# IT Risk: Payment Systems and Operations

# Agenda – Purpose of Presentation

- Describe why high volume and payments system transactions generate operational risk.
- Identify components of internal controls processes that effectively cover products, activities, processes, and systems for operational risk.
- Recognize sound controls for front end, middle, and back office processes.
- Recognize the roles Financial Market Infrastructures (FMIs) play in the business activities of a firm and the risks associated with doing business with them.

# Primary Types of Payment Systems

| Payment System | Summary |
| --- | --- |
| **Retail** | Retail payments usually involve transactions between two consumers, between consumers and businesses, or between two businesses. Given the consumer-oriented nature of these payments, they tend to generate a large volume of transactions each day, though the dollar amount of each transaction is relatively small. |
| **Wholesale** | Wholesale payments typically take place to support domestic and international commercial activities, such as commercial loan and real estate transactions and financial market-related activities like corporate and governance securities and foreign exchange transactions. Wholesale payments, thus, tend to be large in value per transaction but small in terms of the volume of transactions generated daily in comparison to retail ones. |

# Retail Payment Instruments

- Payment instruments for retail purchases of goods and services are used to:
  - receive payments as a merchant;
  - pay one-time and recurring bills;
  - move payments between a consumer's account or the account of another consumer; and
  - access funds to make a payment, such as receiving cash from an automated teller machine (ATM) or with a credit card advance.

# Retail Payment Instruments

- Retail payments, driven by technology innovations and customer demands for faster payments, include:
  - Automated Clearing House (ACH)
  - Credit Card
  - Debit Card
  - Electronic Instruments (Mobile and Internet)

# Non Bank Third Parties

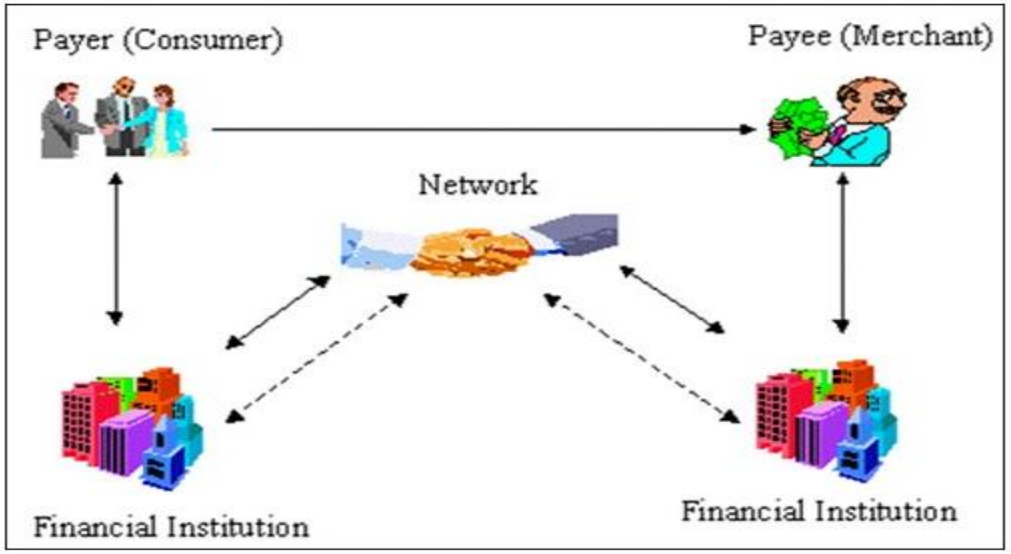
- Increased participation of nonbank third parties
  - Forces innovation
  - Lengthens transaction chain
  - Drives strategic partnerships
  - Requires diligent oversight
  - Necessitates fraud detection evolution

# Governance

- Governance process for evaluating risks introduced with new payment instruments should consider:
  - Deployment
  - Implementation
  - Use, both internally and by customers
  - Fraud detection

# Clearing and Settlement

- **Clearing:** transfer and confirmation of information between the consumer and merchant
- **Settlement:** actual transfer of funds between payer and payee's financial institution



# Financial Market Utilities

- Multilateral systems that provide the infrastructure for:
  - Transferring
  - Clearing
  - Settling payments, securities, and other financial transactions
- Among financial institutions or between financial institutions and systems
- Firms were recognized as systemically important as operational failure could increase the risk of significant liquidity risk or disruption in flow of credit

# Operational Risk Exposure

| Exposure | Summary |
|---|---|
| **Fraudulent transaction** | Transactions resulting from fraud have always been a source of operational risk with respect to check processing. While automated software detection systems are designed to interface with various payment systems and detect fraud, payments that span multiple payment channels are still difficult to catch. Some fraud types have declined with the introduction of this software but, with new payment instruments available, this is a constant struggle to ensure Bank Secrecy Act/Anti-Money Laundering systems can be attributed to all payment instruments. |
| **Interconnectivity** | The complex interconnections between systems and vendors in the financial services industry also increase operational risk. It is difficult to find a firm that is not somehow connected to a shared service provider or other financial entities, as the nature of payment systems is to allow for settlement to take place across accounts and financial organizations. Even so, with greater connectivity, there is the risk that a single point of failure or malicious threat could have a compound impact. |
| **Technology innovations** | New technology is used to innovate the payment instrument offerings, as well as the payment clearing and settlement process itself. The use of still unproven technologies or products deployed from them has the ability to provide points of failure, as well as fraud or malicious exploitation. Further, controls over each payment instrument must be carefully considered prior to deployment to ensure it does not introduce unintended risks to the broader payment system. |

# Operational Risk Exposure

| Exposure | Summary |
|---|---|
| **Nonbank entities** | Fueled by the latest technologies and customer demands for new financial products and services, some nonbank entities serve as competitors while others have products that maybe used or acquired by financial institutions or competing service providers. Regulatory scrutiny over such entities is significantly different. Consequently, the ability for these entities to offer a stable, secure product or handle customer information in a compliant manner may pose a direct or indirect risk to payment systems. |
| **Cybersecurity** | Threats to cybersecurity continue to build as attacks evolve and the introduction of more electronic payment channels offer additional access points to be exploited. System availability has grown in importance, as more transactions and real time information is expected; thus, the threat of cybersecurity also poses a risk that a system or information will not be available or accurate when needed. |
| **Process failures** | Processes resulting in limitations of system automation or errors in human controls can also be a significant source of operational risk, either by allowing fraud or malicious actions to be taken or unintentional errors and omissions to occur. |

# Supervisory Considerations

- Front-end Controls
- Back-end Controls
- Disaster Recovery and Business Continuity
- Information Security
- Vendor Management
- New Product Risk Assessment
- Audit Plans
- Risk Reporting
- Cybersecurity Threats

# Business Resiliency – Sound Practices Paper

The four broad practices identified for core clearing and settlement organizations play a significant role in critical financial markets. They include:

- identifying clearing and settlement activities in support of critical financial markets;
- determining appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets;
- maintaining sufficient geographically dispersed resources to meet recovery and resumption objectives; and
- routinely using or testing recovery and resumption arrangements.

# Payment Systems Evolution - BlockChain