OFFICE OF FINANCIAL RESEARCH

Technology Vulnerabilities for Financial Stability

Stacey Schreft

Presentation to the OFR Financial Research Advisory Committee, October 1, 2024

Assessing financial stability risk

Definition of "financial stability"

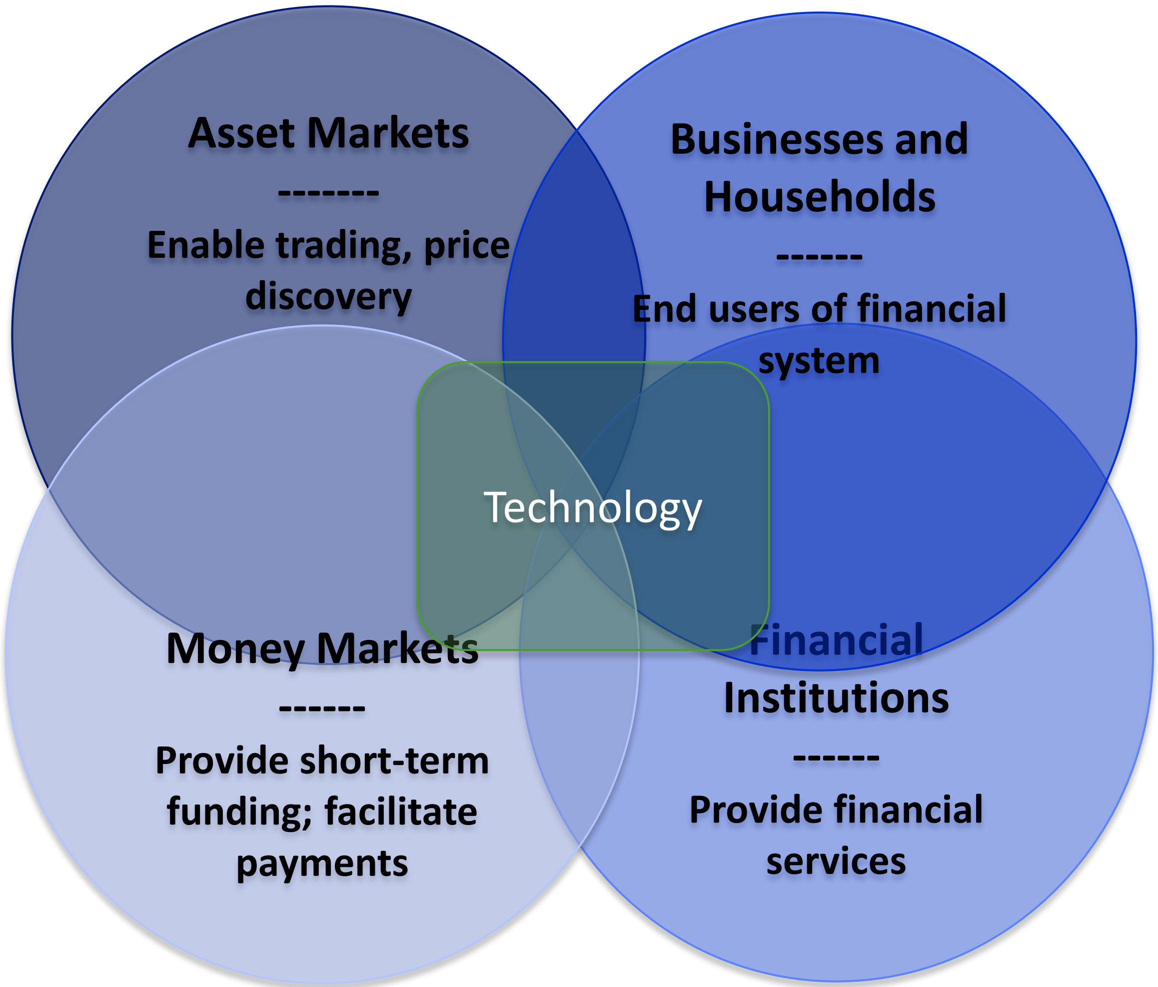
- When the financial system can provide its critical functions to the economy even under stress

Distinguish vulnerabilities from shocks

- Vulnerabilities: weaknesses that make the financial system susceptible to shocks that can impair financial stability
- Shocks: adverse events that can disrupt the functioning of vulnerable parts of the financial system; usually unpredictable

Focus on vulnerabilities; may be apparent only after a shock hits

Four components of financial system



Common technology vulnerabilities

24/7 operations

- Less downtime for response and recovery

Lack of operational resilience

- Inadequate cybersecurity, internal controls, business continuity plans

Human errors and accidents

Technology service providers (TSPs), especially of digital services, with large market share

- Service outages can bring widespread disruption

The technology transmission channel

Technology shock occurs

Malicious attack, accident, or error

Vulnerabilities exist

Limited defenses

Weak internal controls

Limited response and recovery capabilities

Incident disrupts or harms

Systems offline

Money, data stolen

Data corrupted

System vulnerabilities amplify the shock

Data, operational dependencies

Critical services

Time sensitivity

Confidence

Financial stability impaired

Financial system cannot perform one or more essential functions

Note: Based on OFR *2017 Financial Stability Report*, pg. 8

Asset Markets

Through tech, vulnerable to impaired market functioning

High-frequency and algorithmic trading

- Sudden failure to participate may constrain liquidity
- Algorithms may cause price distortions and volatility

ICBCFS – mid-sized broker; global clearing, settlement, financing

- Ransomware forced it offline
- Treasury fails-to-deliver rose 144% from day before, even though customers rerouted most trades

Asset Markets

Enable trading, price discovery

Businesses and Households

OFR

Through tech, vulnerable to business disruption and fraud, increasing default risk

Financial institutions incur most fraud costs

Tech shocks to nonfinancial businesses can reduce liquidity

- Change Healthcare – a claims clearinghouse (a central counterparty)
- Handled $2 trillion in claims and 44% of funds flowing through medical system; about 7% of GDP
- Liquidity provision mitigated the effect
  - Programs for advances against claims by U.S. government and parent of Change
  - Similar to Federal Reserve discount window

Businesses and Households

End users of financial system

Financial Institutions

Through tech, vulnerable to business disruption and fraud, increasing insolvency risk

Technology shocks can quickly reduce liquidity

- Classic example: Knight Capital's collapse
- ICBCFS received $9 billion in credit from BNY
    - Parent repaid the debt

Fraud

- AI aids fraud detection, but also makes fraud easier
- Opening accounts, unauthorized account access or takeover
- Fraud costs banks about $4.40 for each $1 of fraudulent transactions

Financial Institutions

Provide financial services

Money Markets

Through tech, vulnerable to business disruption that raises the risk of runs

Especially problematic are disruptions at financial market utilities …

- Whether public or private sector

… and TSPs that provide critical services

- Finastra – like Change Healthcare – but smaller
- Cyberattack forced it offline; banks and their customers lost access to many tech applications
- Disrupted wire transfers

Money Markets

Provide short-term funding; facilitate payments