value, time-critical payments, such as payments for the settlement of interbank purchases and sales of federal funds, settlement of foreign exchange transactions, or other financial market transactions.

Financial market infrastructures (FMI), also referred to as financial market utilities (FMU), provide payments, clearing, settlement, trading, and depository services. Examples of FMIs include payment systems, depositories, and clearing houses. Banks generally become members or stakeholders of the various domestic and international payment systems and clearing houses to provide payment services to their customers. For U.S. banks, funds transfers are handled by wholesale or large-value payment systems, such as Fedwire and The Clearing House[4] (TCH) Interbank Payments System (CHIPS). Examples of other U.S. FMIs include Continuous Linked Settlement Bank (CLS), Chicago Mercantile Exchange Clearing (CME), National Securities Clearing Corporation (NSCC), and Depository Trust Company (DTC).

Some FMIs are central counterparty (CCP) clearing houses. Risk management of FMIs and CCPs is often performed by the same bank risk function. CCPs provide settlement services that facilitate trades between counterparties in one or more financial markets by either

[3] The Bank for International Settlements (BIS) defines DLT as the processes and related technologies that enable nodes in a network (or arrangement) to securely propose, validate, and record state changes (or updates) to a synchronized ledger that is distributed across the network's nodes. Refer to BIS, Committee on Payments and Market Infrastructures, "Distributed ledger technology in payment, clearing, and settlement: an analytical framework" (February 2017).

[4] TCH is a banking association and payments company that is owned by a group of the largest commercial banks.

guaranteeing trades or replacing contracts. CME and NSCC are examples of CCPs. A CCP has the potential to reduce risks to market participants by imposing robust controls on participants and, in many cases, by engaging in multilateral netting. A CCP concentrates risks and responsibility for risk management in the CCP. Banks that are members of CCPs provide initial margin funds and agree to loss sharing in cases of member default. Risk management is important because of potentially large liabilities and heightened risk exposure.[5]

The following are the typical steps in the payment process. Not all payment types include all steps, and the steps do not always occur in the same order.[6]

- **Initiation:** A participant (payor, payee, or third party) initiates the payment process by sending an instruction to another individual or entity that begins a process that ends in a payment.
- **Authentication:** The process of verifying the identity or veracity of a participant, device, payment, or message connected to a payment system. Authentication can occur at multiple points in the payment process (e.g., at the time of initiating or receiving a payment).
- **Authorization:** The explicit instructions, including timing, amount, payee, source of funds, and other conditions that the payor gives to the payor's account provider or to the payee to transfer funds on either a one-time or recurring basis.
- **Approval:** The step following the initiation of a payment when the payor's account provider verifies that the payor's account has sufficient funds or credit necessary to complete the authorized transactions.
- **Clearing:** The payor's and payee's account providers exchange information to confirm a transaction before settlement.
- **Receipt:** Funds are received by the payee and are available for withdrawal or transfer.
- **Settlement:** Settlement irrevocably extinguishes the obligation of the payor's depository institution and often occurs simultaneously with receipt of funds. Settlement can occur on a gross basis, in which each transfer is settled individually, or on a net basis, in which credits and debits periodically offset each other.
- **Reconciliation:** Responsible parties verify that the records issued by the entities involved in a transaction match. The reconciliation process can include appropriate reversals and post-transaction analysis.

Banks offer various payment products and services to meet customer needs. Payment originations may occur from within a bank's various business lines and may be managed at a centralized enterprise-wide level or dispersed among responsible business lines. Payment products and service offerings provide opportunities to enhance client relationships, grow fee income, and attract deposits.

[5] For more information regarding CCP risk management, refer to the "Membership Risk Management" section of this booklet.

[6] For more information, refer to the Board of Governors of the Federal Reserve System's "The U.S. Path to Faster Payments: Final Report Part One: The Faster Payments Task Force Approach" (January 2017).

The payments industry is dynamic, with banks and nonbanks competing to move money efficiently and ubiquitously. Customers are demanding faster payments, which is driving significant innovation in payment product offerings and technology.

Payment Types

This section provides an overview of common payment types and discusses the transaction and settlement flow.

Checks

Checks are one of the oldest payment types in the United States. The magnetic ink character recognition (MICR) line at the bottom of a check makes it possible for checks to be processed with little or no human intervention. The Check Clearing for the 21st Century Act (Check 21)[7] further standardized check processing by allowing the payee's bank to create a digital image of a check, a process known as check truncation. The electronic image is called a substitute check.[8] The use of substitute checks eliminated the need to process paper checks or return paper checks to the payor. Checks may also be converted to an ACH debit from the payor's deposit account. Instead of processing the digital image of the paper check, as occurs in traditional check processing, the recipient uses the information on the check to create a new ACH transaction.

Remotely created checks (RCC) are another type of check transaction, in which a digital image is created based on an authorization to debit an account, and, instead of a signature, the RCC includes a statement that the account holder authorized the payment. RCCs may be processed as checks or converted to ACH debit transactions. Commercial bank customers acting as payment processors may deposit RCCs into their bank accounts on behalf of their merchant clients.

Lockbox banking is a fee income check-processing service that banks offer to their business customers. The service allows business customers to bypass the receipt of paper checks to their physical establishments. With lockbox services, banks receive physical checks on behalf of their customers, most often for credit card or loan payments, generally to a designated post office box. Once the checks are received, the bank typically processes these payments using high-speed scanners. After the reconcilement process is completed, the checks are incorporated into the image cash letters (ICL). The funds from the payments are deposited directly into the bank customer's accounts. The corresponding payment information is transmitted to the bank customer's accounts receivable system.

[7] Refer to Pub. L. 108-100, as codified at 12 USC 5001-5018.

[8] Refer to the "Depository Services" booklet of the *Comptroller's Handbook* for more information regarding substitute checks.

Check Transaction and Settlement Flow

The check transaction and settlement flow begins with the check payor issuing, authorizing, or writing a paper negotiable instrument payable to the payee (e.g., a check or RCC). This instrument is the binding instruction to pay money to the payee. Once the payee gains possession of the check, the payee generally deposits the check into his or her bank account. The bank that holds the payee's account is the bank of first deposit (BOFD). With the onset of Check 21, the BOFD in most cases is also the converting bank,[9] which is the bank that converts the original paper check into a digital image. The BOFD bundles all outgoing (forward processing) check images into ICLs. Checks that are deposited at the same bank on which they are drawn ("on us"), are cleared internally by the BOFD. Checks deposited into a transaction account, including checks deposited at an unstaffed facility, such as a night depository, lock box, or automated teller machine (ATM) are subject to Regulation CC funds availability requirements.[10]

The bank's settlement or further processing of the forward ICL may be outsourced to a check processor or larger correspondent bank, which forwards the ICL to a clearing house or a Federal Reserve Bank. Some banks contract directly with Federal Reserve Banks or clearing houses, in which case the bank transmits its ICLs directly to its Federal Reserve Bank or clearing house instead of a correspondent bank or check processor. Once the Federal Reserve Bank or clearing house receives a bank's ICL, the Federal Reserve Bank or clearing house performs the settlement function and forwards the digital image to the payor's bank (i.e., paying bank). Upon receipt, the paying bank withdraws the funds from the payor's account and reconciles the ICL. Banks can also clear checks through the Federal Reserve Bank or through independent clearing houses. Many third parties offer processes and systems for imaging, transferring, archiving, and retrieving checks. Many banks participating in check clearing houses use the National Settlement Service (NSS)[11] to effectuate check settlement.

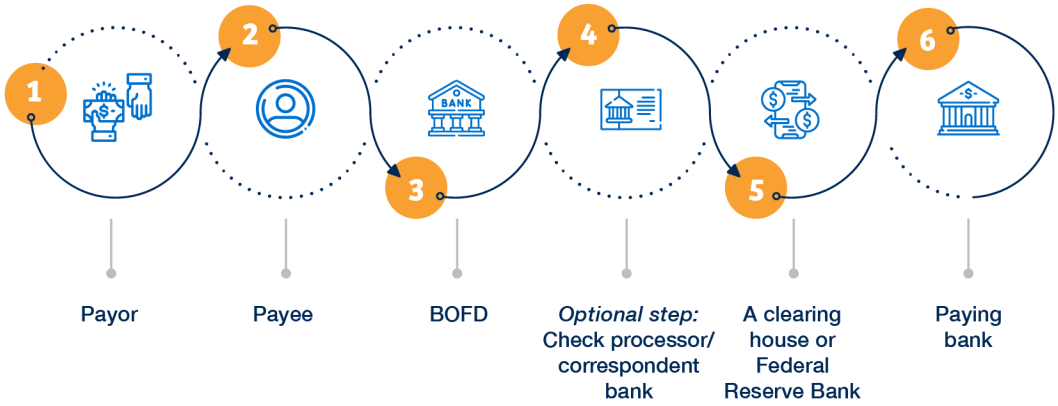
Figure 1 illustrates the check transaction and settlement flow.

[9] A converting bank is also referred to as a truncating bank.

[10] For more information, refer to the "Depository Services" booklet of the *Comptroller's Handbook*.

[11] The NSS is a multilateral settlement service that is offered to member depository institutions and is owned and operated by the Federal Reserve Banks.

Figure 1: Check Transaction and Settlement Flow



Product-Specific Risks: Checks

The following are examples of risks associated with check products:

- Check fraud occurs in a variety of ways including alterations, bleaching, counterfeiting, forgery, and theft. Increased check fraud may expose a bank to heightened operational and credit risks.[12]
- Overdrafts may occur. Banks often issue unsecured lines of credit and overdraft protection products for overdrawn accounts. These products allow the bank to pay a customer's check when the customer does not have funds available. These overdrafts present credit risk to the bank. Management should establish sound underwriting and approval practices when establishing line-of-credit and overdraft protection products.
- Returned depository items (RDI) are checks returned unpaid by the paying bank. These items were originally deposited in a bank's customer's account. RDIs heighten a bank's risk because if the funds are no longer in the bank customer's account when the return check is received, the bank is exposed to a potential monetary loss.
- Check kiting involves a customer presenting checks, some of which may not be funded, at two or more financial institutions and using the uncollected funds while the items settle. In check kiting, the fraudster takes advantage of the time it takes to pay or clear the checks, in effect, taking out an unauthorized and interest-free loan. The time delay is referred to as the float time. Although float time has decreased because of the electronic advancement under Check 21, check kiting still presents risk to banks.
- The purchase or exchange of monetary instruments at the placement and layering stages of money laundering can conceal the source of illicit proceeds.
- Bank customers that are also payment processors may generate and deposit RCCs into bank accounts; the lack of visibility into these activities increases the risks for the bank.
- RCCs may also be generated by merchants that have obtained personal bank account information in order to misuse the customer information to facilitate the creation of an unauthorized RCCs.

[12] Refer to the interagency publication "Check Fraud: A Guide to Avoiding Losses."

Remote Deposit Capture

The technology advancements created by Check 21 paved the way for the development of remote deposit capture (RDC).[13] RDC provides a means for digitally processing items eligible for deposit, primarily checks, at locations such as bank branches, ATMs, or a customer or merchant customer's location via a dedicated RDC scanner or mobile device.

A significant volume of checks is processed through RDC. The benefits can be substantial to banks and their customers. RDC can improve efficiencies, reduce costs associated with paper processing, increase fee income, and reduce geographic limitations. Customers can benefit from accelerated clearing, which can reduce losses from returned or lost checks, may result in faster availability of deposited funds, and can eliminate the need to go to a physical bank. RDC introduces risks compared with traditional deposit methods.[14]

Remote Deposit Capture Transaction and Settlement Flow

The customer creates an image of the check using a scanning device (e.g., RDC scanner or camera on a mobile device) to create a digital image. The digital image is then transmitted over an encrypted connection to the RDC customer's bank or the bank's service provider, which then accepts the deposit and credits the deposit to the customer's account.

Product-Specific Risks: Remote Deposit Capture

The following are examples of risks associated with RDC:

- Unauthorized access occurs when a customer fails to implement adequate physical and logical security controls over RDC systems (customer authentication when accessing the RDC system; transmission, retention, and proper disposal of deposited items; protection of nonpublic personal information; and separation of duties at the bank and customer location).
- Technological issues such as delays or disruptions may occur during processing, clearing, and settlement of transactions.
- Poor image quality and inaccurate data can result from inadequate document management procedures or training.
- Redeposit of items or duplicate presentment can occur when a bank customer (intentionally or unintentionally) transmits an image of a check to the bank and then deposits the original check at a different bank.
- Fraud may occur in a variety of ways including duplicated images, counterfeit items, forged or missing endorsements, bleaching, alterations, and money laundering.[15]

[13] RDC is often called by different names, such as teller capture, bank capture, or merchant capture, depending on how the service is applied within a particular environment.

[14] For more information, refer to OCC Bulletin 2009-4, "Remote Deposit Capture: Interagency Guidance."

[15] Refer to OCC Bulletin 2009-4 and the *FFIEC BSA/AML Examination Manual*.

- Banks may face challenges in controlling or knowing the location of RDC equipment, because the equipment can be readily transported from one jurisdiction to another.

Automated Clearing House

In general, an ACH transaction is a batch-processed electronic funds transfer between an originating bank and a receiving bank. An ACH transaction may be either a deposit (credit) or withdrawal (debit). Traditional examples of ACH transactions include direct deposit payroll deposits and mortgage payment or insurance payment withdrawals.

The ACH Network is a U.S. payment network that electronically transmits payment instructions from one financial institution to another financial institution to debit or credit a deposit account. These payment instructions are transmitted within the United States and across borders through international ACH transactions (IAT).[16]

Automated Clearing House Transaction and Settlement Flow

ACH transactions (entries) are authorized by the receiver, who is the owner of the account at the receiving depository financial institution (RDFI). Entries are identified by the action occurring in the receiver's account. If funds are withdrawn from the receiver's account, the transaction is identified as an ACH debit entry. If funds are deposited to the receiver's account, the transaction is identified as an ACH credit entry. The ACH operator (Federal Reserve Banks or Electronic Payments Network[17] (EPN)) settles the obligation between the banks for the associated ACH file. Nacha[18] is the administrator of the ACH Network and enforces the Nacha Operating Rules and Guidelines.

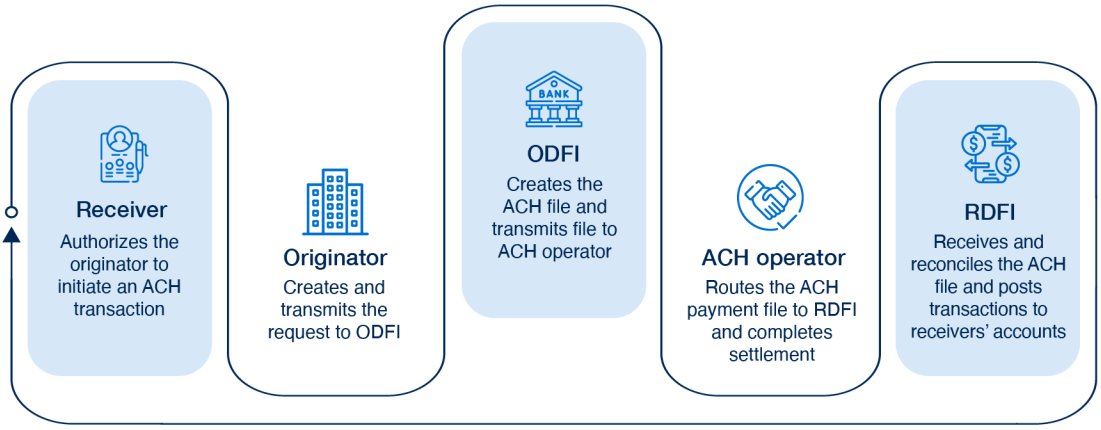
An ACH transaction always begins and ends at the ACH receiver's account. The transaction begins after a receiver authorizes an ACH originator to perform either a debit or credit transaction. The originator initiates the payment instructions and begins the payment transaction flow. The originating depository financial institution (ODFI) initiates and sends the ACH file to the ACH operator. The ACH operator routes the payment instructions to the RDFI and monetarily settles the files. If the ACH operator is a Federal Reserve Bank, the file is settled using the bank's Federal Reserve account. If the ACH operator is the EPN, the file is settled through the NSS. The RDFI credits or debits the receiver's account according to the assigned settlement date. Figure 2 illustrates the ACH transaction and settlement flow.

[16] IAT is the Standard Entry Class (SEC) code that identifies international payments. Using the IAT SEC code facilitates a bank's ability to comply with Office of Foreign Assets Control (OFAC) requirements. Under the Nacha Operating Rules and Guidelines, all U.S. financial institutions that participate in the ACH Network must receive and process IATs. For more information about ACH transactions and IATs, refer to the "Automated Clearinghouse Transactions" section of the *FFIEC BSA/AML Examination Manual.*

[17] EPN is TCH's ACH operations service.

[18] Nacha was formerly the National Automated Clearinghouse Association (NACHA).

Figure 2: ACH Transaction and Settlement Flow



Product-Specific Risks: ACH

The following are examples of risks associated with ACH:

- Human error, training deficiencies, ineffective procedures, and lack of dual controls or separation of duties may cause ACH errors.
- Outages and technical or human errors may cause posting delays at a bank, and delays may cause a bank to miss required deadlines.
- ACH fraud usually affects bank customers and includes transacting with compromised account credentials, email compromise, account takeover, social engineering, and scams involving questionable charges and transactions.
- The bank may lack either ACH reviews or comprehensive reviews and does not test for compliance with regulatory requirements and network rules.
- The receiving bank (RDFI) incurs increased credit risk if it grants its customer funds availability before settlement of the credit entry.
- The bank's credit risk may increase if the bank lacks policies, underwriting standards, and board approvals for ACH originators.
- Lack of appropriate and approved ACH exposure limits may expose a bank to heightened credit risk.
- Lack of sharing of information on or about originators and receivers inhibits a bank's ability to appropriately assess and manage the risk associated with correspondent and ACH processing operations, monitor for suspicious activity, and screen for OFAC compliance.

Wholesale and Large-Value Payments

Banks use wholesale and large-value payment systems, such as Fedwire and CHIPS, to transfer funds related to their own operations (e.g., federal funds transactions) and to transfer funds, such as for securities settlements, on behalf of the banks' customers (e.g., wire transfer). The flow of funds associated with wholesale payments is extremely large compared with the reserve and clearing account balances that represent the payment system's liquidity

base. The value and volume of activity on Fedwire and CHIPS have made intraday credit an essential element in the smooth functioning of both of these systems. In addition to Fedwire and CHIPS, banks use the financial messaging system, Society for Worldwide Interbank Financial Telecommunication (SWIFT), to relay messages regarding incoming and outgoing funds transfers.

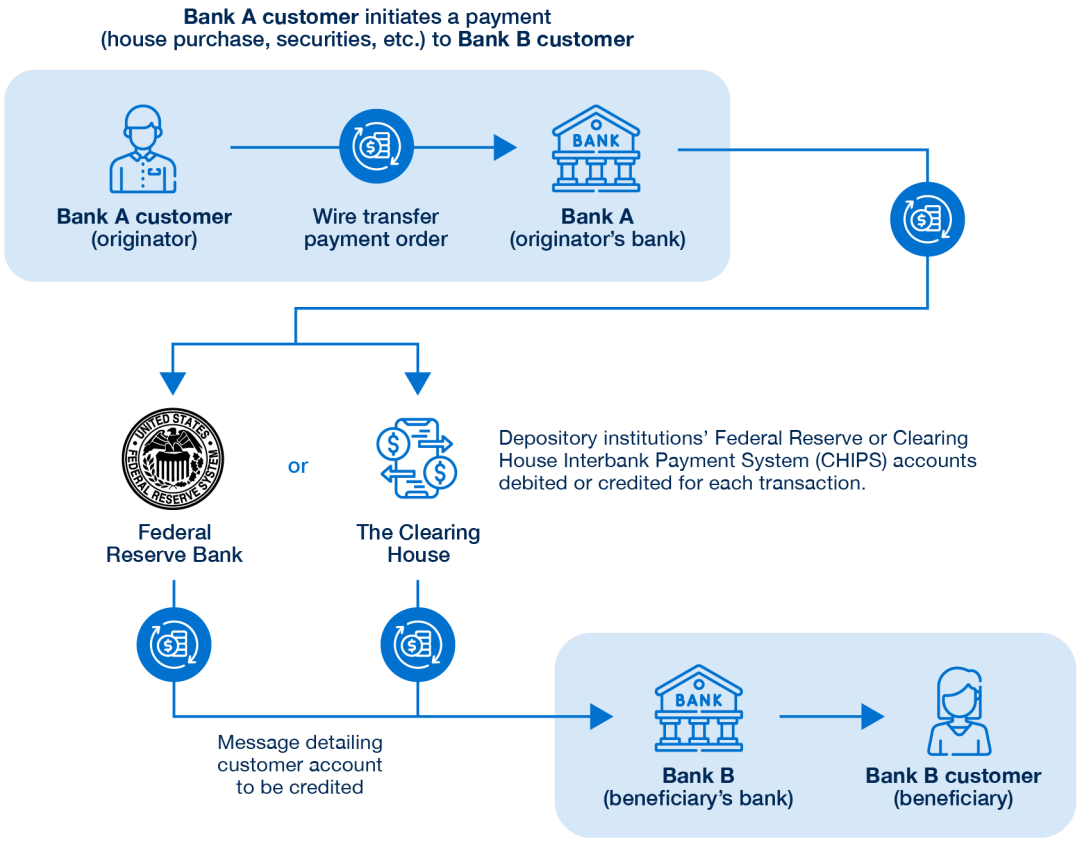
In addition to Fedwire and CHIPS, there are many other international large-value payment systems with which a bank could interact. Many multinational financial institutions become members of payment systems outside the United States to gain direct access to a particular market and avoid using correspondent banks. One of the most widely used systems is TCH Automated Payments System (CHAPS), which is a real-time gross settlement payment system used for sterling transactions in the United Kingdom. Financial institutions may join similar systems in the eurozone or Asia (e.g., Trans-European Automated Real-time Gross Settlement Express Transfer System (TARGET2), the Single Euro Payments Area (SEPA), TCH Automated Transfer System (CHATS)).

Similar to the other payment types, operational risk is the primary risk for wholesale payments. Wholesale payment processing has been significantly automated and is generally performed as straight through processing (STP) with little to no manual intervention. STP can reduce the risks associated with payment processing. Therefore banks often process a large percentage of payment transactions using STP. Reliance on third parties can increase a bank's operational risk exposure. Because of the large value and high volume of wholesale payment transactions, operational disruptions may have widespread impact.

Wire Transfer Transaction and Settlement Flow

A wire transfer transaction begins when the originator (bank customer) requests the transfer. The originating bank verifies the request then initiates the transaction with the operator (e.g., Federal Reserve Bank or TCH). The operator settles the payment between the banks and forwards the message (payment instructions) to the beneficiary's bank. Some transactions also include an intermediary bank. The beneficiary bank then credits the beneficiary account in accordance with the payment instructions. Figure 3 illustrates the wire transfer process.

Figure 3: Domestic Wires Transaction and Settlement Flow



Fedwire

Fedwire is operated by the Federal Reserve Banks and allows any depository institution with a Federal Reserve account to transfer funds from its Federal Reserve account to another institution's Federal Reserve account. Each transfer is final and irrevocable when made because Fedwire is a real-time gross settlement system.[19] Fedwire's operation is based on the provision of liquidity and the absorption of the resulting risk by the Federal Reserve Banks. Therefore, a beneficiary bank is not exposed to credit risk from the sending depository institution, nor does the receiving financial institution bear credit risk in making the proceeds of the transfer immediately available to a customer. The Federal Reserve Banks provide the intraday credit needed to handle the dollar volumes processed each day, during operating hours, on Fedwire by allowing depository institutions to initiate Fedwire transfers that may exceed, at a given moment, the balance in their reserve or clearing accounts. These intraday overdrafts of accounts are referred to as daylight overdrafts.

The Clearing House Interbank Payments System

CHIPS is operated by TCH. Information about individual transfers is exchanged by the participating depository institutions throughout the day. CHIPS is settled on a same-day, net

[19] For more information, refer to 12 CFR 210, subpart B, "Funds Transfers Through Fedwire."

basis at the close of business. At the close of business, the value of all transfers sent and received by each of the participants is totaled and netted to determine a net credit or debit position for each participant. The institutions participating in CHIPS are divided into two categories: funding participants and non-funding participants. Non-funding participants settle their net activity for the day with a designated correspondent bank that is a funding participant. Funding participants are responsible for their own net positions and the net positions of the institutions that they represent in the settlement. Settlement among the funding participants is accomplished through a settlement account at the Federal Reserve Bank of New York. Funding participants in a net debit position make Fedwire transfers into the settlement account equal to their net debit positions. Unlike Fedwire, which uses real-time gross settlement, CHIPS uses a net settlement mechanism.

In contrast to Fedwire, CHIPS creates interbank credit exposures among the system's participants. A transfer cannot be rescinded once a depository institution enters information about the transfer into the system. At any time during the day, some CHIPS participants will have initiated transfers with total dollar value greater than that of the transfers they have received. These participants, in a net debit position, are essentially receiving intraday credit from the other participants (i.e., participants that have received transfers with a total value higher than that of the transfers they have sent).

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

The SWIFT messaging service provides members[20] with a private international communications channel that allows the exchange of structured electronic messages. SWIFT is used to transmit customer and bank funds transfer messages. These messages are used in conjunction with a payment system (e.g., Fedwire and CHIPS), which is used to transfer the associated payment. Additionally, SWIFT communicates foreign exchange confirmations, debit and credit entry confirmations, statements, collections, and trade finance transactions.

Product-Specific Risks: Wholesale and Large-Value Payments

The following are examples of risks associated with wholesale and large-value payments:

- Wholesale payment processing exposes the bank to heightened operational risk. Given the large value and finality of these transactions, even a short operational or technological disruption could have a widespread impact. Wholesale payments are often specifically targeted for cyber attacks, and effective controls are imperative.[21]
- Wholesale payments increase exposure to credit risks because of the large value of the transactions. Credit risk is present in any payment process or product where there is a settlement lag or where provisional credit is provided to the customers. Many banks offer

[20] According to the SWIFT website, members include banks; payment, securities, and treasury market infrastructures; broker/dealers, custodians, investment managers, and fund participants; and corporate clients.

[21] Refer to OCC Bulletin 2016-18, "Cybersecurity of Interbank Messaging and Wholesale Payment Networks: FFIEC Statement." This statement discusses the controls that banks and third parties should implement to maintain safe and secure wholesale payment and messaging operations.

daylight overdraft lines for payments to their business customers, which increases the credit exposure further.
- As banks rely on the daily payment flows to meet their obligations, wholesale payments can create significant liquidity exposures given their value and volume. During a financial crisis, liquidity risk can be amplified and create systemic risk if a bank stops payments or does not process wire transfers in a timely manner.

Payment Cards

Payment cards (i.e., credit, debit, and prepaid) can be used in person at a location or in a variety of ways in which the card need not be physically presented (e.g., online, from a digital wallet, or by telephone). Payment cards may be used to purchase goods or services or to facilitate money transfers. Card networks have developed products and services focused on providing funds in real time or near real time. For example, the use of credit "push" transactions allows the near real-time transfer of funds directly from the sender to the receiving cardholder's eligible account (e.g., Visa Direct and Mastercard Send).

Participants in card transactions typically include the cardholder, merchant, issuing bank, card association network, acquiring bank,[22] and the card processor. Card association networks include credit card networks (e.g., Visa, Mastercard, American Express, and Discover) and debit card networks (e.g., Plus, NYCE,[23] Cirrus, and Star). Networks can be open (e.g., Visa and Mastercard), in which the acquiring bank and issuing bank are different entities, or closed, in which the network and issuing bank are controlled by the same entity (e.g., Discover and American Express). Card transactions are generally authenticated individually and batched for processing through the card association networks.

Issuing banks issue payment cards to cardholders. Issuing banks generate revenue from interchange fees, interest charged on revolving balances, and fees (e.g., late, over-limit, cash advance, and other fees). An acquiring bank is a bank that contracts with merchants for the settlement of card transactions. Acquiring banks contract directly with merchants, or indirectly through agent banks or other third parties, to process card transactions. Acquiring banks generate revenue from the discount rate[24] and processing fees (e.g., chargeback processing and account maintenance fees) they charge to the merchant.[25]

Some banks are involved in an arrangement commonly known as "rent-a-BIN." This arrangement allows an entity to conduct credit card activities using a bank's Visa bank

[22] For more information, refer to the "Merchant Processing" booklet of the *Comptroller's Handbook*.

[23] NYCE stands for New York Currency Exchange.

[24] The discount rate is the fee, as a percent of sales volume, that an acquirer charges a merchant for processing sales transactions. For more information, refer to the "Merchant Processing" booklet of the *Comptroller's Handbook.*

[25] For more information, refer to the "Merchant Processing" booklet of the *Comptroller's Handbook.*

identification number (BIN) or Mastercard Interbank Card Association (ICA) number in return for a fee paid to the bank.[26] There are two types of rent-a-BIN arrangements:

- Issuing rent-a-BIN: The bank "rents" its right to offer credit cards under the card association's logo. The third party generally solicits prospective credit card customers and then provides approved applicants with a credit card. The bank is identified as the card issuer, while the third party and other sub-contracted participants may not necessarily be apparent to the cardholder.
- Acquiring rent-a-BIN: The bank allows an independent sales organization or member service provider to use the bank's BIN or ICA number to settle merchant credit card transactions in return for a fee. The acquiring bank has minimal operational involvement; however, the bank retains the risk of loss, as well as the responsibility for settlement with the card associations.

Credit card networks function differently depending on the role. If the network is both the network and the card issuer, the network processes and approves purchase requests (e.g., American Express and Discover cards). If the credit card network is different from the card issuer, the network acts as an intermediary that connects the merchant with the financial institution that issued the card to process and approve the credit card transaction (e.g., Visa, Mastercard). The four major credit card networks are American Express, Discover, Mastercard and Visa. Some credit card networks are also issuers, but not all credit card networks issue credit cards. For example, some banks (e.g., Discover, American Express) are issuers and networks. Mastercard and Visa are credit card networks. Banks can also be credit card issuers without also being a network by joining an existing network.

A debit card network provides communication between merchants and issuers to complete debit transactions. Major debit card networks are Star, Cirrus, Plus, and NYCE. There are some key differences in processing between the credit card and debit card networks. For instance, if the debit card is processed through a credit card network, it either requires a signature or can be used for a card-not-present transaction and the funds are generally deducted the following day from the related checking account. If the card is used on a debit card network, a personal identification number (PIN) is usually required and the funds are immediately deducted from the associated checking account.

Debit and credit card transactions are batched for settlement between financial institutions. There are some variations in settlement based on the card association network rules. The batch settlements generally occur using ACH.

The following are common types of payment cards:

- **Credit cards:** Funds for purchases are derived from credit lines of an underlying loan agreement.[27] Credit card products generally fall into the following broad categories:

[26] For more information about rent-a-BIN arrangements, refer to the "Merchant Processing" booklet of the *Comptroller's Handbook*.

[27] For more information, refer to the "Credit Card Lending" booklet of the *Comptroller's Handbook*.

general purpose cards (including charge cards), proprietary or private-label cards, corporate or commercial cards, and secured cards.

- **Debit cards:** Funds for purchases are debited directly from the cardholder's checking account. Debit cards are either PIN-based or signature-based. Some cards have options for both PIN-based and signature-based transactions.
  - PIN-based debit cards authenticate customers by matching the PIN and account number at a merchant's point of sale (POS) terminal, in real time. Cardholders can receive cash at the POS because messaging between the merchant and the cardholder's bank confirms funds availability. Processing fees are substantially lower than for signature-based debit cards.
  - Signature-based debit cards authenticate using the cardholder's written signature.
- **Special purpose debit cards:** These cards allow purchases based on specific administrative programs. Merchant codes and product codes can be used at the POS (and are required by some state laws for certain merchants) to restrict sales to permissible products or services. For example, a flexible spending account debit card allows for the purchase of medical goods or services.
- **Prepaid cards:**[28] A prepaid card derives its value from a prefunded account that can only be accessed through the use of the card. Some prepaid cards can be reloaded with funds by the cardholder or another party such as an employer or a government entity. Prepaid cards are divided into two categories:
  - Open-loop general purpose cards are connected to one of the major card networks such as Visa, Mastercard, American Express, or Discover and can be used anywhere those cards are accepted. Some open-loop prepaid cards can also be used at ATMs to withdraw available funds.
  - Closed-loop stored value cards' usage is limited to a specific merchant or a network of merchants. The cards carry a pre-loaded value that becomes available once the card is purchased and activated.
- **ATM cards:** ATM cards can generally only be used for cash withdrawals from ATMs.
- **Virtual cards:** As indicated by their name, virtual cards are not physical payment cards, but they function in the same manner for online payments and use the same card association networks as physical cards. The cardholder obtains information needed to make a payment (e.g., card number and expiration date) from the issuer's portal on the internet or within a mobile application. This information is generated on a per use basis and changes with every use, which can be a fraud mitigation tool. For example, virtual cards are popular in the corporate space as they allow the administrators to issue payment information to their employees for one-time use, and can be restricted in terms of amounts, types of merchants, and other factors.

Card transactions can be initiated with a variety of methods, including

- **Card not present (CNP) transactions:** Some transactions can be processed without presenting the physical card to the payee. For instance, an online purchase involves providing card information to a merchant who will not see the physical card.

[28] Refer to the "Gift Cards" section of the "Consigned Items and Other Customer Services" booklet of the *Comptroller's Handbook* and OCC Bulletin 2011-27, "Prepaid Access Programs: Risk Management Guidelines and Sound Practices."

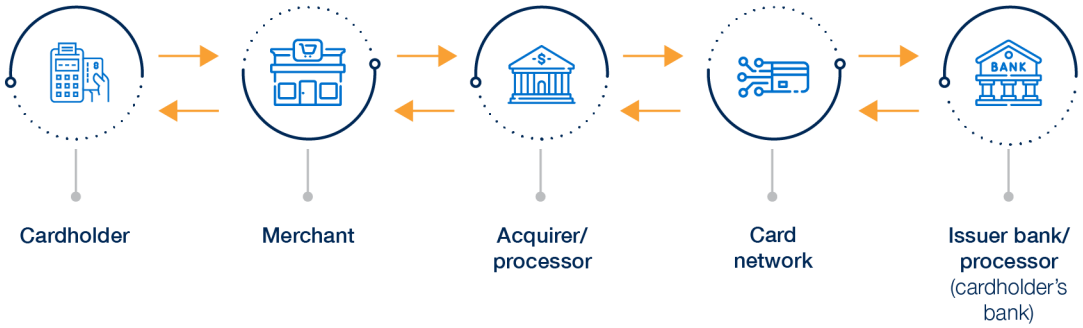
- **Card present (CP) transactions:** There are several ways to initiate a card transaction when the card is physically present, typically using a card reader at a merchant. CP transactions can be conducted in several ways.
  - The magnetic stripe on the card stores the cardholder information (e.g., name, card number, and expiration date), and is unprotected.
  - The EMV[29] chip is an embedded microprocessor that protects the cardholder information and is used to generate unique transaction data and verify card legitimacy when present. Combined with a PIN entry, the transaction becomes even more secure. Most merchants use the chip and signature in the United States and do not require PIN entry.
  - Contactless-enabled cards allow for transactions using near-field communication (NFC) technology in the point-of-sale configuration. When this payment method is used the system generates a unique transaction identifier tied to the chip, which is presented near the terminal.
- **Mobile device proximity payments:** Proximity payments are payments made using a digital wallet application and NFC technology via a cardholder's mobile device. With this payment method, the mobile device is physically present when initiating the payment.
- **Tokenization:** Tokenization is used to protect sensitive information. Tokenization involves a process of replacing credit card information with unique symbols, which creates a token. The token is not based on any known number in the original transaction such as a bank number, account number, or any other information tied to the customer. Tokens allow retention of essential information about the transaction without compromising its security.

Card Payment Transaction and Settlement Flow

Card transactions flow between cardholders, merchants, processors, acquiring banks (acquirer), and issuing banks (issuer), within a card association network. A cardholder initiates a card payment by presenting a payment card (or providing card details, such as the number and expiration date). The merchant's payment system sends the card information to the acquirer or payment processor, which sends the information to the appropriate card network, which forwards it to the issuing bank for approval. The issuer approves or declines the transaction, sending the information back through the payment chain the way it came. The transaction flow for mobile proximity payments is similar to that of a traditional card transaction. The issuing bank is responsible for authenticating the card when the card is added to the customer's mobile device and for approving the payment transaction. Figure 4 illustrates the card payment process.

[29] EMV stands for Europay, Mastercard, and Visa.

Figure 4: Card Payment Transaction Authorization Flow



When the merchant issues a refund, the transaction follows the same process. When the cardholder's refund request is not resolved by the merchant, the cardholder often contacts the issuing bank for credit via a chargeback.[30] The settlement of card transactions may differ depending on the specifics (e.g., type of card, parties involved) and the established agreements or contracts. Generally, payment card transactions are batched and settled through ACH. Refer to the "Merchant Processing" booklet of the *Comptroller's Handbook* for more information.

Product-Specific Risks: Payment Cards

The risks vary depending on the bank's role (i.e., as an issuing bank or acquiring bank), the types of payment cards that the bank issues, the payment card transactions that the bank processes, and the bank's use and oversight of third parties.

The following are examples of risks associated with payment cards:

- Banks that use third parties to administer various aspects of customer card accounts are exposed to increased risks (e.g., operational, compliance, reputation) relating to the activities performed by the third party.
- Prepaid cards have been used for money laundering and can expose banks to BSA/AML risk, including transferring funds to or from an unknown third party.
- Prepaid cards are also one of the preferred payment methods used by fraudsters, primarily because prepaid cards can sometimes be purchased and used to complete a transaction without providing detailed personal information.
- Reloadable cards can be reloaded with funds by the cardholder or another party and present risk of money laundering. Cards can be transported across borders.
- Heightened compliance risk may exist due to multiple rules and regulations that apply (e.g., card association rules and Regulation E).
- Credit risk may be increased with potential fraud and charge-back activity.

[30] Other reasons for a chargeback include processing errors, duplicate billing, identity theft, disputes over price charged versus processed, or missed merchant refunds.

Real-Time Payments

Many banks offer real-time payment (RTP) products in response to customer demand for faster payment options. Some banks have developed or participate in consortiums or networks that offer real-time or near-real-time payment services for their customers or are working with third parties to offer person-to-person (P2P) payment services and faster payment functionality.

Common P2P payment solutions (e.g., Venmo, CashApp, and ApplePay) and consortiums (e.g., Zelle) generally use a directory of accounts and associated phone numbers or email addresses. To transfer funds, a customer enters the unique identifier of the recipient into the mobile banking application and the amount of funds to transfer. Although the customer may have real-time access to the funds, settlement is not necessarily immediate. Banks that participate in consortiums typically agree to provide provisional credit to the recipient's bank, and the funds are typically settled through ACH or the card networks. Use of a consortium enables customers who may not have accounts at the same financial institution to transfer funds between accounts. Payments sent are final and irrevocable, so proper identification of the payee is of paramount importance.

Another real-time payment solution is the RTP network by TCH, which is a real-time payment settlement service owned by a consortium of banks. The RTP network provides participating banks with the ability to send payments directly from eligible accounts 24 hours a day and 365 days a year, and to receive and access funds sent over the RTP network immediately, except as necessary for risk management, legal, or compliance purposes (e.g., account holds, regulatory holds). Banks can participate in the RTP network directly or through third parties, bankers' banks, and corporate credit unions.

The RTP network strictly processes credit "push" transactions, meaning that the person or entity making the payment instructs its financial institution to transmit a deposit to the payee. The irrevocability of a payment sent over the RTP network enables immediate, final settlement to the payee.

At the time of this booklet's publication, the Federal Reserve Banks were in the process of developing the FedNow Service. The FedNow Service will be available to depository institutions in the United States and will allow individuals and businesses to send instant payments through their depository institution accounts.[31]

Product-Specific Risks: Real-Time Payments

The following are examples of risks associated with real-time payment products:

- Payments may be misdirected. Unauthorized transactions could be sent because of customer error. The irrevocability of a payment sent in real time highlights the importance of customer authentication and proper identification of the payee.

[31] For more information, visit https://www.federalreserve.gov, click on "Payment Systems" in the toolbar, then click on "FedNow Service."

- Banks may take losses relating to payments that cannot be recovered.
- Employees may be unfamiliar with the functionality and unable to provide technical support to bank customers. Employee training and awareness help mitigate this risk.
- There is heightened risk of fraud and losses due to the speed and finality of the transactions. Fraudsters prefer to use fast transactions and target the customers rather than the bank. Customer awareness training is critical in preventing this type of fraud.
- Fraudsters may attempt to enroll as new customers, or impersonate existing customers, to make or intercept payments. Effective onboarding and enrollment of customers mitigate fraud.

Mobile Payments

Mobile payments are transacted through the use of an electronic communications device, typically a mobile phone. Mobile payments can be made to a business (i.e., person-to-business [P2B], business-to-business [B2B]) or person (i.e., P2P, business-to-person [B2P]).[32]

Person-to-Person Payments

Mobile devices and applications (internet or mobile) can be used to transfer funds among individuals. A P2P payment provider offers customers a digital wallet, which is funded by a payment card or bank account. The funds transfer is processed through a card network or ACH network, and funds are settled as a typical card or ACH transaction. Once the funds are transferred into the digital wallet, the customer can transfer funds to other users in the provider's system using a phone number, email address, or other unique identifier. To withdraw funds from the digital wallet, a customer initiates a transfer, which is processed through a card network or ACH network. Some providers issue the customer a check or prepaid card with the funds, and some providers also allow customers to purchase goods and services at merchants using funds the customer has in the digital wallet.

Product-Specific Risks: Mobile Payments

Risks associated with other payment types (e.g., card payments) may also apply to mobile payment products. The following are examples of risks associated with mobile payments:

- Mobile devices are at risk of being lost, stolen, or infected with viruses and are often unencrypted, which results in insecure data storage. Risk mitigants include strong security and authentication controls.
- Customers and their mobile devices may be targeted for fraud. A good fraud prevention tool is a customer awareness and education program. An absent or poorly designed program may increase risk if customers are uninformed and ultimately susceptible to fraud or do not understand the finality of payments and related liabilities.

[32] For more information regarding card transactions using a mobile device, refer to the "Payment Cards" section of this booklet.

- Data may be at risk of compromise if application programming interface (API) protocols are not current. The bank's internal network and security architectures for mobile payment processing should consider API standards.
- Outdated technology may present risk of failure. Patch management and change control activities for mobile products and services are key for proper functionality.
- Mobile devices are often targeted with phishing, smishing, and malware attacks. Depending on the type of mobile device, security features and payment and security technologies may differ. Risk mitigants include having an understanding of network architecture, the design of the application, and threats to the application.
- Banks face increased difficulty in positively identifying and verifying the individual's identity and should have robust mobile payment product systems intended only for authorized users.

Risks Associated With Payment Systems

From a supervisory perspective, risk is the potential that events will have an adverse effect on a bank's current or projected financial condition[33] and resilience.[34] The OCC has defined eight categories of risk for bank supervision purposes: credit, interest rate, liquidity, price, operational, compliance, strategic, and reputation. These categories are not mutually exclusive. Any product or service may expose a bank to multiple risks. Risks also may be interdependent and may be positively or negatively correlated. Examiners should be aware of and assess this interdependence. Examiners also should be alert to concentrations that can significantly elevate risk. Concentrations can accumulate within and across products, business lines, geographic areas, countries, and legal entities. Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for an expanded discussion of banking risks and their definitions.

The risks associated with payment systems include operational, strategic, credit, liquidity, compliance, and reputation.

Payment systems risk includes potential loss or harm to those entities or individuals that send or receive payments or information about payments, such as a bank's customers or third parties. Enhanced technology capabilities have enabled banks to meet the demands of the modern economy by delivering faster payments. More banks are offering solutions that provide payments to consumers and businesses with the option of same-day settlements.

As the payments ecosystem and operating systems continue to evolve with new products, services, participants, and partnerships, so do the risks. Accordingly, it is important for a bank's risk management practices and internal controls to evolve and keep pace with changes in the bank's payment systems, products, and services. Effective communication between stakeholders, both internal and external, is key to payment systems risk management.

[33] Financial condition includes impacts from diminished capital and liquidity. Capital in this context includes potential impacts from losses, reduced earnings, and market value of equity.

[34] Resilience recognizes the bank's ability to withstand periods of stress.

Systemic risk to payment systems can result from the inability to clear and settle payments due to a disruption in the overall system. For example, an incident at one large participant could cause a chain reaction that affects the entire payment system. Events can be sudden or result from accumulated risks over time. Operational and liquidity risks are the primary risks that can lead to systemic payment systems risk. The interconnectivity between financial institutions and markets can contribute to financial shocks, which could have systemic impact. The losses in value or confidence in the financial system can have significant adverse effects on economic markets.

Operational Risk

Operational risk is the risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events. Operational losses may result from internal fraud; external fraud; inadequate or inappropriate employment practices and workplace safety; failure to meet professional obligations involving clients, products, and business practices; damage to physical assets; business disruption and systems failures; and failures in execution, delivery, and process management.

The quantity of operational risk and the quality of operational risk management are heavily influenced by the quality and effectiveness of a bank's system of internal controls. The quality of the audit function, although independent of operational risk management, is a key assessment factor. Audit can affect the operating performance of a bank by helping to identify and validate correction of weaknesses in risk management and internal controls. The quality of due diligence, risk management of third-party relationships, business continuity planning, and controls protecting the confidentiality, integrity, and availability of bank information are other key assessment factors for mitigating operational risk.

Operational risk is inherent in all banking products, activities, processes and systems, including payment systems. Operational losses can include fees or charges from unauthorized card, ACH, or other payment activity. Banks may be required to refund payments and related fees to customers and absorb losses; in some cases, these amounts may not be recoverable due to regulations, network rules, insufficient controls, or bank policies.

System disruptions or failures at the bank and its third parties (including FMIs) can delay processing, introduce errors, and introduce other risks, such as liquidity or credit risk. Even a short disruption in payment systems could have a widespread impact due to the large volume and value of transactions. Certain FMIs, such as CCP clearing houses for derivatives trading, have the potential to create a systemic risk in the event of operational failures due to the roles of their larger members. A bank's FMI memberships potentially expose the bank to uncapped liability for operational losses. For more information on payment system memberships, refer to the "Payment Systems Membership Requirements (12 CFR 7.1026)" section of this booklet.

Fraud Risk

Fraud risk is a form of operational risk.[35] Fraud can exist in any part of a payment transaction. Fraud during authentication is often referred to as identity theft. Fraud during authorization may be caused by a variety of internal or external sources. Exploitation of emerging technologies, increased use and availability of alternative payment methods and products, and cyber threats are some of the factors contributing to fraud and criminal activity.

Weak internal controls could allow opportunities for bank insiders to divert payments for their own benefit. Compromised credentials may be used to commit payment fraud across different online channels. Weak internal controls can also allow external fraud to occur unchecked. Check processing controls are important to prevent processing of fraudulent items. Fraud risk applies whether checks are processed traditionally, electronically, or through RDC. Fraudulent cashier's checks can be especially troublesome because of potential legal issues with respect to funds availability and reversing the deposit credit.[36]

Strategic Risk

Strategic risk is the risk to the current or projected financial condition and resilience of a bank resulting from adverse business decisions, inadequate implementation of the strategic plan, or lack of responsiveness to changes in the banking industry and operating environment.

Banks face increased competition from and are partnering with nonbank entities to provide new payment products and services. Banks can face pressure to rush new or innovative payment functionality to market to remain competitive. Premature introduction of a product or service can expose banks to unidentified and unanticipated risks. Effective strategic planning, risk management of new activities, and third-party risk management are essential to controlling the risks in offering new, modified, or expanded payment products and services or partnering with nonbank entities to do so.[37]

Credit Risk

Credit risk is the risk to the current or projected financial condition and resilience of a bank arising from an obligor's failure to meet the terms of any contract with the bank or otherwise fail to perform as agreed.

[35] For more information, refer to OCC Bulletin 2019-37, "Operational Risk: Fraud Risk Management Principles."

[36] For more information, refer to OCC Bulletin 2007-2, "Fraudulent Cashier's Checks: Guidance to National Banks Concerning Schemes Involving Fraudulent Cashier's Checks" (national banks).

[37] For more information, refer to OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles."

A bank assumes sender risk when it makes a payment on behalf of a customer by paying against uncollected or provisional funds or against insufficient balances. A bank can face receiver risk upon acceptance of funds from the sender when payments are credited to the customer before settlement. As the receiver of funds, a bank relies on the sender's ability to settle its obligations.

Credit risk is present when settlement or repayment depends on counterparty, issuer, or borrower performance. Credit risk exists when the provision of funds and settlement do not occur simultaneously. Credit risk in wholesale payments occurs primarily in the form of daylight (intraday) and overnight overdrafts. Banks often permit their corporate and public entity customers to incur daylight overdrafts, which are expected to clear by the end of the business day. Given the volume and value of transactions conducted by these entities, the overall credit risk exposure can be significant. Daylight overdrafts have the potential to become overnight overdrafts or overnight loans when the net of incoming and outgoing funds is negative at the end of the business day.

ACH origination, specifically, the origination of an ACH credit file, is a potential source of credit risk. For instance, a corporate customer's account may have insufficient funds when a payroll file settles because of the time lapse between origination and settlement. Once the ACH file is originated, it cannot be recalled and the ODFI may be required to take the funding account into an overdraft status. Banks usually mitigate this risk by requiring deposits, available credit, or an exception approval policy to be in place.

Returns are another source of credit risk. The payor's institution can return checks and ACH transfers for many reasons (e.g., insufficient funds, closed account, stop payment order, forgery, or fraud). ACH transfers create credit exposure to the receiving bank until the payor's bank can no longer return the ACH. Returns can result in credit risk, particularly if an overdraft results.

FMI memberships can lead to credit risk. In some cases, banks are contractually obligated to financially support the FMI in the event another member defaults. With CCP memberships,[38] a bank may be contractually obligated to cover losses incurred by the network or to assume certain liabilities for actions or omissions of the network, another member, or third parties. Depending on the agreement with the FMI or CCP, the total exposure can be limited to a certain amount or percentage of the total activity or the members can have open-ended liability.[39]

In wholesale payment and securities settlement systems, credit risk can take several forms and have multiple sources, including daylight overdrafts, settlement lags, principal risk, and loss-sharing provisions. Wholesale payment and securities settlement systems include financial intermediaries, financial services firms, and nonbank businesses that create, distribute, and process large-value payments. The bulk of these payments is generally used to

[38] Refer to 12 CFR 7.1026.

[39] For more information, refer to "Current Report of the Financial Market Infrastructure Risk Task Force," Federal Reserve Bank of New York (May 2007).

purchase, sell, or finance securities transactions; disburse or repay loans; settle real estate transactions; and make large-value, time-critical payments, such as interbank purchases and sales of federal funds, settlement of foreign exchange transactions, or other financial market transactions. Wholesale payments are irrevocable at final settlement. The payment system's rules and applicable laws determine what constitutes the final settlement.

Settlement risk is the possibility that the completion or settlement of transactions will not take place as expected. In addition to credit risk, settlement risk often includes elements of liquidity risk. Credit risk in the settlement process is present during the lag time between the origination of the payment and the final funding of the origination instructions. This risk can be significant in foreign exchange and securities transactions.

Specific to check processing, a bank is exposed to credit risk when processing checks for merchants, consumers, and third-party payment processors (TPPP). Additionally, a bank is exposed to credit risk through RDC processing, RDI, and check kiting.

RDIs are checks returned unpaid by the paying bank. If the paying bank does not honor or pay the processed checks, the checks will be returned to the BOFD. The BOFD is exposed to credit risk until final settlement occurs. Furthermore, if the funds credited to the customer from a check deposit are no longer in the customer's account when the RDI is received, the bank is exposed to potential loss.

Check kiting is a form of check fraud that involves a customer presenting checks at two or more financial institutions and using the uncollected funds while the items settle. In check kiting, the customer takes advantage of the time it takes to clear the checks (i.e., float time), in effect taking out an unauthorized and interest-free loan. Although float time has decreased with electronic advancements, check kiting remains a risk.

Liquidity Risk

Liquidity risk is the risk to current or projected financial condition and resilience arising from an inability to meet obligations when they come due.

The primary liquidity risk with payment systems is related to a bank's intraday liquidity positions under normal and stressed market conditions. Banks engaged in significant payment, settlement, and clearing activities that do not effectively manage intraday liquidity may be unable to meet payment and settlement obligations in a timely manner. For example, a primary aspect of liquidity risk in wholesale payments is the inability to settle daylight overdrafts. A daylight overdraft occurs when a bank's Federal Reserve account is in a negative position at any point during the business day. The Board of Governors of the Federal Reserve System's "Policy on Payment System Risk" has specific requirements that apply to banks using intraday credit.[40]

[40] For more information, refer to "Guide to the Federal Reserve Board's Payment System Risk Policy on Intraday Credit," "Overview of the Federal Reserve Board's Payment System Risk Policy," and "Federal Reserve Policy on Payment System Risk," Board of Governors of the Federal Reserve System.

Due to interdependencies within the payments ecosystem, settlement failures or interruptions have the potential to cause systemic disruptions, prevent the efficient functioning of the financial system, and amplify the liquidity risk posed by payment systems.[41] For example, banks are exposed to liquidity risk by their FMI memberships through the risk that a counterparty may be unable to meet fully its financial obligations when due. Certain large participants failing to meet their obligations in a timely manner could create a liquidity crisis if other members are dependent on those payments to meet their obligations.

Compliance Risk

Compliance risk can increase when a bank does not deliver payment products and services to bank customers as expected or disclosed. For example, inappropriate bank practices associated with delivering payment products and services could be deemed as unfair, deceptive, or both under section 5 of the Federal Trade Commission Act.[42] Payment products, services, and activities must comply with all applicable federal consumer protection laws and BSA/AML and OFAC requirements. Some common regulations relating to payments include Regulation CC (12 CFR 229), Regulation E (12 CFR 1005), and the BSA/AML requirements of the funds transfer recordkeeping and travel rules, 31 CFR 1010.410(a) and (f).

Compliance risk also increases when credit is extended explicitly, by granting a loan, or implicitly, by paying against uncollected or provisional funds or against insufficient balances. Regulation Z and the prepaid card provisions therein are particularly relevant when credit is extended in this manner.[43]

Compliance risk is generally higher for banks that have memberships in FMIs outside the domestic market. Having memberships outside the domestic market also exposes the bank to sovereign risk. For example, the imposition of exchange control regulations on a bank participating in international foreign exchange activities could result in compliance risk. Compliance risk from agreements with FMIs could be significant as some require indemnification from members to operators while also placing open-ended liability on the members. Banks can also be exposed to increased compliance risk when contracts with FMIs do not appropriately address the responsibilities of the bank, third parties, or customers.

This booklet does not include all compliance topics. Examiners should consider the specific products and services offered when determining the scope of compliance reviews related to payments. For more information regarding consumer protection-related laws and regulations, refer to the *Consumer Compliance* series of the *Comptroller's Handbook.* For more information about BSA/AML, refer to the *FFIEC BSA/AML Examination Manual.*

[41] For more information, refer to OCC Bulletin 2010-13, "Liquidity: Interagency Policy Statement on Funding and Liquidity Risk Management."

[42] Section 5 of the Federal Trade Commission Act is codified at 15 USC 45(a)(1). For more information, refer to the "Unfair or Deceptive Acts or Practices and Unfair, Deceptive, or Abusive Acts or Practices" booklet of the *Comptroller's Handbook*.

[43] Refer to 12 CFR 1026.61.

Reputation Risk

Reputation risk is the risk to current or projected financial condition and resilience arising from negative public opinion.

Reputation risk can occur when a bank does not deliver payment products and services as expected or disclosed. The bank's culture, protection of payment-related data, security of the bank's payment technology infrastructure, reliability of payment systems, and effectiveness of problem escalation and complaint resolution processes are important aspects of managing reputation risk. Failure to complete dependable payments can affect a bank's reputation. A bank's reputation can be harmed if it fails to protect the confidentiality and integrity of its customers' data.

Banks may be exposed to increased reputation risk through third parties and customer relationships. Products and services offered through third parties may expose a bank to increased reputation risk. Card memberships, third-party relationships, and FMI memberships can affect reputation risk because issues that affect these entities could potentially affect the bank and its customers. Similarly, actions of high-profile bank customers using bank products or services may affect a bank's reputation if the customer's activity results in negative outcomes.

Banks that facilitate ACH transactions for originators engaged in higher-risk activities can be exposed to increased reputation risk. Originators engaged in higher-risk activities could initiate transactions, alone or through third parties, that include companies engaged in potentially illegal activities or that have an unusually high volume of unauthorized returns.

Risk Management

Each bank should identify, measure, monitor, and control risk by implementing an effective risk management system appropriate for the bank's size, complexity, and risk profile. When examiners assess the effectiveness of a bank's risk management system, they consider the bank's policies, processes, personnel, and control systems. Refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook* for an expanded discussion of risk management.

Primary examination objectives are to understand how each bank identifies, measures, monitors, and controls the risks associated with payment systems, products, services, and activities and whether bank management has implemented effective risk management practices for the risks assumed. When assessing the effectiveness of a bank's payment systems risk management, the examiner should consider the bank's policies, processes, personnel, and control systems within payment channels and related technology systems.

An important aspect of payment systems risk management is managing the risks associated with payment systems memberships. Sound membership risk management includes evaluating memberships before new members join and on an ongoing basis thereafter. Specific requirements related to certain payment systems memberships are summarized in the "Payment Systems Membership Requirements (12 CFR 7.1026)" section of this booklet.

A common risk management framework includes the three lines of defense. While many banks have not formally adopted the three lines of defense, most banks have the basic elements. In small, noncomplex banks, risk management processes and internal controls are often integrated in the frontline units. In larger banks, the three lines of defense are more clearly defined and visible. The first line of defense, those responsible for executing day-to-day payment operations, is responsible for risk-taking and executing associated internal controls. The second line provides independent review, oversight, credible challenge, testing via control assessments, and assurance of the control environment. The third line of defense, internal audit, provides independent assurance that the risk management framework is operating effectively and verifies and validates the effectiveness of the first and second lines' execution of policies, processes, and controls.[44]

Policies and Procedures

Policies and procedures are key components of sound payment systems risk management. Policies set the standards established by the board and describe the governance structure and core elements of the bank's payment systems risk management. Policies should align with the bank's business strategy and risk appetite. While the board or a designated board committee is typically responsible for approving policies, management typically develops and implements the policies. The depth and breadth of a bank's policies and procedures

[44] For more information on the three lines of defense, refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook*.

depends on the scope and complexity of payment products, services, and activities. Effective policies and procedures typically include

- governance framework (e.g., committee structure).
- standard operating procedures.
- clearly defined roles and responsibilities for oversight of payment operations.
- descriptions of the payment products and services offered by the bank.
- description of the bank's processes for conducting payment risk assessments.
- risk limits consistent with the risk appetite. Limits are typically tailored to the transaction type (e.g., wire transfers, ATM withdrawals, mobile/RDC deposits, IAT, internet- or mobile-initiated ACH transactions (WEB), and telephone-initiated transactions (TEL)).
- risk monitoring and reporting requirements.
- credit risk management practices for payment products and services.
- compliance risk management practices for payment products and services.
- guidelines for complying with regulatory and contractual requirements.
- description of quality assurance practices.
- description of internal controls specifically designed for payment systems, products, and services.
- description of third-party risk management processes.
- exception review processes (e.g., limit exceptions and file errors).
- independent risk-based audit requirements.

Internal Controls

Policies and procedures should establish sound internal controls, including segregation of duties and dual controls regarding payment systems. Implementing appropriate controls is important to facilitate authorized, accurate, and timely payments processing and to prevent internal and external fraud. Reconcilement and transactional responsibilities should be properly segregated throughout a bank's operations. When dual controls and separation of duties are not well-designed, implemented, and enforced by the bank, the bank's operational risk increases significantly.

Internal controls are discussed throughout this booklet as they relate to various topics and particularly in the "Operational Risk Management" section. Examiners should assess internal controls for payments by completing the examination procedures.

Risk Assessment

Many banks perform an annual risk assessment for payment products and services, but risk assessments may be performed more frequently depending on the bank's size, complexity, and risk profile. An effective risk assessment typically

- identifies and assesses the risks associated with existing and planned payment products and services.

- confirms that current payment products and services remain aligned with the bank's overall strategy and risk appetite.
- assesses whether appropriate controls are in place to mitigate existing, emerging, or changing risks associated with a bank's payment products, services, and activities.
- includes the payment infrastructure supporting all products and services offered by the bank.

Management and Board Reports

Timely, accurate, relevant, and complete reports regarding payment systems are essential for effective management and board oversight. Specific reporting needs may vary based on board and management expectations but generally depend on the bank's size, complexity, and risks. Effective reporting facilitates a timely and accurate assessment of risks associated with payment systems and promotes sound risk management. Reporting typically includes risk appetite monitoring and trend analyses for existing and new activities. Examples of information that may be in management or board reports include

- performance against established limits or triggers, key performance indicators (KPI), and key risk indicators (KRI) such as
  - STP rates.
  - capacity monitoring.
  - chargeback and return (e.g., unauthorized, invalid, total) volume and trends by product.
  - return rates by originator, including third-party senders.
  - volume and dollar value to benchmarks.
  - operating margins.
  - performance to risk tolerance limits and industry thresholds.
  - portfolio composition to industry levels.
  - portfolio stratification by exposure limits and risk rating.
  - expired exposure limits.
  - network rule violations.
  - fraud losses by volume and payment product or service.
  - operational losses, near misses, and related post-mortem analysis.
  - service-level agreement (SLA) exceptions or violations.
  - capital positions relative to the volume of overall payments and broken down by payment products and originators.
  - complaint volumes and trends, including complaint information about or received by third parties.
  - policy exception rates or volume.
- financial reports.
- list of third-party senders.
- list of higher-risk customers (e.g., for BSA/AML purposes).
- analysis of top customers by volume and revenue.
- system outages, including post-mortem assessments.

- processing delays.
- daylight overdraft monitoring reports.
- risk assessment results (e.g., operational, credit, liquidity, compliance, and fraud).
- information regarding the performance of critical third parties.
- internal and external audit results.
- outstanding issues and the status of corrective actions, including outstanding management self-identified issues, rule violations, audit findings, and regulatory findings.
- policy exceptions.
- status and results of risk and control self-assessments.
- significant incidents and associated root cause analysis.
- notices of potential and actual breaches of payment system operating rules or breaches of contracts.
- status of projects that affect payment systems.
- patch management status reports.
- analysis reporting on new or established products (e.g., adoption rates).
- terminations (e.g., ACH originators and customers).
- customers with ACH direct access.

Staffing

Appropriate staffing and training can reduce the likelihood of human error, provide for the timely identification of potentially fraudulent activity, and help prevent operational losses. Examiners should assess the adequacy of payment staffing in terms of sufficient depth, breadth, and skill level. Industry practices often includes a skills assessment performed for the payment operations staff to determine proper competencies. Staffing and training programs should provide foundational knowledge, skills, and tools for the bank's staff to remain knowledgeable and effective at performing their responsibilities.

Compensation practices for the bank's executive officers and employees should be safe and sound, consistent with prudent compensation practices, and comply with laws and regulations. Banks are required to maintain safeguards to prevent the payment of compensation, fees, and benefits that are excessive or that could lead to material financial loss to the bank.[45] If it is unreasonable or disproportionate to the services actually performed, compensation is considered excessive and is therefore prohibited as an unsafe or unsound practice.[46]

[45] For more information, refer to 12 CFR 30, appendix A, section II, I, "Compensation, Fees and Benefits."

[46] For more information, refer to 12 CFR 30, appendix A, III, "Prohibition on Compensation That Constitutes an Unsafe and Unsound Practice." Also refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook* and OCC Bulletin 2010-24, "Incentive Compensation: Interagency Guidance on Sound Incentive Compensation Policies."

Strategic Planning and New Activities

Effective strategic planning is an important foundation for controlling the risks associated with payment products and services. Examiners should determine how management and the board assess and oversee the strategic risk associated with changes in regulations, industry standards, the macroeconomic environment, merger and acquisition activities, sovereign risks, and other market developments that could affect the bank's payment products and services.

Bank management typically determines which payment products and services most appropriately align with the bank's strategic vision, goals, risk tolerance, and business model. The board would typically establish the risk appetite relative to payment products and services.

When a bank has engaged in significant new activities, examiners should assess how management understands and assesses the risks associated with substantial market expansion, the addition of new activities, the technologies used for different payment products and services (e.g., cloud computing and real-time payments), and reliance on third parties. New activities should be developed and implemented consistent with sound risk management practices and should align with the bank's overall business plan and strategy. Appropriate controls should be in place before engaging in new activities. Sound risk management includes periodically verifying that internal controls keep pace with changes in payment products and services.[47]

Banks continue to evaluate and adopt innovative technologies, such as artificial intelligence (AI), machine learning (ML), and DLT. Banks seek to use these technologies in facilitating transactions, customer interaction, and fraud detection as they relate to payment systems. The OCC recognizes that banks have a long history of introducing new activities; those activities might rely on new platforms for payments-related products and services. In recent years, the financial services industry has experienced growth in bank and nonbank participation and competition in offering these services, especially with the application of financial technology (fintech) in payment systems.

Internal Audit

The depth and breadth of a bank's audit activities related to payment systems, products, and services depend on the complexity of the bank's operations and the nature and extent of the bank's payment systems, products, and services. The audit program should be risk-based and include current, potential, new, or modified activities related to payments. Common audit program weaknesses regarding payment systems, products, and services include inadequate coverage as well as lack of audit staff expertise and training.

Growth, new activities, underwriting policies, customer due diligence, and customers' online access to the payment networks (if provided) are key considerations when determining the

[47] For more information about risk management of new activities, refer to OCC Bulletin 2017-43.

appropriateness of audit's scope. If a bank provides ACH payment services, Nacha requires an annual Rules Audit. This audit may be performed by the bank's audit function or a third party. The Nacha Rules Audit is only one element of an effective ACH audit program and is not a substitute for a comprehensive, risk-based audit.

Effective audit programs promote the integrity of the membership risk management processes. The contract with the FMI should include provisions that permit the bank to perform audits, as needed, to monitor performance and evaluate conformance with payment system membership rules and compliance with applicable laws and regulations.

The audit function should be staffed appropriately with auditors who have sufficient expertise to evaluate all aspects of the payment systems, products, and services. Effective audit plans may be achieved with multiple audits that evaluate various risk areas, products, services, and business lines. Examiners should determine whether auditors have sufficient expertise and training to carry out the bank's audit activities and whether the audits are performed by internal audit staff or outsourced.

Third-Party Risk Management

Banks may engage third parties for various aspects of payment systems, products, and services. Examples of payments-related third-party relationships include payment processors, ACH service providers, merchant (card) processors, RDC service providers, correspondent banks, affinity card program managers, ATM providers, and lock box service providers. Holding companies and affiliates that provide banks with services related to payment systems are also third parties that would be incorporated into a bank's third-party risk management processes. For example, payment operations may be performed by the holding company. Additionally, affiliates under the same holding company may specialize in a specific operation and perform the service for the other affiliates.

Use of third parties reduces management's direct control of activities and may introduce new risks or increase existing risks, specifically, operational, compliance, reputation, strategic, and credit risks and the interrelationship of these risks. Increased risk most often arises from greater complexity, ineffective risk management by the bank, and inferior performance by the third party. Processes and controls that are outsourced should be maintained to the same standard as those activities the bank conducts internally. The use of third parties does not diminish the board of directors and senior management's responsibilities to ensure that payment activities are performed in a safe and sound manner and in compliance with applicable laws and regulations.

As discussed in OCC Bulletin 2013-29 and in OCC Bulletin 2020-10, the OCC expects bank management to identify, measure, monitor, and control the risks associated with third-party relationships). Third-party risk management includes planning, due diligence, contract negotiation, ongoing monitoring, and termination. Examiners should consider the following

focal points when assessing payments-related third-party relationships:[48]

- Whether a bank's due diligence
  - assesses a third party's ability to provide the contracted services.
  - evaluates the third party's legal and regulatory compliance program to determine whether the third party has the necessary licenses to operate and the expertise, processes, and controls to enable the bank to remain compliant with domestic and international laws and regulations.
  - evaluates the third party's risk management and information security programs. This generally includes evaluating the third party's processes and controls for transmitting and storing sensitive payment information, authentication, authorization, and fraud detection.[49]
  - assesses a third party's ability to respond to service disruptions or degradations resulting from natural disasters, human error, or intentional physical or cyber attacks.
  - determines whether the third party maintains disaster recovery and business continuity plans that specify the time frame to resume activities and recover data.
  - includes a review of the third party's telecommunications redundancy and resilience plans and preparations for known and emerging threats and vulnerabilities, such as wide-scale natural disasters, distributed denial of service attacks, or other intentional or unintentional events.
  - includes a review of the results of business continuity testing and performance during actual disruptions.
  - includes monitoring and analyzing customer complaints about or received by third parties.
- Whether contracts with third parties
  - specify the rights and responsibilities of each party.
  - specify performance measures that define the expectations and responsibilities for both parties including conformance with regulatory standards or rules. Performance measures should not incentivize undesirable performance, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on customers. Industry standards for service-level agreements may provide a reference point for standardized services, such as payroll processing.
  - address compliance with the specific laws, regulations, guidance, and self-regulatory standards applicable to the activities involved, including provisions that outline compliance with certain provisions of the Gramm–Leach–Bliley Act (GLBA) (including privacy and safeguarding of customer information), BSA/AML, OFAC, and other applicable laws, regulations, and rules.
  - require the third party to provide and retain timely, accurate, and comprehensive information such as records and reports that allow bank management to monitor performance, service levels, and risks.

[48] Refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," and OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," for a full discussion of the OCC's third-party risk management expectations. Refer also to OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures."

[49] Refer to OCC Bulletin 2016-18.

  - prohibit the third party and its subcontractors from using or disclosing the bank's information, except as necessary to provide the contracted activities or comply with legal requirements.
  - specify when and how the third party will disclose, in a timely manner, information security breaches that have resulted in unauthorized intrusions or access that may materially affect the bank or its customers.
  - establish the bank's right to audit.
  - provide for continuation of the business function in the event of problems affecting the third party's operations, including degradations or interruptions resulting from natural disasters, human error, or intentional attacks.
  - require the third party to provide the bank with operating procedures to be carried out in the event business resumption and disaster recovery plans are implemented.
  - include specific time frames for business resumption and recovery that meet the bank's requirements, and when appropriate, regulatory requirements.
  - stipulate whether and how often the bank and the third party will jointly practice business resumption and disaster recovery plans.
- The adequacy of the bank's ongoing monitoring of third parties and whether monitoring is commensurate with the nature of the third-party relationship and associated activities.
- How bank management considers concentrated reliance on a third party.

Payment Systems Membership Requirements (12 CFR 7.1026)

From time to time, banks may seek payment system memberships. Management might consider doing so to provide additional services to the bank's customers and more convenient ways to transfer funds. Banks must, however, comply with certain requirements related to payment systems membership. Risk management of payment system memberships involves evaluating memberships before joining as well as on an ongoing basis. Banks must comply with 12 CFR 7.1026 regarding payment system memberships. 12 CFR 7.1026 applies to a bank's membership in payment systems that meet the definition of a "financial market utility" as defined in 12 USC 5462(2), and includes both retail and wholesale payment systems.[50] Appendix A of this booklet includes a worksheet that examiners may use to review a bank's compliance with 12 CFR 7.1026.

Notice Requirements (12 CFR 7.1026(c) and (d))

A bank must provide written notice to the OCC before or after becoming a member of a payment system, as defined in the OCC's rules. Whether the notice must be submitted before or after the fact depends on whether the payment system would expose the bank to open-ended liability versus limited or no liability.[51] Open-ended liability refers to liability for operational losses that is not capped under the rules of the payment system and includes

[50] For the purposes of 12 CFR 7.1026, "payment system" does not include a derivatives clearing organization registered under the Commodity Exchange Act, a clearing agency registered under the Securities Exchange Act of 1934, or a foreign organization that would be considered a derivatives clearing organization or clearing agency if it were operating in the United States. Refer to 12 CFR 7.1026(b)(5), "Payment System."

[51] Refer to 12 CFR 7.1026(c)(1), "Notice Requirements."

indemnifications of third parties provided as a condition of membership in the payment system.[52]

Prior Notice

The bank must provide written notice to the appropriate OCC supervisory office 30 days before joining a payment system that would expose the bank to open-ended liability.[53] The notice must include representations that the bank[54]

- has complied with the safety and soundness review requirements in 12 CFR 7.1026(e)(1).
- will comply with the safety and soundness review and notification requirements in 12 CFR 7.1026(e)(2) and (3).

After-the-Fact Notice

If the payment system does not expose the bank to open-ended liability, a bank must provide after-the-fact written notice within 30 days of becoming a member of the payment system.[55] The notice must include[56]

- representations that the bank has complied with the safety and soundness review requirements in 12 CFR 7.1026(e)(1).
- representations that the bank will comply with the safety and soundness review and notification requirements in 12 CFR 7.1026(e)(2) and (3).
- a representation that either[57]
  - the rules of the payment system do not impose liability for operational losses on members, or
  - the bank's liability for operational losses is limited by the rules of the payment system to specific and appropriate limits that do not exceed the lower of
    - the legal lending limit under 12 CFR 32.
    - the limit set for the bank by the OCC.

[52] "Open-ended liability" is defined at 12 CFR 7.1026(b)(3). Refer to 12 CFR 7.1026(d)(4) for the definition of "operational loss."

[53] Refer to 12 CFR 7.1026(c)(1), "Prior Notice Required."

[54] Refer to 12 CFR 7.1026(d), "Content of Notice."

[55] Refer to 12 CFR 7.1026(c)(2), "After-the-Fact Notice."

[56] Refer to 12 CFR 7.1026(d).

[57] Refer to 12 CFR 7.1026(d)(2), "Payment System With Limits on Liability or No Liability."

Safety and Soundness Procedures (12 CFR 7.1026(e))

Before joining a payment system, the bank must[58]

- identify and evaluate the risks posed by membership in the payment system, taking into account whether the liability of the bank is limited.
- ensure it has the ability to measure, monitor, and control the risks identified pursuant to 12 CFR 7.1026(e)(1)(i).

After joining a payment system, the bank must manage the risks of the payment system on an ongoing basis. This ongoing risk management must[59]

- identify and evaluate the risks posed by membership in the payment system, taking into account whether the liability of the bank or savings association is limited.
- measure, monitor, and control the risks identified pursuant to 12 CFR 7.1026(e)(2)(i).

If the bank identifies risks during the ongoing risk management that raise safety and soundness concerns, such as a material change to the bank's liability or indemnification responsibilities, the bank must notify the appropriate OCC supervisory office as soon as the safety and soundness concern is identified and take appropriate actions to remediate the risk.[60]

The rules of some payment systems may expose members to open-ended liability for operational losses but, in reality, the bank's liability is capped in some other way. For example, a jurisdiction could have a law that prohibits open-ended liability or restricts the amount of liability to the assets located in that jurisdiction. If that law applies to the payment system, it could effectively cap a member's operational liability. In other situations, a bank may negotiate an agreement with a payment system that allows the bank to limit its potential liability.

A bank that believes its open-ended liability is otherwise limited (e.g., by negotiated agreements or laws of an appropriate jurisdiction) may consider its liability to be limited for purposes of reviews required by 12 CFR 7.1026(e)(1) and (2) if, before joining the payment system, the bank obtains a written legal opinion that[61]

- describes how the payment system allocates liability for operational losses.
- concludes that the potential liability for operational losses for the bank is in fact limited to specific and appropriate limits that do not exceed the lower of the
  - legal lending limit under 12 CFR 32.

[58] Refer to 12 CFR 7.1026(e)(1).

[59] Refer to 12 CFR 7.1026(e)(2).

[60] Refer to 12 CFR 7.1026(e)(3).

[61] Refer to 12 CFR 7.1026(e)(4).

- the limit set for the bank or savings association by the OCC.

After obtaining the written legal opinion, the bank may continue to consider its liability to be limited for purposes of the reviews required by 12 CFR 7.1026(e)(1) and (2) if there are no material changes to the liability or indemnification requirements applicable to the bank since the issuance of the written legal opinion.[62] A written legal opinion is not required to join a payment system in all instances. A written legal opinion is only required when the bank plans to treat its liability as limited when the payment system's rules would otherwise indicate that members are subject to open-ended liability. The legal opinion option is likely to be exercised rarely and offers an additional option for banks wanting to join a payment system where the rules reflect open-ended liability but the bank believes another factor (such as the examples described in this section of the booklet) would limit its potential liability.[63]

Safety and Soundness Considerations (12 CFR 7.1026(f))

A bank should evaluate, at a minimum, the following payment system characteristics when conducting an analysis as required by 12 CFR 7.1026(e):[64]

- Does the processing occur on a real-time gross settlement basis or provide reasonable assurance (e.g., prefunding) that members will meet settlement obligations?
- How do the payment system's rules limit its liability to members?
- Does the payment system have insurance coverage and/or self-insurance arrangements to cover operational losses?
- Do the payment system's rules provide an unambiguous pro-rata loss allocation methodology under its indemnity provisions and does the methodology provide members the opportunity to reduce or eliminate liability exposure by decreasing or ceasing use of the payment system?
- Do the payment system's rules provide for unambiguous membership withdrawal procedures that do not require the prior approval of the system?
- Does the payment system have appropriate admission and continuing participation requirements for system participants? Such requirements should address, among other things,
  - the participants' access to sufficient financial resources to meet obligations arising from participation.
  - the adequacy of participants' operational capacities to meet obligations arising from participation.
  - the adequacy of the participants' own risk management processes.
- Does the payment system have processes and controls in place to verify and monitor on an ongoing basis the compliance of each participant with admission and participation requirements?

[62] Refer to 12 CFR 7.1026(e)(4)(ii).

[63] For more information, refer to 85 Fed. Reg. 83686 and 83702.

[64] Refer 12 CFR 7.1026(f)(1).

- Does the payment system have written policies and procedures for addressing participant failures to meet ongoing participation requirements?
- Are the payment system's rules relating to the system's emergency authorities unambiguous and may they be amended or otherwise altered without prior notification to all members and an opportunity to withdraw?
- Is the payment system governed by uniform, comprehensive, and clear legal standards in its operating jurisdiction that address payment and/or settlement activities?
- Is the payment system subject to and in compliance (or observance) with the Committee on Payment and Settlement Systems and the Technical Committee of the International Organization of Securities Commissions (CPSS—IOSCO) Principles for Financial Market Infrastructures?
- Is the payment system designated as a systemically important financial market utility (SIFMU) by the Financial Stability Oversight Council (FSOC) or is it the international or foreign equivalent?
- Does the payment system provide members with information relevant to governance, risk management practices, and operations in a timely manner and with sufficient transparency and particularity for the bank to ascertain with reasonable certainty the bank's level of risk exposure to the system?
- Is the payment system operated by or subject to oversight of a central bank or regulatory authority?
- Is the payment system legally organized as a nonprofit enterprise or is it owned and operated by a government entity?
- Does the payment system have appropriate systems and controls for communicating to members in a timely manner about material events that relate to or could result in potential operational losses (e.g., fraud, system failures, or natural disasters)?
- Has the payment system ever exercised its authority under indemnification provisions?

A bank should consider, at a minimum, the following characteristics of its risk management program when conducting analysis required by 12 CFR 7.1026(e):[65]

- Does the bank have appropriate board supervision and managerial and staff expertise?
- Does the bank have comprehensive policies and operating procedures with respect to its risk identification, measurement, and management information systems that are routinely reviewed?
- Does the bank have effective risk controls and processes to oversee and ensure the continuing effectiveness of the risk management process? The program should include a formal process for approval of payment system memberships as well as ongoing monitoring and measurement of activity against predetermined risk limits.
- Does the bank's membership evaluation process include assessments and analyses of
  - the credit quality of the entity?
  - the entity's risk management practices?
  - settlement and default procedures of the entity?
  - any default or loss-sharing precedents and any other applicable limits or restrictions of the entity?

[65] Refer 12 CFR 7.1026(f)(2).

  - key risks associated with joining the entity?
  - the incremental effect of additional memberships in aggregate exposure to payment system risk?
- Does the bank's risk management program include policies and procedures that identify and estimate the level of potential operational risks, at both inception of membership and on an ongoing basis?
- Does the bank have auditing procedures to ensure the integrity of risk measurement, control, and reporting systems?
- Does the program include mechanisms to monitor, estimate, and maintain control over the bank's potential liabilities for operational losses on an ongoing basis? This should include
  - limits and other controls with respect to each identified risk factor.
  - reports generated throughout the processes that accurately present the nature and level(s) of risk taken and demonstrate compliance with approved policies and limits.
  - identification of the business unit and/or individuals responsible for measuring and monitoring risk exposures, as well as those individuals responsible for monitoring compliance with policies and risk exposure limits.
- Does a bank with memberships in multiple payment systems have the ability to monitor and report aggregate risk exposures and measurement against risk limits both at the sponsoring business line level and the total exposure organizationally?

Supervisory Review of Payment Systems Membership Requirements

The OCC supervisory office should acknowledge receipt of a bank's notice under 12 CFR 7.1026 within five days.[66]

Examiners should review the correspondence for the requisite information and respond with questions or additional requests from the bank. For instance, if the bank has provided a notice that includes all required information, the acknowledgement of receipt may be the only written response. Examiners should expect to see supporting documentation that includes documentary evidence of previously mentioned items; due diligence; copies of the rules of the payment system (translated into English, if necessary); reports of internal bank review; credible challenge; and approval. Examiners should consider whether the information provided warrants further inquiry or increased supervisory review.

If a bank reports that it identified safety and soundness concerns, the supervisory office may have questions or additional requests for information required to understand the nature of the safety and soundness concern and determine the appropriate supervisory response.

Automated Clearing House Direct Access

ACH operator direct access allows an originator, third-party sender, or third-party service provider to transmit debit or credit transaction files directly to the ACH operator using the

[66] These procedures are consistent with the OCC's processes for written communications, as explained in the "Bank Supervision Process" booklet of the *Comptroller's Handbook*.

bank's routing number and settlement account. Banks that permit direct access are exposed to increased operational, compliance, credit, and liquidity risk due to the potential lack of transparency and due diligence when the entity with direct access conducts ACH transactions.

Comprehensive procedures and strong controls, including thorough underwriting, effective monitoring of the originator's activity, and ongoing monitoring of the originator's relationships with downstream customers, are essential to effectively managing direct access relationships. Direct access relationships should be approved by the board or a board-level committee before initiating ACH file entries. The bank should maintain control over its settlement accounts at all times. A written contract should be in place with the party granted access. The contract should, at a minimum, outline the rights and responsibilities of all parties, and include provisions permitting the bank to perform audits, as needed, to monitor performance, evaluate compliance with applicable laws and regulations and include termination provisions. Contracts usually include[67]

- a requirement that the party granted access obtain the bank's prior approval before originating ACH transactions under the bank's routing number.
- bank-established dollar limits for files that the party granted access transmits to the ACH operator. A file that exceeds these dollar limits should be brought to the bank's attention before being transmitted.
- a provision that restricts the other party's ability to initiate corrections to files. The bank should implement with the ACH operator risk-control measures that limit the correction ability of the party granted access. If bank management allows the other party to correct files, it should impose and enforce strict controls over these corrections.

Nacha Operating Rules and Guidelines require banks to register certain direct access relationships. The direct access registrations promote due diligence and banks' adherence to risk management practices.[68]

Automated Clearing House Third-Party Service Providers and Third-Party Senders

A third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise, and generally does not include arrangements between a bank and its customers.[69] Although most ACH business arrangements are considered third-party

[67] For more information, refer to OCC Bulletin 2006-39, "Automated Clearing House Activities: Risk Management Guidance."

[68] More information regarding direct access registration requirements is available on Nacha's website.

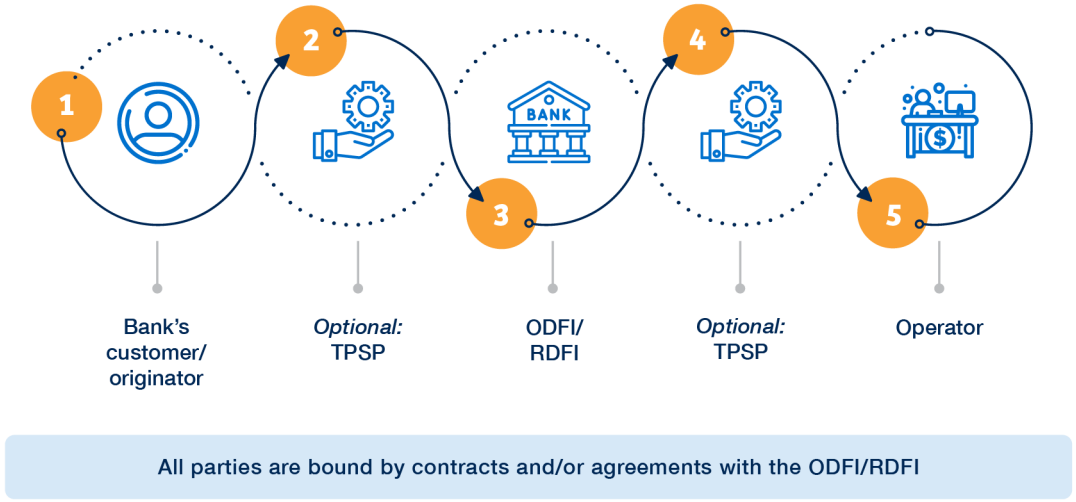
[69] For more information, refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance."

relationships, third-party senders (TPS) are bank customers and are generally not considered a third party under the OCC's definition of a third-party relationship.[70]

A third-party service provider (TPSP), under the Nacha Operating Rules and Guidelines, is an entity that performs functions within the ACH process on behalf of the originator, ODFI, or RDFI. The TPSP may process entries, create entries, or act as a sending point or receiving point on behalf of the participating financial institution.[71]

An ACH originator acting as a TPS is also a TPSP.

Figure 5: Third-Party Service Provider Transaction and Settlement Flow



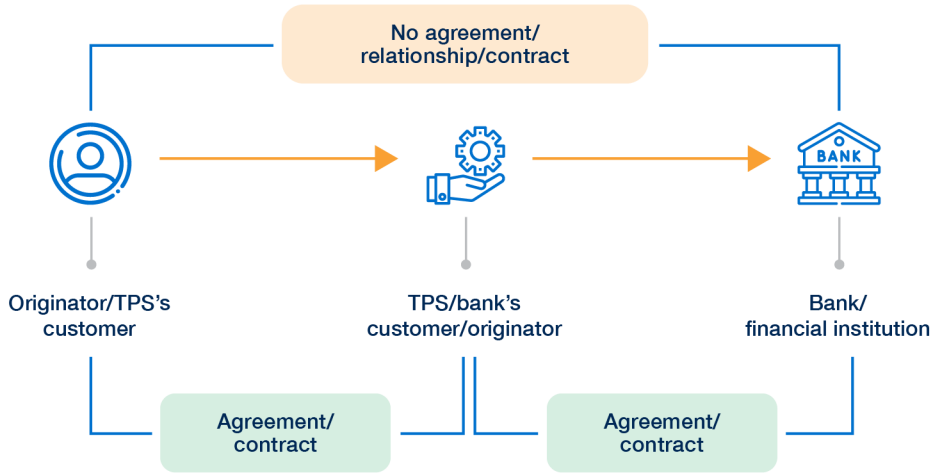
Under the Nacha Operating Rules and Guidelines, a TPS is a type of TPSP that acts as an intermediary between an originator and an ODFI. A TPS may also be referred to as a payment processor. Although the TPS is the bank's originating commercial customer, this customer acts on behalf of other originators or TPSs that have no banking relationship with the TPS's bank, the ODFI. In accordance with the Nacha Operating Rules and Guidelines, as the intermediary, the TPS must have an origination agreement with the ODFI.[72] As the intermediary, the TPS is never the originator for ACH entries that it transmits on behalf of another organization; however, the TPS may originate its own ACH entries when acting on its own behalf.

[70] For more information, refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance."

[71] For more information, refer to the Nacha Operating Rules and Guidelines.

[72] For more information, refer to Nacha Operating Rules and Guidelines Rule 2.2.2.2.

Figure 6: Third-Party Sender Transaction Flow



Due to the lack of transparency over the transactions or the entities for which the TPS is originating ACH entries, a TPS may be viewed as a higher-risk originator by its bank, the ODFI. A common example of a bank and TPS-customer relationship would be a company that engages a TPS to process the company's payroll. The company does not have an account with the ODFI, so it hires the TPS to process the entries on the company's behalf.

For more information, refer to OCC Bulletin 2006-39, "Automated Clearing House Activities: Risk Management Guidance."

Mobile Payment Risk Management

The risks and internal controls associated with mobile payments are discussed in detail in appendix E, "Mobile Financial Services," of the *FFIEC IT Examination Handbook's* "Retail Payment Systems" booklet. As described in appendix E of the "Retail Payment Systems" booklet, management should identify the risks associated with the types of mobile financial services offered as part of the bank's strategic plan. Management should incorporate the identification of risks associated with mobile devices, products, services, and technologies into the bank's risk management processes. Some of the primary risks associated with mobile payments include unsecured data storage (e.g., lost or stolen devices, virus infections on devices, lack of data encryption (in motion and at rest)) and weak server-side controls (e.g., weak security and authentication controls).

Internal controls for mobile payment products predominantly involve logical controls throughout network and transmission systems. Network and transmission systems include cryptographic systems, user profiles, password and authentication, device and near field communications, and core processing.

Internal controls remain relevant to mobile payment products since oversight and performance reporting is necessary for effective senior management decision making. Since

customer trial and general ledger balances are affected by daily transactions, reconciliations and separation of duties are key internal controls for mobile payments.

Banks' risk assessments typically address both standard and unique operational risks associated with mobile device features. Different types of mobile devices have different security features and support different payment and security technologies. Examiners should assess how a bank tailors security controls for mobile payments to the specific risks.

The risk identification process should include risks at the bank and those associated with the use of mobile devices for which the customer implements and manages the security settings. In providing customers with avenues for performing banking activities through mobile devices, a bank may transfer to the customer the ability to implement security settings. This transfer increases dependence on the customer to manage the controls over sensitive financial data. Additionally, there are numerous types of mobile devices that present different risks, and management should identify unique risks associated with specific devices. Before implementing mobile products and services, management should identify the associated risks, particularly in the areas of strategic, operational, compliance, and reputation risks. Many banks have implemented customer awareness programs regarding mobile payments. A common threat to mobile payments is phishing. Customer awareness programs often include information about the finality of P2P payments, especially when the recipient's account is at another institution. An absent or poorly designed customer education program can increase reputation risk if customers are susceptible to fraud or do not understand the liability for P2P payments.

Operational Risk Management

Operational risk management includes identifying, measuring, monitoring, and controlling operational risk associated with payment systems, products, and services. Important operational risk management factors include the adequacy of the bank's governance framework, audit function, system of internal controls, risk management of third-party relationships, business continuity management, IT risk management, and information security controls.

In small or noncomplex banks, operational risk management is generally less formal than in large or complex banks. Effective key controls may be achieved through various methods including independent review, compliance testing, completing risk control self-assessments (RCSA), and audit. The independence of these functions is important; in less-complex banks where a second line of defense is often not clearly defined, these functions may be performed by a unit or individual independent of the target function. RCSAs typically identify key risks and associated mitigating internal controls, establish testing protocols, and include issue reporting and escalation. RCSAs are commonly used to assess the internal control environment and designed and executed to check the effectiveness and identify gaps within the internal control system at the first line of defense. If the bank identifies weaknesses, gaps or deviations between policies, procedures, and practices, examiners would likely observe this within related reporting documentation.

Internal controls[73] for payment systems should include dual controls and segregation of duties throughout the bank's payment operations. Appropriate approvals and authorizations are especially important for controlling payment systems risk. Reconciliation and transactional duties should include independent verification processes designed to prevent fraud or misuse.

Information and Cybersecurity

Information security promotes the objectives of confidentiality, integrity, and availability of information.[74] Payment systems typically contain confidential customer information subject to the interagency information security guidelines.[75] The interconnectivity of payment systems with public and other networks can heighten information and cybersecurity risks, such as when bank customers are permitted direct access to the bank's network. Strong security controls to properly identify and authenticate internal bank administrators and users as well as customers are essential to protecting against external threats and data loss.[76] Network controls should be implemented to monitor network traffic, segregate networks containing payment applications and transactions, and alert bank management to suspicious activity. Additionally, card association rules typically require bank management to attest that security controls exist and that established practices conform to the Payment Card Industry Data Security Standards (PCI DSS).

The following are examples of important aspects of information and cybersecurity related to payment systems:

Patch and version control management: Examiners should determine how the bank remains as current as possible with respect to patch updating. Unpatched or non-current software or hardware version components can lead to unwarranted risks, payment system failure, and a likelihood of data intrusions if not addressed in a timely and effective manner. If a bank has not maintained current patches and software versions, updates should be prioritized to the highest-risk components, such as system components involving payment platforms or authorizations.

Service-level agreement expectations (third-party relationships including cloud arrangements): Examiners should assess whether contracts require third parties to provide safe, sound, continuous, and reliable service to systems that process payments or interface with payment applications. Many of these services are provided under cloud computing

[73] For more information, refer to the "Internal Control" booklet of the *Comptroller's Handbook* (national banks) and *Office of Thrift Supervision Examination Handbook* section 340, "Internal Control" (federal savings associations).

[74] For more information, refer to the "Information Security," "Retail Payment Systems," and "Wholesale Payment Systems" booklets of the *FFIEC IT Examination Handbook.*

[75] Refer to 12 CFR 30, appendix B, "Interagency Guidelines Establishing Information Security Standards."

[76] Refer to OCC Bulletin 2021-36, "Information Security: FFIEC Statement on Authentication and Access to Financial Institution Services and Systems."

agreements. Examiners should assess whether management determines if real-time failover[77] redundancy and transmission security responsibilities are appropriately identified and managed under these agreements. When they are not, the business impact analysis and business continuity management (BCM) program may not align with service-level expectations. If changes are material or gaps identified, additional or new testing under the BCM program may be warranted.

Escalation of security event controls and reporting: Security escalation procedures and response programs should exist within the bank's information security program. These policies and procedures should include security-related events involving payment systems and platforms as part of the bank's routine escalation posture when events warrant. These events might include cyber attacks, identity theft, phishing attacks, or malicious intrusion events that affect payment systems, platforms, and infrastructure.

Strategic and tactical planning for future payment products and services: Examiners should assess how management approaches new activities. When venturing into new activities, consideration of security implications and risks posed by the product or service is important. Examiners should assess how bank management considers the infrastructure and architecture of the current system including the version levels, key software interfaces, transmission capabilities, and security reporting controls. For example, if management considers offering mobile application banking capability to the bank's customers, the bank's general network operating architecture would normally need to be API[78]-compliant before these services can be implemented. API can facilitate building software applications used on mobile platforms, such as tablet or smartphone device technology. The latest versions or patch updates should be running throughout the bank's network environment, core software applications, security and routing appliances, and graphical user interfaces. Without running the most current software versions, a bank's ability to compete and scale mobile payment solutions could be impaired.

Management and board reports: Management reporting may include system performance, capacity, and security events of network and database resources used to process, transmit, and control payment-related activities. Refer to the "Management" booklet of the *FFIEC IT Examination Handbook* for more information on reporting.

[77] The *FFIEC IT Examination Handbook* Infobase Glossary refers to the National Institute of Standards and Technology definition of failover as the capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.

[78] API stands for application programming interface.

Business Continuity Management

BCM[79] is the strategic-level process that involves policies and procedures for coordinating activities used to keep a bank operating during unplanned events and to minimize downtime and disruption. The primary purpose of BCM is to articulate an enterprise-wide management strategy that coordinates all key operational, human, and system infrastructures. Operational resiliency and recovery of payment systems and platforms are important for the safety and soundness of all banks. Because of the critical role payment systems play, BCM should address all payment systems and supporting network architectures.

Key payment systems and their supporting interfaces should be included in the overall recovery strategies identified in the business continuity plan. The criticality and recovery prioritization of payment systems are typically identified in the business impact analysis (BIA). Business continuity management includes a testing program for payment systems to reduce the impact of unplanned outages and disruptions on operations. This may include engaging with industry groups and business partners[80] for planning payment recovery strategies in preparation for widespread or systemic events. Business continuity plans (BCP) and disaster recovery (DR) plans should be evaluated in the context of business changes, changes to the industry (e.g., same-day ACH, real-time payments), and issues encountered during testing. Sound practices include annual testing, or more frequent testing when warranted.

BCP, DR plans, and pandemic plans are key documents used to articulate the specific requirements for recovering and maintaining payment systems and operations. Depending on the bank's size, complexity of operations, and criticality of payment products and services, a bank may have one overall BCP for all enterprise operations, including payments, or it may have an individual plan tied to each business line or department that coordinates with an overall BCP. Pandemic plans should be evaluated and integrated into the overall BCP and DR strategy and appropriately tested to promote continuity of payment systems.[81]

Regardless of the approach, BCP and DR plans generally

- assign employee responsibilities and identify key personnel by job position and security access levels necessary to achieve full recovery.
- identify critical third-party providers and effective alternatives.
- identify the goals needed to achieve recovery.
- are updated annually or when material changes to operations occur that affect payment systems.

[79] For more information, refer to the "Business Continuity Management" booklet of the *FFIEC IT Examination Handbook*.

[80] Banks that use third-party payment services often coordinate and execute BCP and DR testing with those organizations. If weaknesses are identified, sound practices include management's evaluation and reporting of key findings to the board and senior management to determine if a retest is required.

[81] Refer to OCC Bulletin 2020-13, "Pandemic Planning: Updated FFIEC Guidance."

- define the payment systems recovery time objectives and recovery point objectives.[82]
- include risk-ranked inventory[83] of the software necessary to continue the safe and sound operation of the bank's payment systems.

Fraud Risk Management

Fraud risk management is a vital component of effective payment systems risk management. Fraud can originate from within the bank or from external sources that target the bank, its customers, or third parties. Processes and controls designed to anticipate, prevent, and deter fraud are key aspects of fraud risk management.[84]

Fraud risk management practices vary based on the bank's size and complexity and the products and services offered. Fraud risk management practices can range from an informal process consisting of fundamental internal controls to a formal program. Many of the best foundational preventative controls the bank implements for all of its products and services (e.g., dual controls and segregation of duties) also apply to payment systems. Fraud risk management, including fraud prevention and detection practices, should evolve with emerging technologies, and adapt to changes in products and services. Fraud solutions are often specifically designed for each product, service or activity.

Fraud risk management practices relating to payments may include

- identifying potential threats of fraud through risk assessments.
- establishing and testing internal controls for payment systems.
- conducting investigations into reported or potential fraud.
- recording, aggregating, and reporting fraud and associated losses.
- customer awareness campaigns.
- initial and periodic training for employees tailored to their roles and responsibilities.
- a feedback loop of lessons learned that allows improvement of the overall function.

Payment systems users should have appropriate levels of access and authority. The authentication[85] techniques employed should be appropriate to the risks associated with the

[82] Recovery time objectives reflect the maximum amount of downtime the application, department, or business process could be unavailable without severely impacting the recovery of the bank's operations. Recovery time objectives count the time from the event until the recovery. Recovery point objectives are the amount of data that can be lost without severely impacting the recovery of the transactional operations.

[83] A risk-ranked software inventory identifies software by its criticality and includes an exercise to ensure software versions recovered match those used in production in order to achieve full operations.

[84] This section of the booklet provides an overview of fraud risk management related to payment systems. For more information regarding fraud risk management, refer to OCC Bulletin 2019-37. More information regarding specific products, services, and activities can be found in *Comptroller's Handbook* booklets (e.g., "Credit Card Lending" and "Merchant Processing"). For BSA/AML-related information, refer to the *FFIEC BSA/AML Examination Manual.*

[85] For more information, refer to OCC Bulletin 2021-36, "Information Security: FFIEC Statement on Authentication and Access to Financial Institution Services and Systems."

payment product or services. Policies and procedures should be designed to consider the related fraud risks. Bank management should consider how fraud arising from social engineering, elder abuse, account takeover, internal and external collusion, and other types of fraud could affect the bank's payment systems.

A good fraud deterrent is creating the perception of detection. Fraud training typically includes an overview of the bank's fraud detection practices. When employees know that the bank is monitoring internal employee entries and customer transactions, employees may be less likely to attempt fraud. The training documentation should not define the specific fraud controls to a point that individuals could then use the content to circumvent the controls.

Dual controls and segregation of duties should be included in the design of processes to help prevent and deter payment fraud. Layered controls and verifications (e.g., customer authentication, out-of-wallet questions, passwords, and PINs) are useful fraud prevention tools.

Detective controls include standard processes like general ledger reconcilements, balancing of correspondent accounts, and second review practices. They can also include the use of advanced solutions such as machine learning, artificial intelligence, modeling, and data analytics.

A common industry practice includes real-time monitoring of customer behavior as a fraud prevention tool. Such monitoring typically includes identifying irregular or atypical customer payment behavior patterns. Several actions may be taken when monitoring identifies an irregular or typical transaction, depending on the bank's system capabilities and configurations. For example, some banks may decline transactions meeting certain criteria and contact the customer to determine whether the attempted transaction was legitimate.

Many banks implement fraud awareness programs for customers and employees. A well-designed fraud awareness program may mitigate reputation risk by informing customers of common fraud schemes to be wary of and providing frontline employees with situational awareness that can be used to prevent or promptly respond to fraud.

Credit Risk Management

Risk management should be commensurate with the nature of the bank's operations and volume of activity. Payment customer relationships should generally be managed in the same manner as any credit, subjecting the customers to credit administration processes for due diligence and ongoing monitoring. Sound credit risk management includes establishing customer exposure limits. Examiners should determine whether such limits are established with consideration of the bank's legal lending limit, as applicable,[86] and capital position.

Credit risk for ACH originating banks is present in both credit and debit originations until the final settlement occurs. Debit originations expose banks to higher risk due to the potential for

[86] Legal lending limits under 12 CFR 32 do not apply to certain exposures, such as intraday credit exposures. For more information, refer to 12 CFR 32.2(q), "Loans and Extensions of Credit."

returns up to 60 days, according to Nacha Operating Rules and Guidelines.[87] Some banks require the customer to hold an amount in reserve to cover the potential for returns based on risk criteria, such as historical return amounts or a percentage of the average daily debit file. Credit risk for receiving banks is minimal because they have the right to return items that they are unable to post to customers' accounts (within Nacha Operating Rules and Guidelines). ACH credit originations carry less risk than debit originations because they generally settle within three days. Requiring the customer to have sufficient collected funds in an account to cover the credit file (e.g., by prefunding the transfer or using a reserve account) or implementing hold-backs can mitigate credit risk.

Some banks extend credit to corporate customers by allowing them to incur intraday (daylight) overdrafts. Daylight overdrafts have the potential to become overnight overdrafts or overnight loans when the net of incoming and outgoing funds is negative at the end of the day. Sound credit policies include underwriting standards for approving and monitoring daylight and overnight overdraft lines. Though intraday overdrafts are typically unsecured, a bank may require a customer to collateralize these overdrafts. Banks can mitigate credit risk by keeping lines of credit uncommitted and unadvised. By keeping the lines uncommitted, management has the ability to deny the credit extension. Unadvised lines are established internally at the bank, and the customer is not aware of the line's availability.

Many payment and securities settlement systems, especially those that rely on settlement lags, netting, or intraday credit, often implement controls that have important credit risk implications for system participants. Such controls include loss-sharing and supplemental liquidity requirements in the event of settlement failures or disruptions. Participants in payment or securities settlement systems should understand the risks related to these settlement failure procedures and should be prepared to make payments for loss allocation assessments as described in the system rules.

As discussed in OCC Bulletin 2006-39, management should implement credit risk controls that establish effective due diligence and underwriting standards for originators, require analysis of originators' creditworthiness, and set appropriate credit exposure limits. As with other types of credit exposures, credit policies should include formal underwriting standards and an approval policy for ACH originators and RDC customers. An effective credit risk management program includes policies that establish exposure limits and monitoring processes for adherence to limits. Controls should also include monitoring for increases in unauthorized returns and suspicious activity, identifying variances from established parameters such as origination volume, periodically verifying the appropriate use of SEC codes, and monitoring higher-risk transactions to assess whether they are within the bank's risk tolerance.[88]

The OCC has provided detailed examination procedures for merchant underwriting and review, as well as fraud monitoring, in the "Merchant Processing" booklet of the *Comptroller's Handbook.*

[87] Refer to the Nacha Operating Rules and Guidelines.

[88] For more information, refer to OCC Bulletin 2006-39.

Liquidity Risk Management

Effective liquidity risk management provides for a bank to meet its projected and daily funding needs and cover both expected and unexpected deviations from normal operations. Comprehensive processes for identifying, measuring, monitoring, and controlling liquidity risk should be integrated into the bank's risk management processes.[89]

Examiners should determine whether the bank's liquidity risk management practices are commensurate with exposures to payment, clearing, and settlement activities, which are sources and uses of funds. Key elements of liquidity risk management in banks with exposure to these activities include active management of intraday liquidity and collateral with appropriate governance and measurement and monitoring systems commensurate with the bank's complexity and business activities. Understanding the timing of payments sent and received is essential to avoiding liquidity shortfalls. Depending on the complexity and materiality of exposures, bank management may need to monitor and measure expected daily gross liquidity inflows and outflows. This could include monitoring overall payment activity and having the ability to calculate the total payment amount sent and received.[90] Monitoring of maximum intraday liquidity usage may be needed to determine the funds needed in both normal and stress liquidity environments. For FMI memberships, risk management may include analyzing daily liquidity inflows and outflows, peak liquidity needs and associated drivers, and payment activity associated with each FMI, including trend analysis and forecasting liquidity funding needs. Sound liquidity risk management typically includes strategies, policies, and procedures that

- articulate risk tolerances and limits.
- allow the bank to manage and mobilize collateral when necessary to obtain intraday credit. This includes consideration for liquid asset reserves, collateral availability, and maximum daylight overdraft capacity.
- identify and prioritize time-specific and other critical obligations to meet obligations when expected.
- settle other less critical obligations as soon as possible.
- provide sufficient guidance to ensure that liquidity planners understand the amounts of collateral and liquidity needed to perform payment-system obligations when assessing the organization's overall liquidity needs.
- categorize payment activity (e.g., industry type) for monitoring and reporting.
- monitor potential changes in activity that may impact liquidity needs.
- require escalation of liquidity risks to management or the board.

Stress testing and the contingency funding plan (CFP) should adequately consider payment activity needs, under both normal and stressed conditions, commensurate with the bank's complexity and activities. Banks with material exposures may need to account for potential

[89] These liquidity risk management principles are discussed in OCC Bulletin 2010-13.

[90] Examples of payment activities that affect intraday liquidity needs include ACH, Fedwire, CHIPS, check processing, ATM systems, card payment processing, and consumer and business banking (e.g., funding loans, paying depositors, and capital expenditures).

liquidity impacts from payment activities when developing contingent liquidity events. Examples of applicable contingent liquidity events include

- disturbances in payment and settlement systems due to operational or local disasters.
- a counterparty limiting or suspending intraday credit lines.
- a counterparty being unable to meet its obligations and make intraday payments.
- for FMI memberships, a large participant being unable to meet its obligations in a timely manner.
- a market-wide stress event that could have negative implications on the value of liquid assets that a bank holds to meet intraday liquidity.

Processing interdependencies are an important consideration for CFPs, particularly in banks with large-value payment activity. In an extreme stress event, the CFP should consider potentially needed sources of funds for an orderly liquidation of assets.[91]

[91] For more information, refer to OCC Bulletin 2010-13.

Examination Procedures

This booklet contains expanded procedures for examining specialized activities or specific products or services that warrant extra attention beyond the core assessment contained in the "Community Bank Supervision," "Federal Branches and Agencies Supervision," and "Large Bank Supervision" booklets of the *Comptroller's Handbook*. Examiners determine which expanded procedures to use, if any, during examination planning or after drawing preliminary conclusions during the core assessment.

This booklet provides examination procedures for assessing the quantity of risk and quality of payment systems risk management, which may be used to assess all payment products and services within the scope of the examination. Additionally, there are supplemental procedures for deeper review of certain payment activities.

Detailed examination procedures for IT related to payment systems are in the "Retail Payment Systems" and "Wholesale Payment Systems" booklets of the *FFIEC IT Examination Handbook*. Expanded "Risks Associated with Money Laundering and Terrorist Financing" procedures (e.g., for electronic banking, funds transfers, ACH transactions, etc.) are in the *FFIEC BSA/AML Examination Manual* and the "Wholesale Payment Systems" booklet of the *FFIEC IT Examination Handbook.* Examination procedures for third-party risk management are in OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures." Additional procedures related to payment systems are in certain booklets of the *Comptroller's Handbook* (e.g., "Credit Card Lending," "Merchant Processing," and "Depository Services") and interagency examination procedures (e.g., "Electronic Fund Transfer Act" conveyed by OCC Bulletin 2019-16, "Consumer Compliance: Revised Interagency Examination Procedures").

Scope

These procedures are designed to help examiners tailor the examination to each bank and determine the scope of the payment systems examination. Examiners should consider work performed by internal and external auditors, independent risk management, and other examiners reviewing related areas. Examiners should perform only those objectives and procedures relevant to the scope of the examination as determined by the following objectives. Seldom is every objective or step of the expanded procedures necessary.

Objective: To determine the scope of the examination of payment systems and identify examination objectives and activities necessary to meet the needs of the supervisory strategy for the bank.

1. Review the following sources of information to identify issues related to payment systems that require follow-up:

   - Supervisory strategy
   - Scope memorandum

- Previous supervisory activity work papers
- Previous supervisory letters and reports of examination, and management's responses
- Internal and external audit reports, work papers, and management's responses
- Customer complaints and litigation. Examiners should review customer complaint data from the OCC's Customer Assistance Group, the bank, and the Consumer Financial Protection Bureau (when applicable). When possible, examiners should review and leverage complaint analysis already performed during the supervisory cycle to avoid duplication of effort.

2. In discussions with management, determine if there have been any significant changes (for example, in policies, processes, personnel, control systems, third-party relationships, products, services, delivery channels, volumes, markets, and geographies) since the prior examination of payment systems.

3. Review applicable OCC reports or analytical tools, such as payment analytics reports.

4. Select the payment products and services to include within the scope of the examination. Consider the following, including whether there have been any changes since the last examination:

   - Products and services offered
   - Growth or attrition rates
   - Target markets or geographies
   - Technologies used
   - Information security
   - Operational resiliency and business continuity practices
   - Levels and trends for transaction volumes, aggregate exposures, and concentrations, and quality of associated reporting and metrics.

5. Obtain and review applicable payment risk management documentation, policies, procedures, and reports used by management to supervise payment systems, including internal risk assessments. Some commonly requested items may include

   - workflow diagrams.
   - board and committee minutes
   - performance reporting with KPIs and KRIs
   - payment fraud risk management practices, fraud losses/rates, and environment.
   - gap analysis.
   - lists of third-party relationships.
   - organization charts relating to payments, including key executives and risk managers within and outside payment departments or organizational units.
   - documentation supporting experience, expertise, training, and qualifications of key payment personnel.
   - FMI memberships, volumes and dollar values, technology systems, and scope of operations.

- documentation supporting the bank's process for reviewing the payment system membership rules and keeping up-to-date on any changes.

6. Based on an analysis of information obtained in the previous steps, as well as input from the examiner-in-charge, determine the scope and objectives of the payment systems examination.

7. Select from the following examination procedures the necessary steps to meet examination objectives and the supervisory strategy.

Quantity of Risk

Conclusion: The quantity of each associated risk is (low, moderate, or high).

Objective: To determine the quantity of risks associated with payment systems.

1. Analyze the quantity of risks associated with the bank's payment products and services. Consider

   - the nature and volume of products and services offered.
   - whether the bank has introduced new or discontinued payment products, services or activities.
   - payment growth or attrition rates (identify cause for large increase or decrease).
   - target markets or geographies.
   - technologies used.
   - levels and trends for transaction volumes, aggregate exposures, and concentrations, and quality of associated reporting and metrics.
   - the volume and significance of customer complaints, including complaints received by or regarding relied-upon third parties.
   - the effect of external factors, including economic, industry, competitive, and market conditions.
   - the effect of potential legislative, regulatory, payment system rule, accounting, and technological changes.

2. Assess the quantity of operational risk. Consider

   - incidents or operational failures related to payment systems. Consider the duration, customer impact, and losses. Consider the history of disruptions and downtime.
   - payment-related operational losses and near misses, and client accommodations over the past 10 years (including errors, fraud, and misconduct) and comparison with the bank's loss appetite threshold. Consider the volume, trend, and nature of the losses and near misses.
   - the extent to which management relies on manual processes or controls.
   - the extent to which the bank is a member of payment systems or associations and the extent to which these activities affect risk exposure. Consider, for example, the bank's exposure to operational risk liability for members of the payment system(s).
   - the nature and extent of the bank's FMU/FMI memberships. Consider exposures related to FMU/FMI memberships such as securities or cash pledged.
   - the types and criticality of payment services provided based on the bank's risk profile and complexity and the number of payment-related third-party relationships.
   - the rate of employee turnover of personnel responsible for executing or overseeing the bank's payment-related policies, standards, and processes.

3. Assess the quantity of strategic risk. Consider

    - whether the strategic plan identifies strategic vision and goals for payment product and service offerings.
    - whether management evaluates the bank's current payment products and services against its risk appetite and overall strategy.
    - whether management identifies emerging or changing risks associated with the bank's payment products, services, or activities.
    - whether management includes industry, market, regulatory and environmental changes in its assessment of strategic risk.
    - the bank's strategy for payment product and service offerings and the impact of that strategy on losses.
    - the marketing and pricing strategy of payment products and services.
    - whether the strategic plan addresses technology needs for payment products and services.

4. Assess the quantity of credit risk present due to payments. Consider

    - the volume and value of payment transactions that have the potential to introduce credit risk.
    - the extent to which the bank pays on uncollected funds.
    - extension of credit practices through the offering of daylight overdrafts.
    - credit exposure from ACH originations, disputes, chargebacks, and returns (e.g., ACH and checks).
    - credit exposure for enterprise-wide payment systems (e.g., TPPP, RDC, and merchant services).

5. Assess the quantity of liquidity risk. Consider

    - the bank's history of meeting and settling obligations and the extent to which the bank uses credit lines to meet its obligations.
    - whether the bank uses a Federal Reserve daylight overdraft line. If so, review the usage activity in recent years and consider whether this usage impacts the bank's quantity of liquidity risk.
    - the aggregate exposure of the overdraft lines that the bank offers to the business customers. Identify the customers with the largest approved exposure and assess the potential impact on the bank's liquidity profile.

6. Assess the quantity of compliance risk. Consider

    - the volume, trend, and nature of violations, audit findings, errors, consumer complaints, and litigation. (Other examiners may have performed such an assessment during examination scoping or other supervisory activities. Leverage analyses already performed, as appropriate.)

- the extent to which the bank is a member of payment systems or associations and history of conforming to their rules or prescribed practices.
- the extent to which the bank relies on third parties to offer products or services (e.g., transaction processing, handling of customer data or information, or development or delivery of applicable required consumer disclosures).
- the volume and nature of transactions being conducted by originators or counterparties located in higher-risk geographic locations.

7. Assess the quantity of reputation risk. Consider

- the bank's ability to provide reliable payment products and services and whether any breaches, internal or at a third party, have occurred recently (e.g., last three years, since last examination).
- payments-related complaints, negative news reports, and litigation.
- the nature and extent of third-party relationships related to payments as it is impacted by public opinion and media exposure.

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, insufficient, or weak).

The conclusion on risk management considers all risks associated with payment systems. These assessments should consider examination work performed using the supplemental procedures in this booklet, as applicable.

Policies

Policies are statements of actions adopted by a bank to pursue certain objectives. Policies help guide decisions, often set standards (on risk limits, for example), and should be consistent with the bank's underlying mission, risk appetite, and core values. Policies should be reviewed periodically for effectiveness and approved by the board or designated board committee.

Objective: To determine whether the board has adopted effective policies that are consistent with safe and sound banking practices and appropriate to the size, nature, and scope of the bank's payment products, services, or activities.

1. Evaluate relevant policies to determine whether they provide appropriate guidance for managing the bank's payment systems risks and are consistent with the bank's risk appetite, mission, values, and principles. Consider third-party risk management, information and cybersecurity, business continuity, fraud, and other risk management policies, as applicable.

2. Determine whether policies address applicable facets of payment systems risk management. Consider whether policies, procedures, and performance standards include such items as

   - an overview of the risk governance framework (e.g., the bank's approach to risk management, committee structure, risk culture, risk appetite, senior management roles and responsibilities).
   - clearly defined roles and responsibilities for oversight of payment operations.
   - a list and descriptions of the payment products and services offered by the bank.
   - payment-related risk limits consistent with the risk appetite. Limits are typically tailored to the transaction type (e.g., wire transfers, ATM withdrawals, mobile/RDC deposits, IAT, internet- or mobile-initiated ACH transactions (WEB), telephone-initiated transactions (TEL)).
   - prudent actions to be taken if payment-related risk limits are exceeded.
   - payment-related risk monitoring and reporting requirements.
   - credit risk management practices for payment products and services.
   - guidelines for complying with regulatory and contractual requirements for payment products, services, or activities.

- an overview of internal controls specifically designed for payment systems, products, and services.
- a description of third-party risk management standards (e.g., due diligence, monitoring and oversight processes).
- payment exception review processes (e.g., limit exceptions and file errors).
- a description of the bank's processes for conducting payment risk assessments, including when joining a payment system and on an ongoing basis.
- independent risk-based audit requirements for payment products, services, or activities.

3. Verify that the board of directors and business unit management periodically review and approve the bank's payment systems policies.

Processes

Processes are the procedures, programs, and practices that impose order on a bank's pursuit of its objectives. Processes define how activities are carried out and help manage risk. Effective processes are consistent with the underlying policies and are governed by appropriate checks and balances (such as internal controls).

Objective: To determine whether the bank has processes in place to define how payment activities are carried out.

1. Assess the adequacy of management's payment-related risk assessments. Determine whether the bank's risk assessments cover all of the bank's payment products, services, and activities (including related liabilities).

2. Evaluate whether processes are effective, consistent with underlying policies, and effectively communicated to appropriate staff. Consider performing a walk-through with payment operations staff to assess process adequacy for selected payment types. Request a demonstration of the daily end-to-end processing for a variety of live transactions from the specific product offering(s) selected for review (e.g., mobile, consumer, commercial, and business).

3. Evaluate the adequacy of internal controls (i.e., automated and manual) for payment products, services, activities, and systems. Review controls identified within the bank's payment-related risk and control self-assessment. Consider dual controls and segregation of duties and whether personnel have the ability to override or circumvent controls. Evaluate whether controls are effective and functioning as designed. Consider completing the Internal Control Questionnaire (ICQ), as appropriate.

4. Evaluate the adequacy of payment-related management reporting. Consider the timeliness and whether reporting comprehensively includes payment products, services, and activities.

5. Assess the sufficiency of suspicious activity monitoring and reporting processes to identify unusual payments and counterparties.

6. Assess the sufficiency of OFAC processes for payments, including those related to the use of third parties and the sufficiency of their compliance and reporting processes.

7. If the bank has third-party relationships that involve critical activities for payment systems, assess the adequacy of the bank's third-party risk management.[92] Consider selecting a sample of due diligence and ongoing monitoring documentation for critical payments-related third parties.[93] Determine whether

   - payment-related third parties are incorporated into the bank's third-party risk management processes and the bank performs due diligence accordingly to determine whether third-party practices meet bank standards (e.g., securing customer information, information security, and operational resiliency).
   - contracts or agreements with customers and third parties clearly establish the roles, responsibilities, governing regulations or guidelines, and termination and dispute resolution processes.
   - the bank is in compliance with the BSA funds transfer recordkeeping rule and funds transfer travel rule, 31 CFR 1010.410(a) and (f).[94]

8. Assess the adequacy of the bank's processes and internal controls relative to the level of complexity of the bank's payment products, services, and delivery channels.

9. Review planned payment products, services, and technologies for the next 12 months. Determine whether plans to add, modify, or expand payment products, services, or delivery channels are well-developed and reasonable. Consider whether

   - plans align with the bank's risk appetite.
   - the bank follows a board-approved process, inclusive of all federal consumer protection laws and BSA/AML and OFAC considerations, for launching new payment products or services.

10. Consider whether new, modified, or expanded payment products, services, and delivery channels are adequately incorporated into the bank's new activities processes and internal controls for ensuring that risks associated with expanded payment products and services are understood and mitigated within reasonable parameters.[95]

---

[92] For more information and expanded examination procedures about third-party risk management, refer to OCC Bulletins 2013-29, 2017-7, and 2020-10.

[93] For more information about sampling methodologies, refer to the "Sampling Methodologies" booklet of the *Comptroller's Handbook.*

[94] For more information, refer to the *FFIEC BSA/AML Examination Manual*.

[95] For more information, refer to OCC Bulletin 2017-43.

11. Assess whether changes or planned changes to payment technologies and platforms undergo proper due diligence, are scalable, and align with strategic plans. Consider whether payment technologies and platforms are reviewed for assessment of risk, scalability, and alignment with the strategic plan. Related risks include mergers and acquisitions, strategic planning, IT strategic risk, IT strategic risk management, and departmental risk management.

Objective: To evaluate the bank's compliance with 12 CFR 7.1026.[96]

1. Determine whether the bank met notice requirements.

   - If the bank joined any payment systems during the review period, determine whether the bank provided written notice to the OCC in a timely fashion.
   - If the bank provided after-the-fact notice, determine whether that notice states that either
     – the payment system's rules do not impose liability for operational losses on members, or
     – the bank's liability for operational losses is limited by the rules of the payment system to certain limits as outlined in 12 CFR 7.1025(c) and (d) (the legal lending limit under 12 CFR 32 or the limit set for the bank by the OCC, whichever is lower).

2. Determine whether the content of the notice included the required representations that the bank has complied with the safety and soundness procedures in 12 CFR 7.1026(e)(1), and will comply with the safety and soundness review and notification requirements in 12 CFR 7.1026(e)(2) and (3).

3. Assess the adequacy of risk management practices for the bank's payment system memberships as required by the safety and soundness procedures and considerations described in 12 CFR 7.1026(e) and (f). Consider whether

   - the bank identifies and evaluates risks associated with payment system memberships.
   - management has the ability to measure, monitor, and control risks presented by the memberships.
   - if safety and soundness concerns are identified, management informs the OCC as soon as the concerns are noted and takes prompt action to remediate the risk.
   - the bank obtains a written legal opinion when required by 12 CFR 7.1026(e)(4) (if applicable, the legal opinion is required before joining the payment system and does not change the timing of the notice requirement).
   - the bank includes the safety and soundness considerations provided in 12 CFR 7.1026(f) in its analysis required by 12 CFR 7.1026(e).

[96] For a compliance worksheet, refer to appendix A of this booklet.

Personnel

Personnel are the bank staff and managers who execute or oversee processes. Personnel should be qualified and competent, have clearly defined responsibilities, and be held accountable for their actions. They should understand the bank's mission, risk appetite, core values, policies, and processes. Banks should design compensation programs to attract and retain personnel, align with strategy, and appropriately balance risk-taking and reward.

Objective: To determine management's ability to supervise payment systems in a safe and sound manner.

1. Assess the management oversight structure and staffing related to payment systems. Consider the following:

   - The expertise, training (e.g., content, quality, frequency, and status), and number of staff members. When assessing expertise and training, examiners may also consider staff accreditations or industry certifications.
   - Whether reporting lines encourage open communication and limit the chances of conflicts of interest.
   - The level of payment staff turnover.
   - The use of third-party arrangements.
   - Employee recruiting, onboarding, and vetting practices.
   - Capability to address identified deficiencies.
   - Responsiveness to regulatory, accounting, industry, and technological changes.
   - Whether the oversight structure, staffing, and succession planning are adequate in relation to the risks associated with the bank's payment systems.

2. Determine whether management and the board have established a sound corporate, compliance, and risk culture that is clearly communicated throughout the bank.

3. Assess performance management and compensation programs for payment personnel. Consider whether these programs measure and reward performance that aligns with the bank's strategic objectives and risk appetite.

4. If the bank offers incentive compensation programs, determine whether they (1) provide employees with incentives that appropriately balance risk and reward; (2) are compatible with effective controls and risk management; and (3) are supported by strong corporate governance, including active and effective oversight by the bank's board of directors.[97]

Control Systems

Control systems are the functions (such as internal and external audits and quality assurance) and information systems that management uses to measure performance, make decisions about risk, and assess the effectiveness of processes and personnel. Control functions should

[97] For more information about incentive compensation, refer to OCC Bulletin 2010-24.

have clear reporting lines, sufficient resources, and appropriate access and authority. Management information systems should provide timely, accurate, and relevant feedback.

Objective: To determine whether the bank has systems in place to provide accurate and timely assessments of the risks associated with payment systems.

1. Evaluate the effectiveness of monitoring systems used to identify, track, and escalate exceptions to policies, procedures, and established limits.

2. Obtain and review reconcilements for the general ledger accounts. Examine entries for irregularities and for proper and timely clearance. Trace irregular, unusual, or suspicious transactions and obtain explanations for items in the account for periods longer than prescribed in the policy and procedures.

3. Determine whether individuals completing reconcilements are different from the individuals posting to the general ledger account.

4. Obtain and review internal reviews or audits of account activity for bank personnel. Consider any irregular account activity in conjunction with information on transactions from procedure #2 of this Control Systems section.

5. For payment types within the scope of the examination, select a sample of transactions that involve manual intervention (e.g., back-office controls, exception processing, over-limit stops, and sanction screening) and assess the effectiveness of manual controls.[98]

6. Determine whether management information systems provide timely, accurate, and comprehensive information to evaluate risk levels and trends in the bank's payment products and services.

7. Assess the quality of the bank's RCSAs. Consider

   - whether RCSAs adequately capture all payment products and services that the bank offers.
   - whether RCSAs comprehensively include risks and associated controls.
   - whether residual risk ratings are assigned.
   - the adequacy of management's quality assurance in the RCSA process.
   - the timeliness of the RCSA.

8. Assess the effectiveness of independent risk control functions (e.g., independent risk management) related to payment systems. Consider whether independent risk management

   - performs reviews that include all payment products and services.

[98] For more information about sampling, refer to the "Sampling Methodologies" booklet of the *Comptroller's Handbook*.

- reviews the design and implementation of internal controls.
- ensures second-line independence.
- evidences and documents credible challenge.
- reports issues in a timely manner.

9. Assess the effectiveness of tracking and resolution of customer complaints and audit findings, management self-identified findings, and regulatory findings. Consider whether

   - management corrects issues appropriately and in a timely manner.
   - senior management and the board hold employees accountable for correcting issues appropriately and in a timely manner.
   - management performs a root cause analysis for significant control weaknesses and processes, or controls are updated based on findings.
   - the bank has an effective customer complaints response and analysis process that allows the board and management to identify and address trends and concerns.

10. Determine whether payment systems are incorporated in the bank's information security program and business continuity management processes.[99] Determine whether business impact analysis, continuity test plans, and execution of testing activities are consistent with the criticality and complexity of the supporting operations for payment products and services. (Note: Often this assessment is performed in conjunction with an IT examiner or aligned with an IT examination.)

Objective: To determine the adequacy of internal audit[100] relating to payment systems and activities.

1. Determine whether audits of payment systems and activities are appropriately risk-based. Consider

   - the adequacy of the audit risk assessment.
   - whether the scope and frequency for payment-related audits is commensurate with the associated risk. For example, audits may be performed on an enterprise-wide basis, at the line of business, or as a combination of enterprise-wide and line-of-business audits.

2. Determine whether the audit scope includes an assessment of

   - payment activities governance structure.
   - growth areas for payment products and services.

[99] Refer to the *FFIEC IT Examination Handbook* booklets "Information Security" and "Business Continuity Management."

[100] For more information about the internal audit function, refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook*. Internal audit evaluates bank activities by assessing effectiveness of the bank's internal control systems, which include internal controls and information systems (e.g., vulnerability assessments, penetration tests).

- new payment products, services, and systems.
- material policies, standards, processes, and procedures (e.g., payments, customer onboarding, new product approval, RCSA, and customer credit analysis and underwriting approval).
- effectiveness of risk management for material risks associated with payment systems.
- payment systems recoverability and resiliency
- quality of internal controls related to payment systems.
- access controls and management of payment systems platforms.
- bank processes for customers' direct access to payment networks.
- compliance with applicable laws and regulations, including federal consumer protection laws and regulations.
- conformance to network, membership, or association rules.
- anti-fraud controls.
- compliance with BSA/AML and OFAC requirements and the quality of related controls.
- effectiveness of payments-related training.
- whether the first and second lines of defense effectively identify issues, including systemic issues across multiple products, services, and delivery platforms as appropriate.
- effectiveness of risk management for payment system memberships.

3. Select a sample of audit work papers and assess the quality of the work papers.[101]

4. Determine whether significant audit findings, reports, and supporting information are regularly reported to the board or audit committee. Assess the adequacy of practices regarding significant or repeat findings.

5. Determine whether auditors have sufficient training and expertise to evaluate each payment product or service and the related components thereof.

[101] Refer to the "Sampling Methodologies" booklet of the *Comptroller's Handbook* for more information about selecting a sample. Refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook* for more information about reviewing internal audit work papers.

Supplemental Procedures

Examiners may use supplemental procedures for examining specific payment products and services.

Automated Clearing House Activities

Examiners may use these procedures to assess the adequacy of the bank's ACH risk management. For more information about ACH, refer to OCC Bulletin 2006-39.

Objective: To determine the adequacy of management and board oversight over ACH activities.

1. Determine whether the board (or designated committee) receives periodic reports to monitor whether ACH activities are within established risk limits. Assess the adequacy of reports considering the bank's size, complexity, risk profile, and ACH activities. Consider whether reports include, as appropriate,

   - metrics and trend analysis on ACH volume, returns, operational losses, and transaction types, with explanations for variances from prior reports.
   - metrics and trend analyses related to the composition of the bank's portfolio of originators and third-party senders.
   - the bank's capital position relative to the volume of ACH activity and the level of risk associated with originators.
   - the percentage of the deposit base linked to ACH origination activity.
   - a summary of return rates by originator and third parties.
   - unauthorized, administrative, and total returns exceeding established thresholds or limits.
   - profitability measures.
   - a comparison of actual performance to established risk limits.
   - notice of potential and actual Nacha Operating Rules violations and fines.

2. Assess the adequacy of oversight practices for higher-risk ACH transactions.[102] Consider whether

   - bank policies
     - define higher-risk ACH activities.
     - provide clear direction to management for engaging in higher-risk ACH activities.
   - board and management reporting adequately captures higher-risk ACH activities.
   - higher-risk transactions are monitored, reported, and within the originator's approved underwriting limits.

[102] For more information on higher-risk ACH transactions, refer to the "Credit Risk Management" section of this booklet.

Objective: To determine whether the bank has adequate policies and procedures regarding ACH activities.

1. Assess the adequacy of ACH-related policies and procedures. Examiners may request a walk-through with ACH operations to aid in completing this procedure. Consider whether policies and procedures include

   - a summary of the ACH activities and objectives.
   - an overview of ACH risk management within the governance risk management framework (e.g., committee structure).
   - risk monitoring and reporting requirements.
   - risk limits consistent with the risk appetite for approved businesses and permissible SEC codes.
   - actions to be taken when risk limits are exceeded.
   - clearly defined roles and responsibilities.
   - a description of third-party risk management standards (e.g., due diligence, monitoring, and oversight processes).
   - exception review processes (e.g., limit exceptions, effective date errors, and file errors).
   - a description of the bank's processes for conducting ACH risk assessments.
   - independent risk-based audit requirements.

Objective: To determine the adequacy of credit risk management related to ACH activities.

1. Assess the adequacy of ACH credit risk management policies and procedures. Determine whether policies and procedures include

   - underwriting and approval standards for ACH originators.
   - definitions for permissible, restricted, and prohibited originators.
   - authorization procedures for approving originators.
   - procedures requiring ongoing communication regarding the originator's financial and overall condition.
   - permissible SEC codes.
   - monitoring procedures that include transaction volume by SEC code and associated risk limits.
   - the type and timing of financial information to be provided by the originator.
   - guidelines for setting exposure limits, including requirements for prefunding, hold-back, or reserve accounts.
   - guidelines for over-limit monitoring, exception processing, and approvals.
   - procedures for originator account terminations.

2. Select a sample of ACH originator credit files and determine whether the files include

   - a credit analysis memorandum, which includes the initial evaluation of the originator's creditworthiness and a comprehensive financial analysis.

- the types of ACH transactions authorized.
- the bank's financial analysis and evaluation of creditworthiness.
- approved exposure limits for daily and multi-day settlements.

3. If the bank imposes prefunding, hold-back, or reserve requirements, assess adherence to the bank's policies and procedures regarding the prefunding, hold-back, or reserve requirements as follows:

   - For prefunding, determine whether the collected funds are in a designated bank-owned account (e.g., general ledger or suspense account) before an ACH file is transmitted.
   - For reserve accounts, determine whether collected funds are in a designated customer-owned account before an ACH file is transmitted.
   - For hold-back, determine whether the hold-back processes are consistent across accounts and the system verifies funds availability before an ACH file is transmitted.

4. Assess the adequacy of processes for monitoring for adherence to ACH credit and debit exposure limits. Consider whether

   - processes provide for monitoring adherence to individual and aggregate exposure limits across multiple settlement dates.
   - limits and approval processes are consistent with the bank's policies for extending unsecured credit.

Objective: To determine the adequacy of due diligence, risk monitoring, and ongoing monitoring for ACH activities.

1. Determine whether the following are performed during onboarding and periodically thereafter:

   - Background checks for the originator and beneficial owners.
   - Communication of changes to an originator's financial condition.
   - Documentation for each originator, including
     - approved exposure limits for daily and multi-day settlements.
     - review of the originator's actual vs. projected activity.
     - BSA/AML and OFAC review documentation (e.g., information to determine the nature and purpose of the customer relationships, customer due diligence, identification and verification of beneficial owners, and verification that the ACH originator is not a Specially Designated National (SDN) or subject to other non-SDN OFAC sanctions).
   - Initial and ongoing credit analysis on ACH originators to determine creditworthiness and set exposure limits.
   - Verification to determine whether an originator is using multiple financial institutions to originate ACH transactions.
   - Periodic audit of originators' ACH processes and controls.

2. Assess the adequacy of first-line risk monitoring for ACH activities. Consider whether payment operations

   - monitor the level of ACH returns.
   - identify and escalate exceptions to established parameters.
   - restrict transaction use to the approved SEC codes.
   - assess the proper coding for all ACH transactions, including IATs.
   - conduct OFAC screening as appropriate.

Objective: To determine the adequacy of internal audits of ACH activities.

1. Assess whether ACH-related audits are conducted with appropriate frequency. Consider

   - whether audit coverage is risk-based.
   - the adequacy of the audit risk assessment.

2. Assess the ACH audit scope and objectives. Consider whether the audit scope includes an assessment of

   - governance structure around ACH activities.
   - areas of significant ACH growth.
   - new ACH products, services, and systems.
   - policies and procedures (e.g., ACH, credit, and compliance)
   - ACH-related internal controls (e.g., reconciliation, segregation of duties, and dual controls).
   - BSA/AML and OFAC controls.
   - conformance to ACH network or association rules.
   - ACH training (e.g., for employees or customers; internal or external training).
   - internal controls and Nacha Operating Rules compliance for direct access to the ACH network.
   - ACH risk assessments.
   - audits or reviews of third parties and originators.

3. Determine whether the individual(s) performing ACH-related audits have sufficient expertise to evaluate all aspects of the ACH program. Consider whether auditor(s) receive periodic ACH training.

4. Verify completion of the annual Nacha Operating Rules audit. If the audit identified noncompliance with Nacha rules or other issues, determine whether management took timely and appropriate corrective action.

Objective: To determine the adequacy of ACH compliance risk management.

1. Consider whether

   - the bank's compliance management system adequately covers ACH activities, including activities conducted through third parties.
   - the bank conducts testing for compliance with applicable laws, regulations, and rules, such as
     - Regulation CC (12 CFR 229).
     - Regulation D (12 CFR 204).
     - Regulation DD (12 CFR 1030).
     - Regulation E (12 CFR 1005).
     - Regulation GG (12 CFR 233).
     - Nacha Operating Rules.
     - BSA/AML requirements.
     - OFAC requirements.
     - other network rules (e.g., card association rules).
   - error resolution practices comply with regulatory and Nacha requirements.

Objective: To determine the adequacy of third-party risk management for ACH activities.

1. Determine whether management effectively oversees ACH activities conducted through third parties. Consider whether

   - management conducted adequate due diligence on each third party.
   - written agreements with each third party
     - outline the specific board-approved risk parameters within which the TPS must operate.
     - detail the obligations and liabilities of the TPS.
     - define the information that must be provided to the bank before the TPS can submit transactions for a new originator.
     - define approved and disallowed originator and transaction types.
     - provide the bank ongoing access to all originators' files.
     - outline the bank's right to audit periodically originators' or third parties' files so that the bank can verify the TPS's compliance with bank policies.
   - management has implemented procedures to
     - monitor the third party's operations.
     - assess the third party and the type of business it conducts.
     - conduct background checks for each third party, including principal owners.
     - assess the third party's financial condition.
   - management verifies that the third party's BSA/AML compliance program includes procedures or standards to monitor, identify and escalate irregular, unusual, or suspicious activity for ACH transactions processed through third parties.
   - management reviews the third party's IAT processes.

Objective: To determine the adequacy of oversight and risk management of third-party senders.

1. Determine whether the bank identifies and registers third-party senders (Nacha Operating Rules requirement).

2. Determine whether the bank collects the following information on the third-party senders (or nested relationships that include the underlying third-party sender customers of third-party senders):

   - Customer's name.
   - Taxpayer ID number.
   - Principal business activity.
   - Geographic location.
   - Verification that the third-party sender's customer is operating a legitimate business before originating transactions.

3. Determine whether the bank establishes a written agreement with each third-party sender that includes

   - requirements for the information that must be provided to the bank before the third-party sender can submit transactions for a new originator.
   - notification to the bank of a new third-party sender nested relationship.
   - exposure limits and whether prefunding, hold-back, or reserve accounts are required.
   - details regarding the bank's and third-party sender's obligations and liabilities.
   - definitions of approved and disallowed originator and transaction types.
   - provision for the bank's ongoing access to an originator's files.
   - provision for the bank's right to audit the third-party sender and its originators.
   - termination clause.

4. Determine whether the bank requires the third-party sender to establish a written agreement between that third-party sender and its customers that includes

   - exposure limits and determination of whether prefunding is required.
   - details regarding the third-party sender's and the customer's obligation and liabilities.
   - definitions of approved and disallowed originator and transaction types.
   - provision for the third-party sender's ongoing access to a customer's files.
   - provision for the third-party sender's right to audit the customer.
   - termination clause.

5. Assess the adequacy, including frequency, of the bank's process to monitor and periodically audit third-party senders.

6. Determine whether management monitors the ongoing financial condition of third-party senders and their customers.

Objective: To determine the adequacy of risk management of direct access customers.

1. If the bank allows originators direct access to the ACH operator, determine whether

   - the board (or board-level committee) approves each ACH originator's direct access.
   - the bank completes the Nacha direct access registration.
   - the bank establishes written agreements that
     - permit direct access.
     - outline roles and responsibilities.
     - restrict the ability to initiate file corrections.
   - the bank monitors and reconciles the originator's transaction activity.

Objective: To determine the adequacy of information security and business continuity management for ACH activities. Coordinate with the bank information technology examiner as appropriate.

1. Determine whether ACH-related systems, processes, and controls are included in the bank's information security program.

2. Determine whether the bank's information security program[103] addresses the following for ACH:

   - **Customer access:** Does the bank implement dual controls and require confidentiality in the initial set-up and activation of new customers?
   - **Access security:** Does the bank secure the distribution and reset process for any authenticators used to access ACH services?
   - **Employee access:** Does the bank minimize and monitor the number of personnel with access to systems supporting ACH services?
   - **ACH access authorization levels:** Does the bank minimize and segregate ACH staff and limit access to various maintenance and transaction support functions (e.g., changing account numbers, adding or deleting new users, and changing transaction limits)?
   - **Data security:** Does the bank utilize risk-based data security controls for all ACH-related systems, applications, and processes?
   - **Data policies and procedures:** Does the bank have control policies and procedures in effect for data in transit or storage?
   - **Communication standards:** Do ACH operations accept data from properly authenticated sources and provide a secure communication channel for all critical or confidential data?
   - **Data classification:** Does the bank identify confidential or critical data used in ACH operations?
   - **Storage and disposal procedures:** Does the bank implement and monitor adherence to proper storage and disposal procedures and practices (purging data from online applications, encrypting data, and destroying trace data from any storage media)?

[103] Refer to the "Information Security" booklet of the *FFIEC IT Examination Handbook*.

3. Determine whether business impact analysis, continuity test plans, and execution of testing activities are consistent with the criticality and complexity of the supporting operations for ACH services. Consider whether ACH activities are factored into the bank's overall business continuity plans.

4. Assess the adequacy of business continuity testing. Consider whether

   - testing includes failover testing.
   - testing results are reported to the board or designated board committee.
   - remediation and retesting practices are adequate if weaknesses are noted in testing.

Remote Deposit Capture

Examiners may use these procedures to assess the adequacy of the bank's RDC risk management. For more information about RDC, refer to OCC Bulletin 2009-4.

Objective: To determine the adequacy of the RDC risk assessment.

1. Assess the adequacy of the bank's risk assessment for RDC. Consider whether management has

   - identified all RDC-associated risks (e.g., compliance, money laundering, fraud, and information security) and engaged all potential stakeholders in RDC.
   - accurately assessed the risks commensurate with the scope of operations.
   - identified and implemented mitigating controls.
   - reviewed and obtained board approval for risk acceptance.

Objective: Assess the adequacy of RDC governance.

1. Determine whether the board (or designated board committee) receives periodic reports to monitor RDC activities. Assess the adequacy of reports, considering the bank's size, complexity, risk appetite, risk profile, and RDC products and services. Consider whether reports include, as appropriate,

   - risk-based data and analysis, such as
     - type and nature of RDC activity.
     - customer activity analysis (e.g., limit breaches, profitability, volumes, and return rates).
   - portfolio-wide perspective for
     - RDC volume compared to total deposits.
     - RDC returns to RDC deposits.
     - RDC contract aging.
     - customer distribution by risk rating.
     - individual account activity.

- trends for
  - return items.
  - over-limit occurrences.
  - duplicate deposits.
  - image quality issues.
  - changes in risk rating.

2. Determine whether management has defined risk limits that are appropriate for the bank's RDC products, services, and operational activities and are board-approved.

3. Determine whether policies and procedures include the following, as appropriate for the bank's RDC products and services:

   - Eligibility requirements.
   - Customer due diligence requirements.
   - Credit review standards.
   - Standards for written agreements.
   - Standards for the RDC customer operating environment (e.g., hardware, software, quality assurance, processing controls, and encryption).
   - Separation of duties (e.g., receipt, logging, input, balancing, and reconciliations).
   - Funds availability (e.g., reserve requirements, processing cutoff times, and required holds).
   - Exception processes (e.g., non-posts, nonsufficient funds, and special handling).
   - Escalation processes (e.g., irregular, unusual, or suspicious activity, and potential OFAC match).

Objective: To assess the adequacy of inclusion of RDC in the bank's information security program, business continuity planning, and business impact analysis processes.

1. Determine whether the bank adequately includes RDC processing in its information security program and business continuity planning.

2. Determine whether the bank includes RDC processing in its business continuity testing, including customer connectivity.

Objective: To determine whether the bank has effective processes in place that are commensurate with the nature, scope, complexity, and risks associated with the bank's RDC products and services and customer use.

1. Assess the adequacy of internal controls for item processing. Consider

   - image quality monitoring.
   - dual controls.
   - document retention and destruction.
   - exceptions processing, such as

  - reversals.
  - adjustments.
  - controls.
  - reporting.
  - image quality exceptions.
- confirmations (i.e., receipt and transmittal).
- reconciliations.
- edit controls.

2. Perform a walk-through with RDC operations to assess process adequacy. Request a demonstration of the daily end-to-end processing for a variety of live transactions from the specific product offering(s) selected for review (e.g., mobile, consumer, commercial, and business).

3. Assess the adequacy of fraud identification and mitigation practices and controls. Consider

   - due diligence for RDC customers.
   - adherence to credit and related policies and standards.
   - adherence to RDC customer limits.
   - use of restrictive endorsement.
   - the bank's record of compliance with laws, regulations, and rules.
   - adherence to service-level agreements.
   - monitoring of daily reports and exceptions.
   - fraud escalation processes.
   - a process for identifying duplicate presentments.

4. Assess the adequacy of credit risk management practices for RDC. Consider whether management

   - conducts thorough credit and financial analyses for all RDC customers (e.g., analyses that include credit reports, Dunn & Bradstreet reports, and financial statements).
   - adheres to a sound credit approval decision process (e.g., decisions are made by qualified experienced credit officer(s) independent of the sales or operations functions).
   - maintains and updates RDC agreements.
   - adheres to policy requirements.
   - effectively resolves policy exceptions.
   - operates within established risk limits.
   - monitors transaction trend and volume reports.
   - establishes effective controls for funds availability, payment on uncollected funds, and overdraft limits.

5. Determine whether management effectively selects and oversees RDC activity conducted through third parties. Consider whether management

   - conducted adequate due diligence on the third party.
   - appropriately resolved significant issues identified during implementation.
   - established well-defined agreements (e.g., service-level agreements, customer contracts) with the third party.
   - adheres to the bank's policies and procedures to
     – monitor the third party's operations.
     – assess the third party and the type of business it conducts.
     – conduct background checks for each third party, including principal owners.
     – assess the third party's financial condition.
   - verifies that the third party's BSA/AML and OFAC compliance program includes procedures or standards to monitor, identify, and report irregular, unusual, or suspicious activity and identify and block activity that may be sanctioned by OFAC for RDC transactions processed through third parties.

Objective: To assess the adequacy of written agreements with RDC customers.

1. Determine whether the agreement or contract clearly and accurately addresses

   - roles, responsibilities, and liabilities.
   - provisions requiring the customer to adhere to applicable laws, regulations, and rules (e.g., Check 21 and Uniform Commercial Code).
   - financial reporting requirements.
   - warranties and indemnification (e.g., alterations and fraud).
   - responsibilities for processing exceptions (e.g., duplicate files and adjustments).
   - daily transaction and deposit limits.
   - reserve requirements.
   - funds availability.
   - daily processing deadlines.
   - information security (e.g., Section 501(b) of GLBA, including handling of digital and paper copy items).
   - requirements for
     – the operating systems environment (e.g., encryption standards).
     – document maintenance and destruction.
     – adherence to the bank's standards.
   - standards for image quality.
   - standards for acceptable and unacceptable items.
   - customer responsibility for accuracy and quality assurance.
   - procedures for submitting image files, including acceptable methods, format, and timing.
   - signature authority and authorized personnel.

- site inspections or audits to verify controls (e.g., check destruction practices, customer control, and customer education and training).
- termination rights.

Objective: To determine the adequacy of customer and employee RDC training.

1. Assess the effectiveness of the bank's RDC customer awareness training. Consider

   - content quality.
   - delivery methods.
   - frequency.

2. Assess the adequacy of RDC training for bank personnel. Consider whether RDC-specific training is

   - provided with appropriate frequency.
   - tailored to the employee's job duties.
   - completed by all applicable employees in a timely manner.
   - enforced by management.

Objective: To determine whether the bank has audit and review functions in place to provide accurate and timely assessments of the risks associated with RDC.

1. Assess the scope, frequency, and effectiveness of the internal audit of RDC. Consider

   - the adequacy of the audit risk assessment.
   - the appropriateness of audit frequency and scope.
   - management's remediation plans and actions taken in response to deficiencies.
   - quality of audit reports and supporting work papers.
   - adequacy of the audit staffing levels and expertise.
   - communication with the audit committee.

2. Assess the adequacy of independent reviews (e.g., compliance and independent risk management reviews). Consider

   - whether reviews are independent.
   - frequency, scope, and depth of reviews.
   - management's remediation plans and actions taken in response to deficiencies.
   - quality of reports and supporting work papers.
   - communication with the board or responsible management committee.

3. Assess the adequacy of commercial customer site inspections. Consider

   - frequency and scope of inspections.

- depth of inspection to verify controls (e.g., check destruction practices, customer control, and customer education and training).
- quality of procedures and work papers.

Objective: To determine the adequacy of RDC compliance risk management.

1. Consider whether

   - the bank has implemented appropriate compliance, BSA/AML, customer identification, due diligence, OFAC, and GLBA policies and processes for RDC customers.
   - management assesses RDC agreements, customer disclosures (e.g., funds availability), and reporting practices for appropriate regulatory requirements.

Checks and Other Monetary Instruments

Examiners may use these procedures to assess the adequacy of the bank's check or other monetary instrument (item) processing controls.

Objective: To determine whether the bank has adequate policies, processes, and personnel to effectively perform item-processing functions.

1. Assess policies and procedures regarding item-processing activity and bank operations related to bank checks or drafts, including foreign drafts, money orders, cashier's/official checks, and traveler's checks. Consider whether policies and procedures address

   - separation of duties.
   - funds availability.
   - exception processes.
   - the ability to override or circumvent designed controls.
   - BSA/AML requirements (31 CFR 1010.415, "Purchases of Bank Checks and Drafts, Cashier's Checks, Money Orders, and Traveler's Checks").

2. Assess the adequacy of training related to item processing. Consider whether training is

   - provided with appropriate frequency.
   - tailored to employees' job duties.
   - completed by all applicable employees in a timely manner.

Objective: To determine the adequacy of internal controls over item-processing activities.

1. Obtain and review reconcilements for the item-related general ledger accounts.

   - Examine entries for irregularities and for proper and timely clearance.

- Trace irregular, unusual, or suspicious transactions, and consider obtaining and reviewing personnel account statements if irregular activity is noted.
- Obtain explanations for items in the account for periods longer than prescribed in the policy and procedures.
- Determine whether individuals completing the reconcilements are different from the individuals posting to the general ledger account.

2. Verify that dual controls are in place for item-processing and return items (e.g., cashier's/official check stocks and supplies).

3. Perform a walk-through with relevant operations to assess process adequacy. Request a demonstration of the daily end-to-end processing for a variety of live transactions.

4. Select appropriate sample(s) for transaction testing. Refer to the "Sampling Methodologies" booklet of the *Comptroller's Handbook* for more information about judgmental and statistical sampling. Perform one or more of the following transaction testing steps:

   - Review the items received for processing via mail or drop box, including such items as loan payments, deposits, cash, ATM deposits, and checks. Assess adherence to the bank's policies and procedures. Review supporting documentation to determine whether items are promptly processed, forwarded, and reconciled.
   - Review cash-related activity to determine if any transactions appear to be structured in a manner to evade currency transaction reporting (CTR) requirements (31 CFR 1020.310, "Reports of Transactions in Currency").
   - Review documentation supporting corrections made to customer accounts for items received for processing. Determine whether bank customers are promptly notified of all changes to deposit totals resulting from these corrections.
   - Determine whether original items are securely safeguarded and destroyed according to policies and procedures.
   - Review documentation supporting cash letter differences. Determine whether the differences are researched, traced, and adjusted according to the associated policies and procedures.
   - Review charged-off check items. Determine whether items are properly documented and approved and follow the policies and procedures.

5. Evaluate whether item processing practices are effective, consistent with underlying policies, and effectively communicated to appropriate staff.

Objective: To determine whether the bank has audit and review functions in place to provide accurate and timely assessments of the risks associated with its item-processing activities.

1. Assess the scope, frequency, and effectiveness of the internal audit of item-processing activities. Consider

   - the adequacy of the audit risk assessment.

- the appropriateness of audit frequency and scope.
- management's remediation plans and actions taken in response to deficiencies.
- quality of audit reports and supporting work papers.
- adequacy of the audit staffing levels and expertise.
- communication with the audit committee.

2. Assess the adequacy of independent reviews (e.g., compliance and independent risk management reviews). Consider

   - whether reviews are independent.
   - frequency, scope, and depth of reviews.
   - management's remediation plans and actions taken in response to deficiencies.
   - quality of reports and supporting work papers.
   - communication with the board or responsible management committee.

Objective: To determine the adequacy of item-processing compliance risk management. Consider whether

- the bank has implemented appropriate compliance, BSA/AML, customer identification and due diligence, OFAC, and GLBA policies and processes.
- management assesses applicable agreements, customer disclosures (e.g., funds availability) and reporting practices for appropriate regulatory requirements.

Conclusions

Conclusion: The aggregate level of each associated risk is (low, moderate, or high). The direction of each associated risk is (increasing, stable, or decreasing).

Objective: Determine, document, and communicate overall findings and conclusions regarding the examination of payment systems.

1. Determine preliminary examination findings and conclusions and discuss with the examiner-in-charge, including

   - quantity of associated risks (as noted in the "Introduction" section of this booklet).
   - quality of risk management.
   - aggregate level and direction of associated risks.
   - overall risk in payment systems.
   - violations of laws and regulations or other deficiencies.

Summary of Risks Associated With Payment Systems				
Risk category	**Quantity of risk**	**Quality of risk management**	**Aggregate level of risk**	**Direction of risk**
	(Low, moderate, high)	(Weak, insufficient, satisfactory, strong)	(Low, moderate, high)	(Increasing, stable, decreasing)
Credit				
Liquidity				
Operational				
Compliance				
Strategic				
Reputation				

2. Discuss examination findings with management, including violations, deficient practices, and conclusions about risks and risk management practices. If necessary, obtain commitments for corrective action.

3. Compose conclusion comments, highlighting any issues that should be included in the report of examination or supervisory letter. If necessary, compose matters requiring attention and violation write-ups.

4. Update the OCC's supervisory information systems and any applicable report of examination schedules or tables.

5. Document recommendations for the supervisory strategy (e.g., what the OCC should do in the future to effectively supervise payment systems, including time periods, staffing, and workdays required).

6. Update, organize, and reference work papers in accordance with OCC policy.

7. Appropriately dispose of or secure any paper or electronic media that contain sensitive bank or customer information.

Internal Control Questionnaire

An ICQ helps an examiner assess a bank's internal controls for an area. ICQs typically address standard controls that provide day-to-day protection of bank assets and financial records. The examiner decides the extent to which it is necessary to complete or update ICQs during examination planning, after reviewing the findings and conclusions of the core assessment, or after reviewing conclusions from expanded procedures.

Strategic Planning

- Does management include industry, market, regulatory, and environmental changes in its assessment of the bank's strategic risk?
- Does the bank have a board-approved written strategic plan that identifies strategic vision and goals and integrates new, planned, and existing payment products, services, and delivery channels?
- Does the strategic plan align with the risk appetite, capital plan, and business model?
- Do the strategic plan and budget include the allocation of resources needed to achieve strategic objectives, including human, technology, and financial resources?
- Does the bank have a process for measuring progress against established goals including timelines, budget variances, and milestones?
- Do the board and management update the strategic plan for payment products, services, and activities at least annually and more often, if warranted by emerging or changing risks?
- Does management plan for growth in the bank's payment products or services?
- Has management considered whether technology platforms can provide for planned growth?
- Has the board established the bank's risk appetite for payment system membership risks, including liabilities, whether pass-through or shared liability?

Risk Assessment

- Does management conduct a periodic risk assessment of payment systems activities?
- Do risk assessments consider payment products, services, and delivery channels used in all affected lines of business?
- Do risk assessments evaluate the risks, including BSA/AML, OFAC, and compliance risk, for each of the bank's various payment systems?
- Are risk assessment results communicated to the board or a designated committee?
- Do risk assessments identify risks arising from different payment products, services, and delivery channels?
- Do risk assessments include such strategic factors as the potential size of the bank's market, customer needs, changes in technology, and changes in the operating environment?
- Does the bank's process for identifying, monitoring, measuring, and controlling reputation risk include payments-related risks?

Governance

- Does the bank have written payment system risk policies, procedures, and standards?
- Do payment systems functions or units have anti-fraud policies and procedures?
- Do payment systems functions or units have policies and procedures in place to comply with BSA/AML and OFAC requirements?
- Do policies and procedures clearly define roles and responsibilities of key staff involved in payment systems and operations?
- Is management reporting accurate and timely?
- Does reporting include all products, services, and delivery channels for all affected lines of business?
- Does reporting include volume, variance, outstanding item, and charge-off information?
- Has management established risk escalation procedures (e.g., policy or procedure exception standards, exception documentation tracking and reporting, and documentation of approval decision process)?
- Does management review and monitor payment activity, especially those activities that expose the bank to heightened credit and liquidity risk? Are the reviews documented?
- Does the bank have procedures for monitoring risks associated with higher-risk originators?
- Has management established key risk indicators or metrics for payment products, services, and activities? Does the board or a designated board committee regularly receive reports of key risk indicators or metrics relative to established limits?
- Has the board established a risk appetite or tolerance limits? Does the bank operate within these limits?
- When operations occur outside of risk appetite or tolerance limits, does management follow established processes for remediation or risk acceptance?
- Are payment products, services, and delivery channels included in the bank's risk management framework, as detailed in 12 CFR 30, appendix D (applicable only to banks subject to heightened standards)?

Internal Controls

- Has management implemented internal controls related to payment systems and activities, such as
  - dual controls?
  - segregation of duties?
  - physical controls?
  - logical controls?
  - manager or supervisor controls?
- Are reconciliations independent and timely?
- Do policies and procedures document processes for escalating and clearing variances, out-of-balance conditions, and suspense items?
- Do exception processing policies, procedures, and controls include verification processes?
- Does the bank perform independent risk reviews for payment systems internal controls?

- Do payment personnel monitor and report suspicious payments and potentially fraudulent activities?
- If management allows direct access to ACH operators, does it monitor related transactions, settlements, and activity (e.g., reversals and corrections)?
- Is there documentary evidence of supervisor or management sign-off on daily activities?

Audit

- Is internal audit's coverage of payment systems risk-based?
- Does audit coverage include all material payment products, services, and activities?
- Does audit cover all material payment policies, processes, and procedures?
- Does audit check for completion of the Nacha Operating Rules audit?
- Are significant audit findings, reports, and supporting information regularly reported to the board or audit committee?
- Does management respond to, track, and resolve audit findings in a timely manner?
- Does audit staff receive training on payment systems, products, and services?

Personnel

- Does every payment systems employee receive payment-specific training? Are job descriptions and responsibilities clearly defined?
- Is training timely, appropriate, and tailored to the employee's duties?
- Are staff members cross-trained?
- Does the bank have a performance management or review program?
- Does the bank's vacation or rotation policy require two weeks off?
- Do payment systems employees undergo initial and periodic background checks?

Operational Risk

- Has the board established the bank's risk appetite regarding operational risk associated with payment products, services, and activities?
- Does management identify and register third-party senders that are initiating entries into the ACH network?
- Does business continuity management and disaster recovery planning undergo periodic testing and include payment processing operations and systems?
- Does management assess the security and reliability of payment systems?
- Does management maintain an inventory of the bank's payment platforms and security features?
- Does management have controls in place to manage access to payment systems applications and data? Are controls in place that limit administrative access to payment systems applications to authorized personnel?
- Does the bank have a process for assessing the risks associated with its payment systems, including risks associated with third-party relationships?
- Are the bank's software patches' versions current?

- Are payment losses measured and reported? Do these include fraud losses?
- Have the bank's payment system-related losses resulted in litigation? Has management appropriately reserved against probable losses?

Credit Risk

- Has the board established its risk appetite regarding credit risk associated with payment products, services, and activities?
- Does the bank have written credit policies and procedures, including formal underwriting standards?
- Does the policy address underwriting standards for ACH originators, commercial RDC customers, overdraft lines for commercial customers, and other applicable payment customers?
- Does management set and monitor credit exposure limits for payment products and services for each customer (e.g., over-limit and utilization reports)? Is this limit monitored in relation to the customer's overall limit?
- Has management established processes to assess and monitor the financial condition of payment customers?
- Do the credit department and payment systems personnel communicate with each other about credit exposure information?
- Does the bank mitigate credit risk through prefund, hold-back, or reserve accounts?
- Does the bank allow third parties direct access to settle transactions using the bank's accounts? If so, does management have a process in place to mitigate associated risks?

Liquidity Risk

- Has the board established its risk appetite regarding liquidity risk associated with payment products, services, and activities?
- Do liquidity policies and procedures include all payment products and services (e.g., clearing and settlement)?
- Do policies and procedures address the Board of Governors of the Federal Reserve System's Payment System Risk Policy on Intraday Credit?[104]
- Have the board and management established limits for the bank's intraday liquidity position?
- Does management have processes in place to monitor and control the bank's intraday liquidity position?
- Does the contingency funding plan consider all applicable payment products and services in normal and stressed environments?

[104] For more information, refer to "Guide to the Federal Reserve's Payment System Risk Policy on Intraday Credit" and "Overview of the Federal Reserve's Payment System Risk Policy," Board of Governors of the Federal Reserve System (July 2012).

Compliance Risk

- Has the board established its risk appetite regarding compliance risk associated with payment products, services, and activities?
- Does the bank have processes to evaluate compliance with applicable laws and regulations related to payment products, services, and delivery channels?
- If the bank offers ACH processing, does the bank have processes to evaluate compliance with Nacha Operating Rules?[105]
- Does the bank have processes for reviewing, tracking, reporting, escalating, and resolving complaints?[106]
- Does the bank have processes for error resolution and disputes?[107]
- Does the bank have processes for addressing payment-related pending litigation?
- Does the bank have pending payment-related litigation?
- Does management consider compliance when developing new products, services, delivery channels, payment technologies, and other payment initiatives?
- As part of the bank's compliance management system, does management monitor the effectiveness of payment systems compliance processes?
- Does management monitor and report suspicious and fraudulent activity within payment systems?[108]
- Do payment staff members receive BSA/AML, OFAC, anti-fraud, and other compliance training that is timely and aligned with the staff's duties?
- Do payment systems interface with the BSA/AML/OFAC reporting systems for identifying suspicious activities and transactions?

[105] Refer to Nacha Operating Rules and Guidelines. (Although the OCC does not enforce Nacha Operating Rules, noncompliance can result in safety and soundness concerns and could subject the bank to Nacha's ACH rules enforcement and potential monetary fines.)

[106] Refer to the "Compliance Management Systems" booklet of the *Comptroller's Handbook*.

[107] Refer to the "Electronic Fund Transfer Act" booklet of the *Comptroller's Handbook* and OCC Bulletin 2019-16.

[108] Refer to the *FFIEC BSA/AML Examination Manual*.

Appendixes

Appendix A: 12 CFR 7.1026 Compliance Worksheet

Examiners may use the worksheet to assess a bank's compliance with 12 CFR 7.1026 regarding payment system memberships. The worksheet should be used in conjunction with the related examination procedures.

Note: Negative responses may indicate noncompliance with 12 CFR 7.1026. In such cases, further review may be necessary to determine the appropriate corrective action.

12 CFR 7.1026 Worksheet			
	Reference	**Yes/No**	**Comments**
Notice requirements and content of notice **Note:** The bank is required to provide written notice to the OCC before joining a payment system with open-ended liability. Otherwise, after-the-fact notice to the OCC is required.			
1. Did the bank provide written notice to the OCC at least 30 days before joining a payment system that exposed it to open-ended liability?	12 CFR 7.1026(c)(1)		
2. Did the bank provide written notice to the OCC within 30 days of joining a payment system that does not expose it to open-ended liability?	12 CFR 7.1026(c)(2)		
3. Did the bank's notice include the following representations:			
a. That the bank complied with the safety and soundness review requirements of 12 CFR 7.1026(e)(1) before joining the payment system? **Note:** Refer to questions 5 and 6 for the safety and soundness review requirements.	12 CFR 7.1026(d)(1)(i)		
b. That the bank will comply with the safety and soundness review and notification requirements of 12 CFR 7.1026(e)(2) and (3)? **Note:** Refer to questions 7, 8, and 9 for the safety and soundness review and notification requirements.	12 CFR 7.1026(d)(1)(ii)		
4. If the bank submitted an after-the-fact notice for joining a payment system that does not expose the bank to open-ended liability, does the notice include a representation that either			
a. the rules of the payment system do not impose liability for operational losses on members, or	12 CFR 7.1026(d)(2)(i)		
b. the bank's liability for operational losses is limited by the rules of the payment system to specific and	12 CFR 7.1026(d)(2)(ii)		

12 CFR 7.1026 Worksheet			
	Reference	**Yes/No**	**Comments**
appropriate limits that do not exceed the lower of (1) the legal lending limit under 12 CFR 32 or (2) the limit set for the bank by the OCC?			
Safety and soundness procedures			
5. Before joining a payment system, does the bank identify and evaluate the risks posed by membership in the payment system, considering whether the liability of the bank is limited?	12 CFR 7.1026(e)(1)(i)		
6. Before joining a payment system, does the bank ensure that it can measure, monitor, and control the risks identified by the bank's evaluation under 12 CFR 7.1026(e)(1)(i)?	12 CFR 7.1026(e)(1)(ii)		
7. Does the bank identify, evaluate, measure, monitor, and control the risks on an ongoing basis?	12 CFR 7.1026(e)(2)		
8. Does the bank notify the OCC as soon as safety and soundness concerns are identified (e.g., a material change to the bank's liability indemnification responsibilities)?	12 CFR 7.1026(e)(3)(i)		
9. If the bank identifies risks raising safety and soundness concerns, does the bank take appropriate actions to remediate the risks?	12 CFR 7.1026(e)(3)(ii)		
10. If the bank's open-ended liability is otherwise limited, refer to procedures 13, 14, and 15 in the "Safety and soundness procedures: legal opinion" section of this table.	12 CFR 7.1026(e)(4)		
Safety and soundness considerations			
11. Does the bank evaluate the following payment system characteristics when conducting its risk analysis under 12 CFR 7.1026(e):			
a. Does the processing occur on a real-time gross settlement basis or provide reasonable assurance (e.g., prefunding) that members will meet settlement obligations?	12 CFR 7.1026(f)(1)(i)		
b. How do the payment system's rules limit its liability to members?	12 CFR 7.1026(f)(1)(ii)		
c. Does the payment system have insurance coverage and/or self-insurance arrangements to cover operational losses?	12 CFR 7.1026(f)(1)(iii)		
d. Do the payment system's rules provide an unambiguous pro-rata loss allocation methodology under its indemnity provisions and does the methodology provide members the	12 CFR 7.1026(f)(1)(iv)		

12 CFR 7.1026 Worksheet			
	Reference	**Yes/No**	**Comments**
opportunity to reduce or eliminate liability exposure by decreasing or ceasing use of the payment system?			
e. Do the payment system's rules provide for unambiguous membership withdrawal procedures that do not require the prior approval of the system?	12 CFR 7.1026(f)(1)(v)		
f. Does the payment system have appropriate admission and continuing participation requirements for system participants? Do the requirements address the following:	12 CFR 7.1026(f)(1)(vi)		
i. The participants' access to sufficient financial resources to meet obligations arising from participation?	12 CFR 7.1026(f)(1)(vi)(A)		
ii. The adequacy of participants' operational capacities to meet obligations arising from participation?	12 CFR 7.1026(f)(1)(vi)(B)		
iii. The adequacy of the participants' own risk management processes?	12 CFR 7.1026(f)(1)(vi)(C)		
g. Does the payment system have processes and controls in place to verify and monitor on an ongoing basis the compliance of each participant with admission and participation requirements?	12 CFR 7.1026(f)(1)(vii)		
h. Does the payment system have written policies and procedures for addressing participant failures to meet ongoing participation requirements?	12 CFR 7.1026(f)(1)(viii)		
i. Are the payment system's rules relating to the system's emergency authorities unambiguous; can they be amended or otherwise altered without prior notification to all members; and is there an opportunity to withdraw?	12 CFR 7.1026(f)(1)(ix)		
j. Is the payment system governed by uniform, comprehensive, and clear legal standards in its operating jurisdiction that address payment and/or settlement activities?	12 CFR 7.1026(f)(1)(x)		
k. Is the payment system subject to and in compliance (or observance) with the Committee on Payment and Settlement Systems and the Technical Committee of the International Organization of Securities Commissions (CPSS—IOSCO) Principles for Financial Market Infrastructures?	12 CFR 7.1026(f)(1)(xi)		

12 CFR 7.1026 Worksheet			
	Reference	**Yes/No**	**Comments**
l. Is the payment system designated as a systemically important financial market utility (SIFMU) by the Financial Stability Oversight Council (FSOC) or is it the international or foreign equivalent?	12 CFR 7.1026(f)(1)(xii)		
m. Does the payment system provide members with information relevant to governance, risk management practices, and operations in a timely manner and with sufficient transparency and particularity for the bank to ascertain with reasonable certainty the bank's level of risk exposure to the system?	12 CFR 7.1026(f)(1)(xiii)		
n. Is the payment system operated by or subject to oversight of a central bank or regulatory authority?	12 CFR 7.1026(f)(1)(xiv)		
o. Is the payment system legally organized as a nonprofit enterprise or is it owned and operated by a government entity?	12 CFR 7.1026(f)(1)(xv)		
p. Does the payment system have appropriate systems and controls for communicating to members in a timely manner about material events that relate to or could result in potential operational losses (e.g., fraud, system failures, natural disasters)?	12 CFR 7.1026(f)(1)(xvi)		
q. Has the payment system ever exercised its authority under indemnification provisions?	12 CFR 7.1026(f)(1)(xvii)		
12. Does the bank consider the following characteristics of its risk management program when conducting an analysis under 12 CFR 7.1026(e):			
a. Does the bank have appropriate board supervision and managerial and staff expertise?	12 CFR 7.1026(f)(2)(i)		
b. Does the bank have comprehensive policies and operating procedures with respect to its risk identification, measurement, and management information systems that are routinely reviewed?	12 CFR 7.1026(f)(2)(ii)		
c. Does the bank have effective risk controls and processes to oversee and ensure the continuing effectiveness of the risk management process? The program should include a formal process for approval of payment system memberships as well as ongoing monitoring and measurement of activity against	12 CFR 7.1026(f)(2)(iii)		

12 CFR 7.1026 Worksheet			
	Reference	**Yes/No**	**Comments**
predetermined risk limits?			
d. Does the bank's membership evaluation process include assessments and analyses of	12 CFR 7.1026(f)(2)(iv)		
i. the credit quality of the entity?	12 CFR 7.1026(f)(2)(iv)(A)		
ii. the entity's risk management practices?	12 CFR 7.1026(f)(2)(iv)(B)		
iii. settlement and default procedures of the entity?	12 CFR 7.1026(f)(2)(iv)(C)		
iv. any default or loss-sharing precedents and any other applicable limits or restrictions of the entity?	12 CFR 7.1026(f)(2)(iv)(D)		
v. key risks associated with joining the entity?	12 CFR 7.1026(f)(2)(iv)(E)		
vi. the incremental effect of additional memberships in aggregate exposure to payment system risk?	12 CFR 7.1026(f)(2)(iv)(F)		
e. Does the bank's risk management program include policies and procedures that identify and estimate the level of potential operational risks, at both inception of membership and on an ongoing basis?	12 CFR 7.1026(f)(2)(v)		
f. Does the bank have auditing procedures to ensure the integrity of risk measurement, control, and reporting systems?	12 CFR 7.1026(f)(2)(vi)		
g. Does the program include mechanisms to monitor, estimate, and maintain control over the bank's potential liabilities for operational losses on an ongoing basis? This should include	12 CFR 7.1026(f)(2)(vii)		
i. limits and other controls with respect to each identified risk factor.	12 CFR 7.1026(f)(2)(vii)(A)		
ii. reports generated throughout the processes that accurately present the nature and level(s) of risk taken and demonstrate compliance with approved polices and limits.	12 CFR 7.1026(f)(2)(vii)(B)		
iii. identification of the business unit and/or individuals responsible for measuring and monitoring risk exposures, as well as those individuals responsible for monitoring compliance with policies and risk exposure limits.	12 CFR 7.1026(f)(2)(vii)(C)		

12 CFR 7.1026 Worksheet			
	Reference	**Yes/No**	**Comments**
h. If the bank has memberships in multiple payment systems, does it have the ability to monitor and report aggregate risk exposures and measurement against risk limits both at the sponsoring business line level and the total exposure organizationally?	12 CFR 7.1026(f)(2)(viii)		
Safety and soundness procedures: legal opinion			
Note: A written legal opinion is not required to join any payment system, nor does it change when the bank must provide notice to the OCC. It is only required for the bank to treat its liability as limited when the payment system's rules indicate open-ended liability. The written legal opinion option is likely to be exercised rarely and offers an additional option for banks wanting to join a payment system in which the rules do not limit the liability of its members, but the bank believes another factor effectively limits its potential liability.			
13. For a bank that believes its open-ended liability is limited by something other than the rules of the payment system itself (e.g., by negotiated agreements or laws of an appropriate jurisdiction), did the bank obtain a written legal opinion prior to joining the payment system that describes how the payment system allocates liability for operational losses?	12 CFR 7.2016(e)(4)		
14. Does the legal opinion conclude the potential liability for operational losses for the bank is limited to specific and appropriate limits? The limits should not exceed the lower of • the legal lending limit under 12 CFR 32 or • the limit set for the bank by the OCC.	12 CFR 7.2016(e)(4)(i)(B)		
15. Have there been any material changes to the liability or indemnification requirements applicable to the bank since the issuance of the written legal opinion?	12 CFR 7.2016(e)(4)(ii)		

Appendix B: Glossary

Automated clearing house (ACH): An electronic network for financial transactions in the United States that processes large volumes of credit and debit transactions in batches.

ACH credit entry: A transaction that deposits funds into an account. Examples of ACH credit transactions include direct deposit of payroll, government benefits, tax and other refunds, annuities, and interest payments.

ACH debit entry: A transaction that withdraws funds from an account. Examples of ACH debit transactions include such consumer payments as mortgage payments and insurance premiums.

ACH file: An electronic payment file that comprises batched ACH entry data and is subjected to formatting and structural specifications defined in the Nacha "Operating Rules and Guidelines."

ACH operator: An entity that acts as a central facility for the clearing, delivery, and settlement of entries between or among participating depository financial institutions.

ACH origination: An ACH credit or debit entry originated by an ODFI.

ACH originator: A person or organization that has authorized an ODFI (directly or through a third-party sender) to transmit, for the account of that party, a credit entry, debit entry, or non-monetary entry to the receiver's account at the RDFI.

ACH receiver: An individual or organization that has authorized an originator to initiate a credit entry, debit entry, or non-monetary entry to the receiver's account at the RDFI. With respect to debit entries, the term receiver means all persons whose signatures are required to withdraw funds from an account.

Acquiring bank (acquirer): A bank that contracts with merchants to settle payment card transactions. Acquiring banks contract directly with merchants or indirectly through agent banks or other third parties to process card transactions. The acquiring bank generally provides all backroom operations to the agent bank and owns the bank identification number (BIN) or Interbank Card Association (ICA) number through which settlement takes place.

Agent bank: A member of a card association network that agrees to participate in an acquirer's merchant processing program. The agent may or may not be liable for losses incurred on its merchant accounts. Agent banks that only refer merchants are known as referral banks. Referral banks typically do not assume any merchant liability. Note: The term agent bank is not exclusive to credit card relationships and may also refer to other functions or duties performed on behalf of the bank.

Approval: The step after the initiation of a payment when the payor's account provider verifies that the payor's account has sufficient funds or credit necessary to complete the authorized transactions.

Artificial intelligence (AI): AI is broadly defined as the application of computational tools to address tasks traditionally requiring human analysis.[109]

Authentication: The process of verifying the identity or veracity of a participant, device, payment, or message connected to a payment system. Authentication can occur at multiple points in the payment process (e.g., when initiating or receiving a payment).

Authorization: The explicit instructions, including timing, amount, payee, source of funds, and other conditions, that the payor gives to the payor's account provider or to the payee to transfer funds on either a one-time or recurring basis.

Bank identification number (BIN)/Interbank Card Association (ICA): Series of numbers used to identify the issuer. These identifiers are a component of the customer account number embossed on credit cards.

Bank of first deposit (BOFD): A financial institution that accepts a check for deposit from a customer. Referred to as depository bank or payee's depository financial institution.

Beneficiary: The ultimate party to be credited or paid as a result of a funds transfer.

Beneficiary bank: The financial institution that is to credit or pay the beneficiary party.

Bleaching: A fraudster may use chemicals to wash off the ink from the original item and replace it with new payee or amount information.

Business-to-business (B2B): Payments initiated by a business entity and made payable to another business entity.

Business-to-person (B2P): Payments initiated by a business entity to a person.

Card association network: A card association is an organization that licenses a bank card program. Visa, Mastercard, and American Express are examples of card associations. The associations generally require that banks be members of an association to offer the association's card services. Membership rights and obligations are specifically defined by the associations. Also known as card association or bank card association.

Card processor: A third party that provides transaction processing and other services for an issuing bank or an acquiring bank. It is a card association member, or an association-approved non-member acting as the agent of a member, that provides authorization, clearing,

[109] For more information, refer to the Financial Stability Board's November 2017 report, "Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications."

or settlement services for merchants and members. Some banks act as their own card processors while other banks use third parties for card processing.

Central counterparty (CCP): A counterparty (e.g., a clearing house) that facilitates trades between counterparties in one or more financial markets by either guaranteeing trades or novating contracts.[110]

Chargeback: Generated when a cardholder disputes a transaction or when the merchant does not follow proper procedures. The issuer and acquirer research the facts to determine which party is responsible for the transaction. Strict card association rules govern which party is responsible.

Check clearing: The movement of a check from the depository institution where it is deposited to the institution on which it was written. The funds move in the opposite direction, with a corresponding credit and debit to the involved accounts.[111]

Check kiting: A form of check fraud that occurs when a bank customer deposits a check and intentionally misuses the float time to transact against uncollected funds.

Check truncation: The practice of capturing an image of a paper check at the bank at which it was deposited and converting it to electronic form.

CHIPS: The Clearing House (TCH) Interbank Payments System: A privately owned electronic payment system that performs U.S. dollar clearing of domestic and international payments. CHIPS is a counterpart to Fedwire.

Clearing: Process of transmitting, reconciling, and, in some cases, confirming payment orders or financial instrument transfer instructions before settlement.

Converting bank (truncating bank): The bank that truncates the original check.

Correspondent bank: A private depository institution, banker's bank, or Federal Reserve Bank providing clearing or settlement services to a paying bank or collecting bank.

Credit "push": A transfer of funds directly from the sender to a payee. The person or entity making the payment instructs its financial institution to transmit a deposit or credit to a specific payee or account.

Daylight overdraft: An overdraft condition that occurs when withdrawals from an account exceed the available amount. Generally, incoming funds eliminate overdrafts by the end of the day.

[110] The definition is from 12 CFR 47.2, "Definitions."

[111] For more information, refer to the "Retail Payment Systems" booklet of the *FFIEC IT Examination Handbook.*

Depository: An entity that holds deposits or other assets for safekeeping.

Digital wallet (also mobile or e-wallet): A software application (usually running on a personal device or computer) that stores payment information and allows users to communicate with other enabled devices via NFC technology to complete transactions.

Direct access: A situation in which an originator, third-party sender, or third-party service provider transmits credit or debit entries to an ACH operator using the ODFI's routing and transit number and settlement account.

EMV: A technology that embeds a microprocessor chip on credit cards and debit cards to encrypt transaction data. The technology was jointly developed by Europay, Mastercard, and Visa, and the technology is named for the original developers.

Fedwire: The Federal Reserve Banks' nationwide real-time gross settlement electronic funds and securities transfer network. Fedwire is a credit transfer system. Each funds transfer is settled individually against an institution's Federal Reserve account. Settlement of funds is immediate, final, and irrevocable.

Financial market infrastructure (FMI) or financial market utility (FMU): Multilateral systems that provide the infrastructure for transferring, clearing, and settling payments, securities, derivatives, and other financial transactions among financial institutions or between financial institutions and the system.

Float time: The time it takes between clearing and settling funds related to a payment.

Funding participants: Banks participating in CHIPS that are responsible for their own net positions and the net positions of the institutions that they represent in the settlement.

Image cash letters (ICL): An electronic check file that includes batched data and is transmitted for clearing and settlement. Also known as check cash letter.

Independent sales organization (ISO): An organization that provides merchant processing functions on behalf of the acquirer. These functions may include soliciting new merchant accounts, arranging for terminal purchases or leases, and providing backroom services. An ISO and an MSP are functionally similar. The acquirer must register all ISOs/MSPs with the bank card associations. Also, see the definition of MSP.

Initiation: A participant (e.g., payor, payee, or third party) initiates the payment process by sending an instruction to another individual or entity that begins a process that ends in a payment.

Interchange fee: A fee paid by one bank to another to cover handling costs and credit risk in a bank card transaction. The interchange fee, a percentage of the transaction amount, is derived from a formula that takes into account authorization costs, fraud and credit losses, and the average bank cost of funds.

Issuing bank: Institution (or agent) that issues a payment card to the cardholder. Sometimes referred to as issuer.

Large-value payment system: A wholesale payment system used primarily by financial institutions in which large values of funds are transferred between parties. FedWire and CHIPS are the two large-value payment systems in the United States.

Machine learning (ML): ML is a subcategory of AI and is a method of designing a sequence of actions to solve a problem that optimizes automatically through experience and with limited or no human intervention.[112] ML algorithms[113] give computers the ability to identify patterns without requiring a human to specify all of the pattern elements.

Member service provider (MSP): A nonmember of MasterCard who markets bank card merchant acceptance on behalf of MasterCard financial institutions. An MSP is functionally similar to an ISO. Also, see the definition of ISO.

Mobile payment: Payments transacted though the use of an electronic communications device, typically a mobile phone.

Multilateral netting: Payment transactions are pooled for simplification instead of being processed separately.

Nacha: The association formally known as the Electronic Payments Association and formerly known as the National Automated Clearing House Association is the sponsor and national administrator for the automated clearing house and participating financial institutions in the United States.

National Settlement Service (NSS): The NSS is a multilateral settlement service offered to member depository institutions owned and operated by the Federal Reserve Banks. NSS is offered to depository institutions that settle for participants in clearing houses, financial exchanges, and other clearing and settlement groups. Settlement agents acting on behalf of those depository institutions electronically submit settlement files to the Federal Reserve Banks. Files are processed on receipt, and entries are automatically posted to the depository institutions' Federal Reserve accounts. Entries are final when posted.[114]

Near-field communication (NFC): A technology for digitally transmitting information over short distances (usually between a smartphone and another device) using radio waves.

---

[112] For more information, refer to the Financial Stability Board's November 2017 report, "Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications."

[113] An algorithm is a set of computational rules to be followed to solve a mathematical problem. More recently, the term has been adopted to refer to a process to be followed, often by a computer.

[114] For more information, refer to the "Retail Payment Systems" booklet of the *FFIEC IT Examination Handbook.*

Net settlement: Settlement of payment transactions in a batch of credits and debits that are combined for a total.

Non-funding participants: Participants that settle their net activity for the day using a designated correspondent bank that is a funding participant.

Originating depository financial institution (ODFI): A participating depository financial institution with respect to entries that (1) it transmits directly or indirectly to an ACH operator for transmittal to an RDFI and (2) on which it is designated as the ODFI. An RDFI is not considered an ODFI solely by reason of its initiation of acknowledgment entries, return entries, extended return entries, or notifications of change.

Payment: A transfer of value.

Payment card: A card that can be used by a cardholder and accepted by a merchant to make a payment for a purchase or in payment of some obligation.

Payment channel: A commerce path or conduit that exists to connect buyers with sellers or merchants in a marketplace for the purpose of initiating business transactions and settling those exchanges in some form of payment activity.

Payment platform: Collection of hardware, software, and middleware technology designed to manage, move, and process data for the purpose of performing payment transactions in accordance with a set of standard authentication and communication protocols.

Payment system: The mechanisms, rules, institutions, people, markets, and agreements that make the exchange of payments possible.[115] This definition applies to the discussion of payment systems throughout this booklet, but does not apply to the requirements of 12 CFR 7.1026. Refer to 12 CFR 7.1026(a)(5) for the definition of "payment system" applicable to 12 CFR 7.1026.

Payment technology infrastructure: Software, hardware, telecommunication protocols, data-security, layered techniques, and automated control systems used to initiate, process, monitor, and settle payment transactions.

Payments ecosystem: The landscape or totality of payment systems and mechanisms that operate, support, and connect payment products, services, and networks.

Person-to-person (P2P): A payment or a funds transfer initiated by a person and made to another person.

Person-to-business (P2B): A payment or a funds transfer initiated by a person to benefit a business.

[115] Ibid.

Phishing: A type of social engineering that involves sending fraudulent emails to a random or targeted list of individuals and directing them to provide their confidential information or to perform other tasks at a spoofed website.[116]

Platform: Consists of a collection of hardware, middleware, and a range of software frameworks designed to process instructions that perform logic to manage, manipulate, and move data in accordance with a set of authentication and communication protocols.

Real-time gross settlement: Continuous settlement of payments as they are processed.

Real-time payments: Recipients receive payments within seconds of the sending bank initiating the transaction.

Receiving depository financial institution (RDFI): A participating depository financial institution with respect to entries that (1) it receives from the ACH operator to the accounts of receivers and (2) on which it is designated as the RDFI.

Reconciliation: Reconciliation is the process through which responsible parties verify that the records issued by the entities involved in a transaction match. The reconciliation process can include appropriate reversals and post-transaction analysis.

Remote deposit capture (RDC): A deposit transaction delivery system that allows a bank to receive digital information from deposit documents captured at remote locations.

Remotely created check (RCC): A type of check transaction whereby a digital image is created that is based on an authorization to debit an account, and, instead of a signature, the RCC includes a statement that the account holder authorized the payment.

Retail payments: Payments, typically small, made in the goods and services market.[117]

Returned depository items (RDI): A check that has been returned unpaid to the depositing bank because the BOFD did not honor the check.

Standard Entry Class (SEC) code: Three-character code used to identify the type of ACH payment.

Settlement: Settlement irrevocably extinguishes the obligation of the payor's depository institution and often occurs simultaneously with receipt of funds. Settlement can occur on a gross basis, in which each transfer is settled individually, or on a net basis, in which credits and debits periodically offset each other.

[116] For more information, refer to OCC Bulletin 2005-24, "Threats from Fraudulent Bank Websites: Risk Mitigation and Response Guidance for Website Spoofing Incidents."

[117] For more information, refer to the "Retail Payment Systems" booklet of the *FFIEC IT Examination Handbook.*

Smishing: A type of social engineering that involves sending fraudulent text messages to a random or targeted list of individuals and directing them to click on a link that will download malicious programs onto their devices or direct them to a spoofed website where individuals are asked to provide confidential information.

Sovereign risk: The risk that action by a government may affect either a system or particular participants in a system. This action could be detrimental to other participants in the system. An example of this risk would be the imposition of exchange control regulations on a bank participating in international foreign exchange activities.

Substitute check: The electronic image of the original paper check.

SWIFT: Society for Worldwide Interbank Financial Telecommunication. A global member-owned cooperative and provider of secure financial messaging services.

Third-party payment processor (TPPP): An entity that provides payment-processing services to merchants and other businesses. TPPPs traditionally contract primarily with merchants with physical locations to process the merchants' transactions (e.g., RCC and ACH). TPPPs often use their commercial bank accounts to conduct payment processing for their clients. For example, a TPPP may deposit into its account RCCs generated on behalf of a merchant client, or process ACH transactions on behalf of a merchant client. In either case, the bank does not have a direct relationship with the merchant.

Third-party sender (TPS): A type of TPPP that acts as an intermediary in transmitting entries between an originator and an ODFI, including through direct access, and acts on behalf of an originator or another third-party sender. A TPS is never the originator for entries it transmits on behalf of another organization but may be an originator of other entries in its own right.

Tokenization: When applied to data security, the process of substituting a sensitive data element with a non-sensitive equivalent—referred to as a token—that has no extrinsic or exploitable meaning or value. Tokenization is used to protect sensitive information.

Wholesale payment: Funds transfer using large-value payment systems, such as Fedwire and CHIPS, to make payments related to their own operations (e.g., federal funds transactions) between businesses or governments or to transfer funds on behalf of their customers. Wholesale payments are typically large-value transactions and generally used to purchase, sell, or finance securities transactions; disburse or repay loans; settle real estate transactions; and make large-value, time-critical payments, such as payments for the settlement of interbank purchases and sales of federal funds, settlement of foreign exchange transactions, or other financial market transactions.

Wire transfer: A general term used to describe funds sent from one customer or bank to another customer or bank using a large-value payment system (e.g., Fedwire and CHIPS).

Appendix C: Abbreviations

The abbreviations listing includes terms abbreviated in this booklet and terms that examiners may find abbreviated in bank documents, such as management and board reports.

ABA	American Bankers Association
ACH	automated clearing house
AI	artificial intelligence
API	application programming interface
ARC	accounts receivable entry
ATM	automated teller machine
AVS	address verification system
B2B	business-to-business
B2P	business-to-person
BCM	business continuity management
BCP	business continuity plan
BIA	business impact analysis
BIN	bank identification number
BIS	Bank for International Settlements
BOC	back office conversion
BOFD	bank of first deposit
BSA/AML	Bank Secrecy Act/anti-money laundering
CCP	central counterparty
CFP	contingency funding plan
CFR	Code of Federal Regulations
CHAPS	Clearing House Automated Payments System
CHATS	Clearing House Automated Transfer System
Check 21	Check Clearing for the 21st Century Act
CHIPS	Clearing House Interbank Payments System
CIE	customer-initiated entry
CLS	Continuous Linked Settlement Bank
CME	Chicago Mercantile Exchange Clearing
CNP	card not present
CP	card present
CPSS—IOSCO	Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions
CSC	card security code
CTR	currency transaction reporting
CVC	card validation code
CVV	card verification value
DFI	depository financial institution
DLT	distributed ledger technology
DR	disaster recovery
DTC	Depository Trust Company
DTCC	Depository Trust and Clearing Corporation

EBT	electronic benefit transfer
EFT	electronic funds transfer
EFTA	Electronic Fund Transfer Act
EIC	examiner-in-charge
EMV	Europay, Mastercard, and Visa
EPN	Electronic Payments Network
FEIC	functional examiner-in-charge
FFIEC	Federal Financial Institutions Examination Council
FICC	Fixed Income Clearing Corporation
FMI	financial market infrastructure
FMU	financial market utility
FSA	flexible spending account
FSOC	Financial Stability Oversight Council
GLBA	Gramm–Leach–Bliley Act
IAT	international ACH transaction
ICA	Interbank Card Association
ICL	image cash letters
ICQ	internal control questionnaire
IIN	issuer identification number
IL	OCC Interpretive Letter
INVN	independent node verification network
ISO	independent sales organization
IT	information technology
KPI	key performance indicators
KRI	key risk indicators
MICR	magnetic ink character recognition
MIS	management information systems
ML	machine learning
MSP	member service provider
NFC	near-field communication
NSCC	National Securities Clearing Corporation
NSS	National Settlement Service
NYCE	New York Currency Exchange
OCC	Office of the Comptroller of the Currency
ODFI	originating depository financial institution
OFAC	Office of Foreign Assets Control
P2B	person-to-business
P2P	person-to-person
PAN	primary account number
PCI DSS	Payment Card Industry Data Security Standard
PIN	personal identification number
POP	point of purchase
POS	point of sale
PPD	prearranged payment and deposit
Pub. L.	public law
RCC	remotely created check

RCSA	risk control self-assessment
RDC	remote deposit capture
RDI	returned depository item
RDFI	receiving depository financial institution
RFID	radio frequency identification
RTGS	real-time gross settlement
RTP	real-time payment system
SDN	Specially Designated National
SEC	Standard Entry Class
SEPA	Single Euro Payments Area
SIFMU	systemically important financial market utility
SLA	service-level agreement
STP	straight through processing
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TARGET2	Trans-European Automated Real-time Gross Settlement Express Transfer System
TCH	The Clearing House
TEL	telephone-initiated ACH transaction
TPPP	third-party payment processor
TPS	third-party sender
TPSP	third-party service provider
UBPR	Uniform Bank Performance Report
UDAAP	unfair, deceptive, or abusive acts or practices
UDAP	unfair or deceptive acts or practices
USC	United States Code
WEB	internet-initiated ACH transaction

References

Listed references apply to national banks and federal savings associations unless otherwise noted.

Laws

12 USC 5462(2), "Designated Activity"
15 USC 45(a)(1)
Pub. L. 108-100, "Check Clearing for the 21st Century Act" (Check 21)
Gramm–Leach–Bliley Act

Regulations

12 CFR 7.1026, "National Bank and Federal Savings Association Payment System Memberships"
12 CFR 30, appendix B, "Interagency Guidelines Establishing Information Security Standards"
12 CFR 30, appendix D, "OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches"
12 CFR 204, "Reserve Requirements of Depository Institutions (Regulation D)"
12 CFR 210, "Collection of Checks and Other Items By Federal Reserve Banks and Funds Transfers Through Fedwire (Regulation J)"
12 CFR 210, subpart B, "Funds Transfers Through Fedwire"
12 CFR 229, "Availability of Funds and Collection of Checks (Regulation CC)"
12 CFR 233, "Prohibition on Funding of Unlawful Internet Gambling (Regulation GG)"
12 CFR 1005, "Electronic Fund Transfers (Regulation E)"
12 CFR 1026, "Truth in Lending (Regulation Z)"
12 CFR 1030, "Truth in Savings (Regulation DD)"
31 CFR 500, "Office of Foreign Assets Control (OFAC)"

Comptroller's Handbook

Examination Process
"Bank Supervision Process"
"Community Bank Supervision"
"Federal Branches and Agencies Supervision"
"Foreword"
"Large Bank Supervision"
"Sampling Methodologies"

Safety and Soundness
"Consigned Items and Other Customer Services"
"Corporate and Risk Governance"

"Credit Card Lending"
"Internal Control" (national banks)
"Internal and External Audits"
"Merchant Processing"

Consumer Compliance
"Compliance Management Systems"
"Depository Services"
"Electronic Fund Transfer Act"
"Unfair or Deceptive Acts or Practices and Unfair, Deceptive, or Abusive Acts or Practices"

OTS Examination Handbook

340, "Internal Control" (federal savings associations)

OCC Issuances

OCC Advisory Letter 1996-6, "Check-Kiting, Funds Availability, Wire Transfer Activity"
OCC Bulletin 2005-24, "Threats from Fraudulent Bank Websites: Risk Mitigation and Response Guidance for Website Spoofing Incidents"
OCC Bulletin 2006-39, "Automated Clearing House Activities: Risk Management Guidance"
OCC Bulletin 2007-2, "Fraudulent Cashier's Checks: Guidance to National Banks Concerning Schemes Involving Fraudulent Cashier's Checks" (national banks)
OCC Bulletin 2008-12, "Payment Processors: Risk Management Guidance"
OCC Bulletin 2009-4, "Remote Deposit Capture: Interagency Guidance"
OCC Bulletin 2010-13, "Liquidity: Interagency Policy Statement on Funding and Liquidity Risk Management."
OCC Bulletin 2010-24, "Incentive Compensation: Interagency Guidance on Sound Incentive Compensation Policies"
OCC Bulletin 2011-27, "Prepaid Access Programs: Risk Management Guidelines and Sound Practices"
OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"
OCC Bulletin 2016-18, "Cybersecurity of Interbank Messaging and Wholesale Payment Networks: FFIEC Statement"
OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures"
OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles"
OCC Bulletin 2019-16, "Consumer Compliance: Revised Interagency Examination Procedures"
OCC Bulletin 2019-37, "Operational Risk: Fraud Risk Management Principles"
OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"
OCC Bulletin 2020-13, "Pandemic Planning: Updated FFIEC Guidance"
OCC Bulletin 2021-36, "Information Security: "FFIEC Statement on Authentication and Access to Financial Institution Services and Systems"

FFIEC

Information Technology Examination Handbook
- "Business Continuity Management"
- "Information Security"
- "Management"
- "Retail Payment Systems"
- "Wholesale Payment Systems"

BSA/AML Examination Manual

Other

"Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications," Financial Stability Board (November 2017)
"Check Fraud: A Guide to Avoiding Losses"
"Current Report of the Financial Market Infrastructure Risk Task Force," Federal Reserve Bank of New York (May 2007)
"Federal Reserve Policy on Payment System Risk," Board of Governors of the Federal Reserve System
FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency," Financial Crimes Enforcement Network
"Guide to the Federal Reserve's Payment System Risk Policy on Intraday Credit," Board of Governors of the Federal Reserve System (July 2012)
"Operating Rules and Guidelines," Nacha (2020)
"Overview of the Federal Reserve's Payment System Risk Policy," Board of Governors of the Federal Reserve System (July 2012)
"National Terrorist Financing Risk Assessment," U.S. Department of the Treasury (2018)
"National Money Laundering Risk Assessment," U.S. Department of the Treasury (2018)