Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis

Thomas M. Eisenbach Anna Kovner Michael Junho Lee*

Bank of Canada Annual Economic Conference, November 2020

* Federal Reserve Bank of New York. The views expressed are those of the speaker and do not necessarily reflect the position of the Federal Reserve Bank of New York or the Federal Reserve System. In compliance with FOMC Policy on External Communications during blackout periods, during this presentation the speaker will refrain from expressing views or providing analysis to members of the public about current or prospective monetary policy issues.

Cyber risk increasingly important factor of systemic risk

- “Pre-mortem" approach to assessing cyber risk in the financial system
    1. Assume a **successful cyber attack**, build empirical framework to understand how attack would be amplified
    2. Analyze network impact of various scenarios
- Key dimensions with **financial stability** in mind:
    - How might cyber risk be amplified and/or propagated?
    - What are the systemic features specific to cyber risk?

Main Results

- **Main Scenario**: Cyber attack on one of five most active U.S. banks
  - Significant dislocation of liquidity within system
  - Amplifications by adversely impacting other banks' liquidity
- Banks' strategic **liquidity hoarding** can propagate shock
  - Forgone payments: 75% of daily GDP on average, up to 250% of daily GDP
  - Disproportionately impacts financial market activity
- Attacker's intent and information brings rise to **tail risk**
- **Correlated Vulnerabilities**
  - Technological linkages between banks, e.g. **third party providers**
  - **Reverse stress test**: interruptions originating from small banks sufficient to impair significant amount of the system

Empirical setting: Wholesale payments system

- Key area where cyber attack may have systemic impact
  - Smooth functioning depends on coordination
  - Scope for strategic behavior
- Real and financial spillovers
- Fedwire Funds data allow analysis of complete network of interactions

Framework for Cyber Vulnerability

- Single-day impact of cyber attack on top-5 institution
- **Shocked institution** cannot send payments but can receive
  - Comprised availability and/or integrity
  - Institutional feature
- Direct impact of attack
  - Payment failures
  - Liquidity “black hole”

Strategic Behavior of Banks

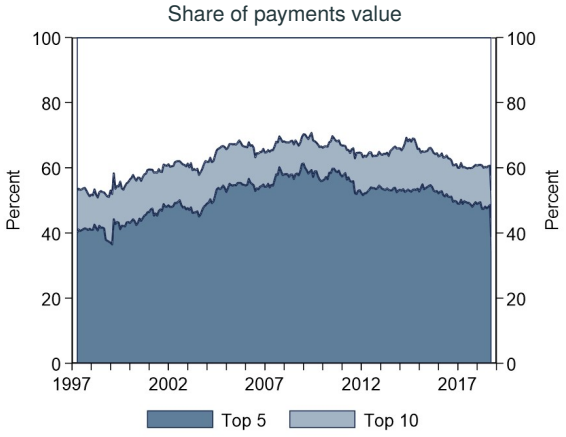
Two sets of scenarios on banks' reaction

1. **Baseline.** Other banks' payment activity unaffected
   - Incomplete information on arrival of cyber attack
   - Inattention to delays in intraday payment flows
2. **Cascade.** Banks strategically hoard liquidity in response to shortages

Derivative Impact

- Failure to receive payments affects other institutions' liquidity position
- Identify banks that become **impaired institution(s)**
  - **Impaired** if counterfactual end-of-day reserves fall more than 2 std. dev. below average balance
  - Rolling threshold based on past 30 days for each bank

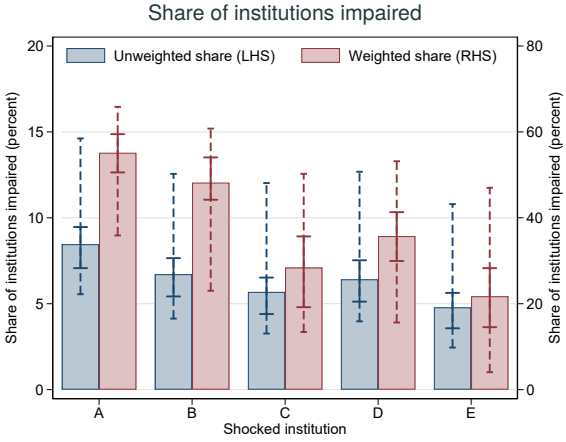
Payment Network Concentration



- Highly concentrated: 50% of payment value by top 5 institutions
- Core-periphery structure (Soramäki et al. 2007)

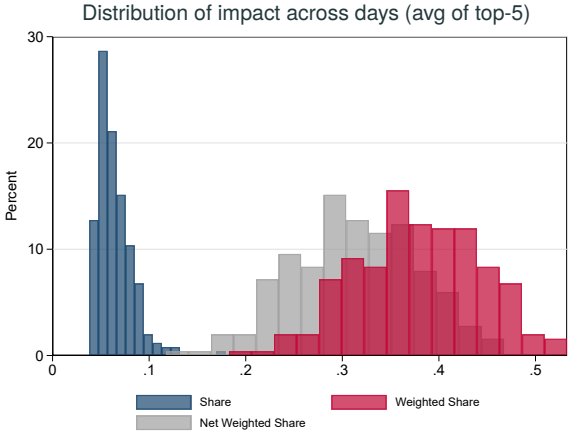
Baseline Scenario of Attack on Top 5

Network Impact of an Attack on Top-5



- Single day network impact substantial for any top-5
  - 5% to 9% of institutions impaired on average
  - Weighted impact over 4x larger on average: 22% to 55% of assets

Daily Distribution of Network Impact



- Average network impact across top-5
  - Greater weighted share reflects interconnectedness and concentration
  - Dispersion in network impact across days

Intent and Timing of Attacks

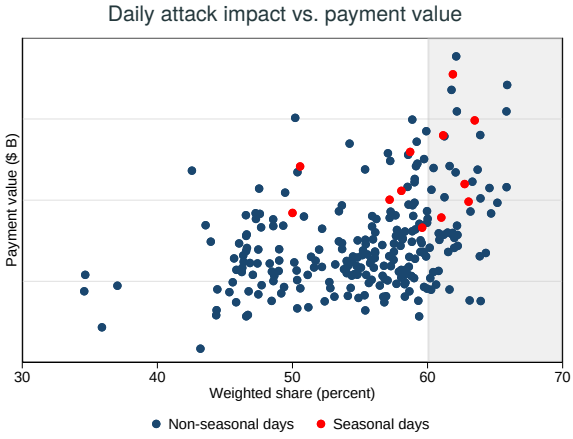
Potential for Strategic Attack

- A defining feature of cyber risk: attacker's intent
  - Objective could be to cause **maximum damage**
- Impact depends on attacker's information about
  - Payment system
  - Target institution

Key Variable: Information Set of Attacker

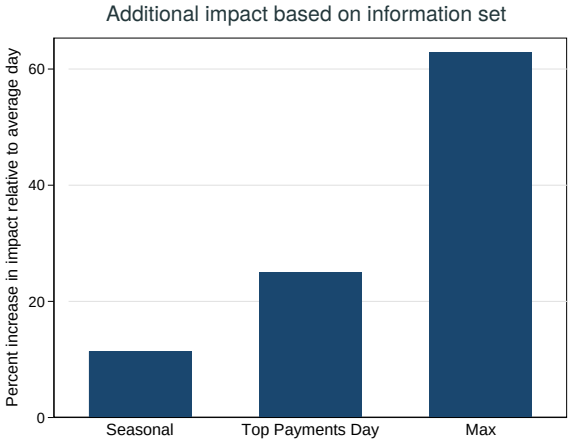
- **Public information.**
  Seasonalities, calendar effects, and market events all drive payment activity.
- **Private information on target institution.**
  Detailed information on target institution's payment activity to target days of high predicted payments in value.
- **Private information on network.**
  Detailed knowledge and data on target institution and network interconnectedness.

Timed Attacks



- Network impact correlated with payment activity
- Private information captures non-seasonal, high impact

Tail Risk Property of Cyber Risk



- Significant increases in impact (11% → 25% → 63%)
- With (Intent x Information), cyber risk can exhibit **tail risk** property

Liquidity Hoarding and Cascades

Liquidity Hoarding

- Baseline scenario assumes no active response
- Strategic reaction of single bank:

  Abnormal payment activity ➔ system illiquidity ➔ self-preservation

- Bank *i* is triggered to strategically hoard liquidity if:
  - Intraday payment deficit exceeds bank *i*'s maximum in sample period
  - Endogenous "black holes"

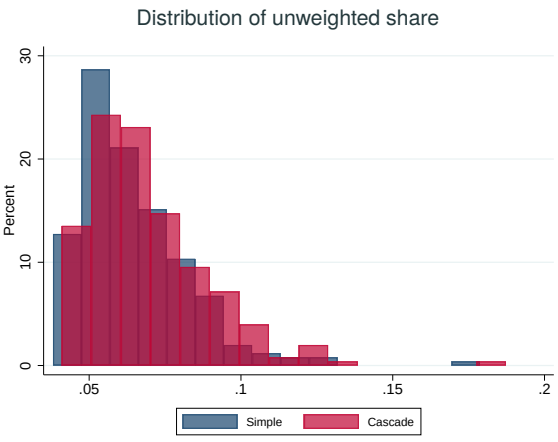
Effect of Liquidity Hoarding on Distribution of Reserves

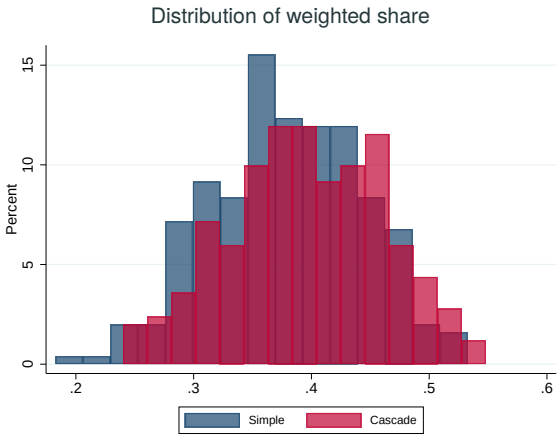
- Overall impact:

  More banks soak up liquidity ➔ more banks triggered ➔ cascade effect

- Potential effects ambiguous *a priori*:
  - Banks that hoard are less likely to become impaired
  - ... but banks further out more likely to become impaired

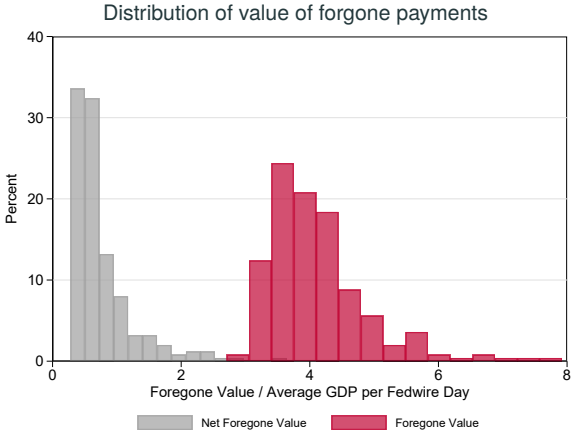
Cascade Scenario: Results





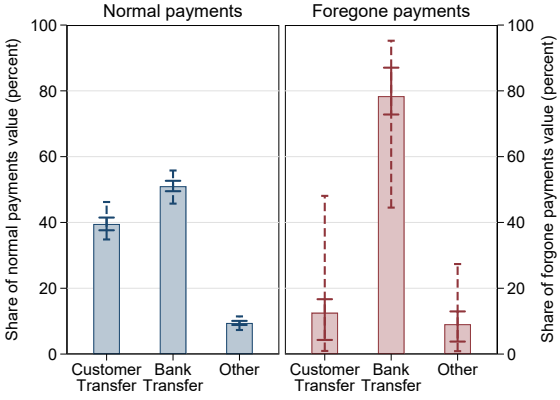
- Impact in cascade scenario similar to baseline
- Hoarding behavior slightly amplifies liquidity dislocation on average

Value of Forgone Payments



- Hoarding liquidity ➔ Forgoing payments that are vital for financial and real economy
- Significant disruptions
  - 5% to 35% of payment value not sent ➔ 1x to 11x daily GDP
  - Even net of attacked bank, 75% of daily GDP on average

Forgone Payments by Type



- Share of payments by business code for normal vs. forgone payments
  - Outsized representation of financial payment activity
  - Considerably more variation across days

Correlated Vulnerabilities

Other Scenarios: Correlated Vulnerabilities

- Technological commonality, e.g. third-party service providers
  - Potential to link banks that are otherwise unrelated
  - Magnifies impact through simultaneous shock throughout network

- Reverse stress test: attack on multiple small institutions
  - 10% of days could result in impairing at least one top-5
  - 1 or 2 branches of FBOs on average sufficient

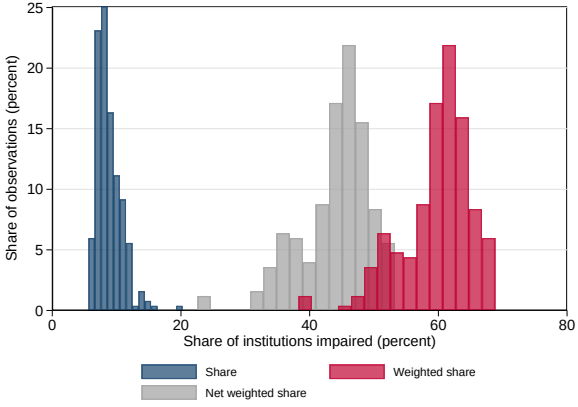
Attack on service provider Reverse stress test

Conclusion

- Simple framework to assess cyber vulnerability of US financial system
  - System vulnerable to crippling attack on most active banks
  - Sensitivity to knowledge and information available to attacker
  - Additional risks from significant service providers, small banks, and FBOs
- Implications
  - Shock can originate from multiple vulnerabilities
  - Significant interaction between liquidity and cyber resiliency
  - Additional liquidity may improve system's resiliency to cyber risk

Technological Commonality

Scenario: Attack on significant service provider specializing in data and system management for large and medium-sized banks



- Simultaneously effects multiple institutions → can have systemic consequences
  - 60% of assets impacted on average
  - Richer data on technological commonalities could reveal hidden risks

Back

Reverse Scenario

- One top-5 enough to inflict systemic risk
- Tradeoff – large, systemically important institutions
  - Resources and scale to invest in cyber defense
  - Heightened supervisory standards and regulation
- Malicious actor may instead target
  - Smaller, more vulnerable institutions
  - Network interconnectedness

Scenario: What is minimum number of **small** institutions to impair a top-5?

- “Mid-sized" entities – banks with less than $ 50 billion in assets
- “Small-sized" entities – banks with less than $ 10 billion in assets

Reverse Scenario

Scenario: Attack on small ($< \$10B$) or medium sized ($\$10 - \$20B$) banks

Number of attacked banks sufficient to impair a top-5 bank

Impairment	p1	p25	p50	p75	p99	Mean	SD	Days with Impairment
U_{10}	1	1	5	24	221	24	50	23 of 250
U_{50}	1	1	3	8	111	10	25	101 of 250

With branches of FBOs

Impairment	p1	p25	p50	p75	p99	Mean	SD	Days with Impairment
U_{10}	1	1	2	6	381	11	43	180 of 250
U_{50}	1	1	1	1	6	1	1	250 of 250

- Roughly 10% of days small banks can impair top-5
- With FBOs, attack on 2 or fewer sufficient
  - Large value of payments relative to assets
- Potential gaps in regulatory oversight to ensure cyber resiliency

Back