PRC PAYMENTS RISK COMMITTEE

Sponsored by: FEDERAL RESERVE BANK of NEW YORK

Best Practices for Payments, Clearing, and Settlement Activities

Report of the

Payments Risk Committee

As of April 2019

Sponsored by the Federal Reserve Bank of New York, the Payments Risk Committee is a private sector group that includes senior managers from several major banks in the United States. The Committee identifies and analyzes issues of mutual interest related to risk in payment, clearing, and settlement systems. Where appropriate, the Committee seeks to foster broader industry awareness and discussion and to develop input on public and private sector initiatives. Current members of the Committee are representatives of the Bank of America N.A., The Bank of New York Mellon, Citibank N.A., Deutsche Bank AG, Goldman Sachs, HSBC Bank USA, JPMorgan Chase, Morgan Stanley, MUFG Bank, State Street Bank and Trust Company, UBS AG, and Wells Fargo.

Contents

Introduction

The Payments Risk Committee ("PRC" or the "Committee") is a private-sector body sponsored by the Federal Reserve Bank of New York that works to identify and analyze risks in payments, clearing and settlement of financial transactions. The primary goal of the Committee is to foster enhancements to the safety and efficiency of financial market infrastructure, which includes identifying opportunities to strengthen the clearing and settlement of financial transactions.

Financial market infrastructures and their bank customers provide core infrastructure for the economy by facilitating a wide range of large value transfers (e.g., foreign exchange settlements, derivatives clearing, and government securities clearing). Because of the complexity of the interconnections between banks in the payments, clearing, and settlement ("PCS ") environment, and the importance of these activities, the Committee recognizes the importance of shared practices that enhance the safety and efficiency of PCS activities across the network of participants.

These best practices seek to affirm sound existing practices and suggest enhancements to generally practiced behavior. The best practices are not intended as binding rules or regulatory guidance.[1] As each bank considers these best practices, it should take into account its own unique characteristics, such as asset size, transaction volume, and the level of the bank's integration within the financial market infrastructure.[2]

The best practices effort will be a living document structured so that new practices can be added or existing practices can be modified to address changes and challenges over time.

[1] In addition to considering these best practices, banks should be sure that they are following all applicable laws and regulations at all times. In some cases, Financial Market Infrastructure rule books may set more stringent requirements that supersede best practices.

[2] For the most part, the Committee recommends that these best practices apply in their entirety to any large and medium sized financial institutions that are material participants in any of the major Financial Market Infrastructure in the United States, although there may be some applicability to participants in global FMUs.

Payment Lifecycle

The PRC defines the payment lifecycle as the interval of time beginning when a direct participant in a wholesale payment system first receives an instruction from the originator or originating bank (customer), and ending when such payment is settled and available to the beneficiary at their bank. The PRC focuses on practices related to operations, risk management and liquidity management. These practices, taken together, could reduce systemic risk amongst each bank that may play different roles in the PCS system by:

- Achieving final settlement as early in the day as practicable, without creating undue risks, which may include credit, operational, and liquidity risks.[3]
- Providing settled funds to the beneficiaries as early in the day as practicable, without creating undue risks among originating, intermediary, and beneficiary's banks in the payment lifecycle.
- Reducing the potential for failed payments, particularly for settlement late in the business day.

While a shorter lifecycle does not necessarily increase turnover of liquidity, the chances of liquidity being used multiple times can be enhanced with shorter payment lifecycles. Banks should therefore seek to shorten the payment lifecycle in a safe and efficient manner, taking a holistic view of the various risks they face and mitigating these during the lifecycle.

1. Promoting timely payment lifecycle

A bank should have internal policies and guidelines to manage wholesale payment flows throughout the settlement day:

A bank should have internal guidelines or benchmarks regarding payments throughput. In this context, payment throughput is the value/volume of payments to be settled by the bank in the wholesale payment system by certain times in the day.

- Internal guidelines should incorporate any throughput requirements established by the wholesale payment system if applicable.
- Internal guidelines should be commensurate for the bank's business model, risk appetite, customer base, and composition of payments.
- Banks should monitor adherence to their internal guidelines and should review their guidelines periodically, potentially under the auspices of a Key Risk Indicator ("KRI").

[3] CPMI-IOSCO defines final settlement as "the irrevocable and unconditional transfer of an asset or financial instrument, or the discharge of an obligation in accordance with the terms of the underlying contract." See paragraph 3.8.1 of the CPMI-IOSCO *Principles for financial market infrastructures*, available at https://www.bis.org/cpmi/publ/d101a.pdf.

A bank should avoid late day concentration of payments

In general, if a bank delays payments activity and accumulates liquidity, this can lead to late day concentrations of payments.[4] Late day concentrations could cause systemic liquidity imbalances as other banks delay payments as they await anticipated receipt of funds. To maintain an efficient wholesale payments system, banks are encouraged to optimize the timeliness of payments.

- On a real time basis, a bank should strive to update (i) its own balances with the wholesale payments system, (ii) its customer balances held on the bank's books, and (iii) credit line availability.
- A bank should establish appropriate intraday credit limits for customers to efficiently release payments from credit risk queues.
- A bank should prefund payments in the wholesale payments system, if relevant.
- A bank should have internal processes to identify payments that should be prefunded by customers and ensure funds are available early if appropriate.

2. Optimizing payments processing operations

A bank should conduct end to end straight through processing of payments.

Banks should conduct end to end straight through processing of payments and perfect each critical operational step to minimize most, if not all, delays in the lifecycle. A bank should:

- Minimize manual intervention in payment queues (e.g. due to payment message formatting errors) to allow payments to be processed straight through the wholesale payments system and all other banks in lifecycle.
- Net payments with counterparties bilaterally, where appropriate, to improve settlement efficiency while ensuring transparency on underlying transactions and discharge of contractual obligations is not compromised. A bank should encourage its customers to bilaterally net payments with their counterparties, where appropriate. All netting should be legally enforceable.
- Monitor and manage all relevant internal payment queues, such as repair, sanctions screening, credit risk, and liquidity management to avoid excessive backlogs of payments during the business day.
- Connect to external PCS systems and begin processing as soon as they are open for the day.

[4] Basel Committee on Banking Supervision's Risk Concentration Principles (1999) define liquidity concentration as an exposure with the potential to produce losses large enough to threaten a financial institution's health or ability to maintain its core operations (Basel December 1999). https://www.bis.org/publ/bcbs63.pdf

- Continuously monitor systems (internal service layers as well as external PCS systems) interfacing with an internal core payment system to ensure that they are operating effectively.
- Conduct frequent testing to help ensure the capacity, durability and redundancy of payment infrastructure in times of stress.

A bank should reconcile payments activity intraday

In addition to conventional end-of-day reconciliation, banks should reconcile incoming and outgoing payments intraday and against expected/historical flows. Banks should strive to reconcile in real-time. More frequent reconciliation can help banks detect any issues or anomalous activities, such as pending credits/receipts of funds, suspected fraudulent transactions, and irreconcilable receives. Frequent reconciliation also enables banks to recover payments data more readily. Banks that detect any issues should remediate them as soon as possible, and if appropriate, advise payment system operators.

A bank should have communication guidelines in place to address issues or reporting as applicable:

A bank should establish communications protocols among its internal functions (for example, operations, treasury and front office) as well as with customers, its own counterparties and PCS service providers. A bank should:

- Provide real time or near real time reporting to customers on their balances and activities.
- Maintain lines of communication between the treasury, operations, and front office team to ensure unusual intraday liquidity requirements (amount/timing) are quickly detected, escalated, and continuously monitored. Additionally, escalation protocols should be clear, well understood, and tested regularly.
- Have standardized reporting, which includes baseline requirements and thresholds that are shared across all internal payment functional areas.
- Communicate with customers, external PCS system providers, and other stakeholders as applicable should they experience an outage to avoid further delays in payment execution.

3. Identifying and prioritizing time sensitive payments

A bank should identify and prioritize its own and customers' time sensitive and critical payments.

A bank should first define and identify time sensitive and critical payments and then be able to prioritize them.[5] The implication of missing these critical payments could result in financial penalty, default, reputational, and legal risk. More importantly, executing time sensitive and critical payments as early as possible would reduce overall systemic risk by reducing late day concentration of payments, avoiding a

[5] BCBS 248: Time-specific obligations are defined: obligations which must be settled at a specific time within the day or have an expected intraday settlement deadline (Basel April 2013). https://www.bis.org/publ/bcbs248.pdf

critical payment failure, and avoiding settlement delays in PCS systems. Those payments could include critical payments related to PCS infrastructures, funds transfers that support critical Federal Reserve operations, and customer designated priority payments. A bank should:

- Have a process in place to identify proprietary and customers' time sensitive and critical payments.
- Monitor time sensitive and critical payments in various queues in the internal payment system.
- Have a documented and tested escalation process concerning issues in executing time sensitive and critical payments.
- Have a process in place to prioritize time sensitive and critical payments with proper controls.
- Have the ability to extract and back up procedures to execute time sensitive and critical payments in the event of system delays or failures.

Direct and Indirect Participation in Payment Systems

Having access to large value payment systems ("LVPS") is vital for banks. There are two primary ways to access an LVPS: 1) direct participation in an LVPS or 2) indirect participation in an LVPS, defined herein as the use of the services of a correspondent bank that participates in an LVPS directly. Opportunities for direct participation are rather limited as it is available only to banks that meet certain regulatory and LVPS requirements in order to gain and maintain such access; whereas indirect participation is available to a large number of banks in both home and foreign currencies. Indirect access may not provide the level of control and market transparency offered by direct participation, but it provides banks that have a relatively small volume of payments or require specialized payment services with the ability to access markets necessary to achieve their strategic and business needs. For either direct or indirect participation, banks should consider ways to proactively address the inherent credit, liquidity, legal, regulatory, and operational risks. While direct and indirect participation arrangements share similar risk considerations, the risks might manifest themselves in different ways and require different risk management approaches.

This chapter offers operational considerations and best practice recommendations for direct and indirect participation in payment systems. Given that the payment system operator has rules and requirements that govern direct participation in the payment system, these best practices build upon those requirements. Correspondent banking relationships are less defined and as such, we will focus best practices on indirect participation. This chapter is organized as follows:

- Direct participation with a focus on maintenance of access
- Indirect participation

Direct Participation

In maintaining direct participation in an LVPS, a bank must meet the minimum requirements[6] imposed on them by the payment system as well as by regulatory bodies. However, there are additional practices banks should consider implementing to proactively manage the various risks to minimize potential systemic contagion. The bank should:

- Establish an oversight process of payment system risks that includes periodic review of payment system risks and processes to mitigate identified risks.
- Fully document and test business continuity/resiliency plans as part of operational risk management. These plans should include scenarios that examine a significant interruption in access to the LVPS, as well as an alternative process to continue to execute time critical payments. The plan should be tested regularly to ensure effectiveness and to minimize impact from a range of disruptive

[6] Those requirements may include Banking Circular 235 (https://www.occ.gov/static/news-issuances/bulletins/pre-1994/banking-circulars/bc-1989-235.pdf) or third party relationship guidance provided by the Federal Reserve (https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf) and Office of Comptroller of Currency (https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html)

events, including minor system outages, facility disruptions such as power outage, or a catastrophic scenario.

- Maintain available capital/collateral/liquidity to ensure continued system access, as an LVPS may impose additional liquidity requirements or invoke loss sharing especially during times of idiosyncratic or market stress for the system or the participant.
- Monitor and provide reporting for available and utilized lines of credit provided by the LVPS. The bank should also have contingency plans in place to address any dislocations in access to credit, should credit no longer be made readily available or potentially retracted by other participants due to idiosyncratic or market stress.
- Incorporate liquidity stress testing, develop liquidity contingency plans and meet regulatory liquidity requirements as prescribed. If a direct participant is providing transactional services to their customers, the direct participant should be able to monitor customer activities and set strict and manageable counterparty credit and liquidity limits, or require customers to prefund payments prior to execution.
- Review and document emerging risks, such as wholesale payments fraud, data privacy and information security, and implement adequate controls to manage and mitigate those risks.
- Ensure the costs and other required resources of maintaining direct participation are well understood and adequately provided for, including unencumbered liquidity needs for normal and idiosyncratic scenarios, and staffing and IT infrastructure to meet regulatory and payment system operator requirements.

Indirect Participation

Banks may require access to products and services in markets where they do not maintain required infrastructure to achieve their business needs. In this case, a relationship with a correspondent bank that participates directly in a payment system can provide access. Accessing the payment system via a correspondent bank can shield the indirect participant from the direct liquidity risk and loss-sharing that may arise from another direct participant's default. However, indirect participants still face operational, liquidity, credit, and business risk as a result of reliance on the correspondent bank for transactional services. Concentration risk may be another factor if there are a limited number of correspondent banking service providers in the market. Operational and risk management considerations for indirect participation focus more on the relationship with the correspondent bank providing the payment services instead of the relationship with the LVPS. These best practices address governance, operational risk, liquidity, legal and regulatory considerations, and information technology.

Governance Considerations

A bank should have a governance program in which relevant stakeholders are engaged to evaluate indirect participation in a payment system and to monitor the bank's continued access.

A bank should:

- Create a governance program, periodically identify and review potential risks associated with the correspondent banking relationship, and determine ways to accept and manage the risks. Those reviews should include onsite visits with correspondent banks and/or service review meetings, where necessary.
- Have policies and processes in place that guide selection of a correspondent bank that meets risk tolerance levels including, but not limited to, credit, operational, and reputational risks.
- Maintain consistent lines of communication between relevant stakeholders on any current and potential governance policies and procedures as decision making, business strategies, and financial outlooks evolve.

Liquidity Considerations

A bank should understand liquidity implications of utilizing a correspondent bank for access. The largest liquidity implication for a bank using correspondent banking services involves the failure of the correspondent bank to execute payments. A bank should have an adequate liquidity buffer in the form of cash, credit lines or collateral to account for both abnormally high amounts of transactions and potential stressed environments.

A bank should:

- Obtain appropriate credit and/or liquidity facilities from the correspondent bank to address potential needs arising from unexpected shortages.
- Establish and maintain contingency liquidity arrangements to meet critical payment obligations in the event that the correspondent bank is unable to execute payments on the bank's behalf due to stress or failure.

Regulatory and Legal Considerations

A bank should understand the regulatory and legal environment, including any potential impact across currencies and international boundaries, which govern its relationship between the payment system and any third parties. Indirect participants are accountable for compliance with relevant regulatory requirements. Service and product level agreements/contracts with a correspondent bank present additional legal considerations. Banks using correspondent banking services must account for any contractually binding ramifications in the event that there is a dispute between the bank and a correspondent bank or in the event that a correspondent bank should go into default.

A bank should:

- Account for and monitor domestic and international legal and regulatory restrictions on the use of the account and payments service (for example, certain types of payments cannot be executed by the correspondent bank in an international setting). Local regulations may require additional details such as import/export license, remittance purposes, and investment approval.

- Document protective, enforceable agreements with its correspondent bank that clearly define each party's obligations. The agreements should include, but are not limited to, services provided, business continuity and contingency plans, dispute resolution, termination and withdrawal provisions, and expectations around confidentiality, privacy, and information security. These agreements should be reviewed on a regular basis and revised as needed and as permitted.

Operational Considerations

A bank should establish operating policies and procedures to meet the operating rules imposed on them by a correspondent bank to minimize errors and optimize efficiency. The bank should establish service level agreements with internal and external partners to manage each other's performance. The execution and reconciliation considerations are driven by each bank's unique set of circumstances.

A bank should:

- Establish a two-way communication process with its correspondent bank to resolve any potential issues in an efficient and timely manner. This process should be supported by up-to-date contact information at both the indirect participant and correspondent bank, as well as internal escalation and response procedures at both firms.
- Ensure that systems are in place to monitor transaction activity and intraday liquidity position in real time and to reconcile payments in real-time.
- Request and have the ability to receive real time balance and transactional information reporting from its correspondent bank.
- Perform sufficient and ongoing due diligence with the correspondent bank and ensure regularly that the correspondent bank maintains business continuity processes per policies/procedures that accurately reflect the materiality/risk-tolerance of accepting inherent risks of third-party reliance.
- Establish procedures to cancel, stop, and recall payments for pending payment instructions with its correspondent bank.
- Fully document and test business continuity/contingency plans in place to cover any disruption of services provided by the correspondent bank.
- Have a contingency arrangement with the correspondent bank to execute time critical payments should the indirect participant have a system outage which cannot be recovered in a timely manner.
- Create, independently or in partnership with its correspondent bank, an alternative process including, but not limited to, working with multiple correspondent banks to continue to execute time critical payments should the primary correspondent bank services become unavailable and regularly test the contingency process.

Information Technology Considerations

An indirect participant should have the infrastructure and knowledgeable staff capable of maintaining information technology to ensure systems operate efficiently with its correspondent bank. The effectiveness of controls must be regularly validated.

A bank should:

- Ensure IT infrastructure can facilitate daily operating requirements including real-time transactional and intraday liquidity monitoring, reconciliation, and reporting efficiently.
- Conduct vigorous IT testing to ensure that payments will be straight-through processed by the correspondent bank and the indirect participant can receive all types of applicable reporting from the correspondent bank and integrate them into their reporting program.
- Take into special consideration back-up IT facilities should there be a disturbance or shutdown in either bank's primary transaction system(s).

Cost Considerations

Cost should not be the sole criteria when deciding on a correspondent bank. All costs and requirements of indirect participation should be fully understood and evaluated, once each of the considerations is reviewed and satisfied, or risk mitigated and accepted.

A bank should be fully aware of and assess:

- Cost of different types of possible transactions with the correspondent bank, including cost tiers vs. projected payment volumes.
- Additional costs associated with a backup correspondent banking service provider(s)
- Cost associated with meeting each of the considerations in addition to technology costs, fixed or variable.