# The Propagation of Cyberattacks through the Financial System: Evidence from an Actual Event

Antonis Kotidis and Stacey Schreft

Annual ECB Banking Supervision Research Conference May 2-3, 2023

#### Disclaimer

The views expressed in this paper are those of the authors and do not reflect the position of the Federal Reserve System, its Board of Governors, the Office of Financial Research, or the U.S. Treasury Department.

## Cyberattacks and the financial system

- At a time of unprecedented digital transformation of the global financial system,
   cyberattacks emerge as a new threat to financial stability
- *Policymakers* are concerned that a cyberattack could trigger a financial crisis (e.g., Lagarde, 2021; Powell, 2019; 2021)
- <u>Academics</u> have emphasized cyberattacks as a financial stability risk and need for cyber monitoring and macroprudential regulation (e.g., Kashyap and Wetherilt, 2019; Duffie and Younger, 2019)
- <u>Industry participants</u> consistently cite cyber risk as a top risk in surveys (e.g., DTCC 2021 Systemic Risk Barometer; BoE 2021 Systemic Risk Survey; BoC 2021 Financial System Survey)
- Yet: no paper of an actual cyberattack that potentially threatened financial stability

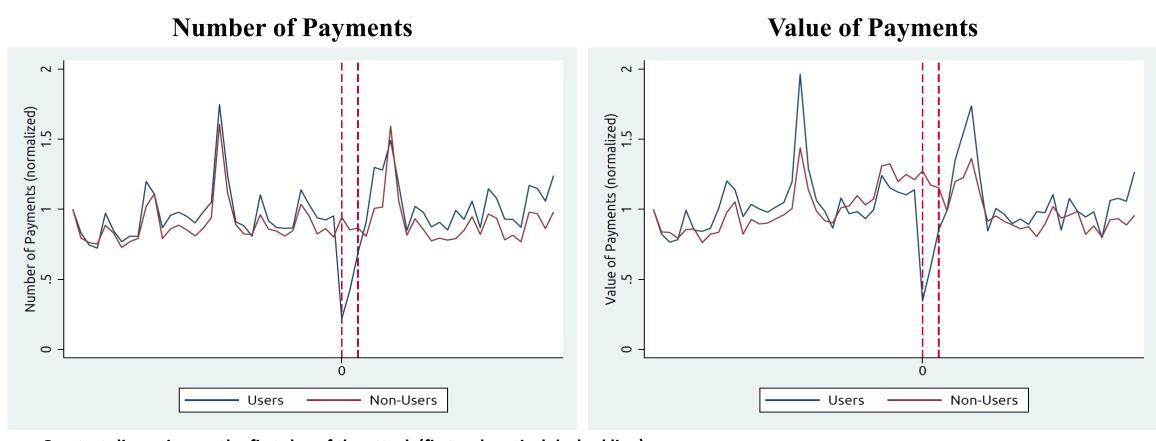
#### This paper:

Studies an actual multi-day cyberattack, that is representative of many others in the nature of the attack, on a major technology service provider (TSP) -> given the size and scale of operations of the TSP, potentially a financial stability event

#### Background

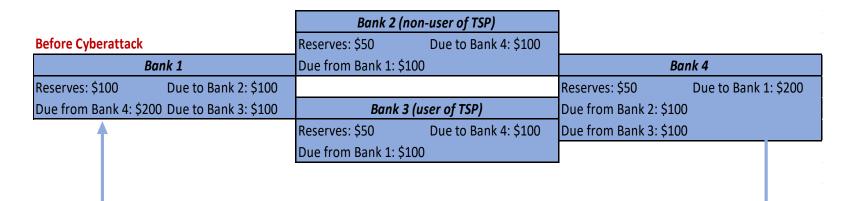
- The TSP discovered evidence of an attack on its computer network and disconnected from the internet to contain it
- Treatment group (users of the TSP): banks relying on the TSP to send payments over Fedwire
- Control group (non-users of the TSP): banks not reliant on the TSP to send payments over Fedwire
- We study the financial stability effects of attack and contagion through the payment system, a common transmission channel for stress in the financial system
  - E.g., Afonso, Kovner, and Schoar, 2011; Afonso and Shin, 2011; Afonso and Lagos, 2015

#### Users sent fewer payments than non-users



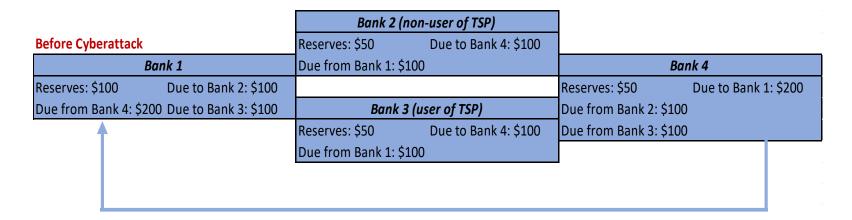
- Greatest disruption on the first day of the attack (first red vertical dashed line)
- Improvement the next days as banks switched to alternative methods in sending payments and TSP gradually restored services
- Similar trends before and after the cyberattack

## Conceptual framework



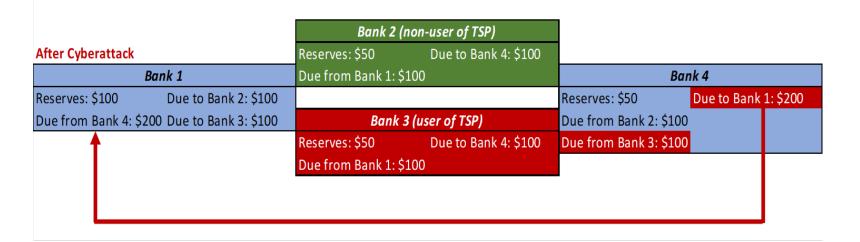
Direct network connection:
bank → TSP → Fedwire (FedLine Direct)

## Conceptual framework

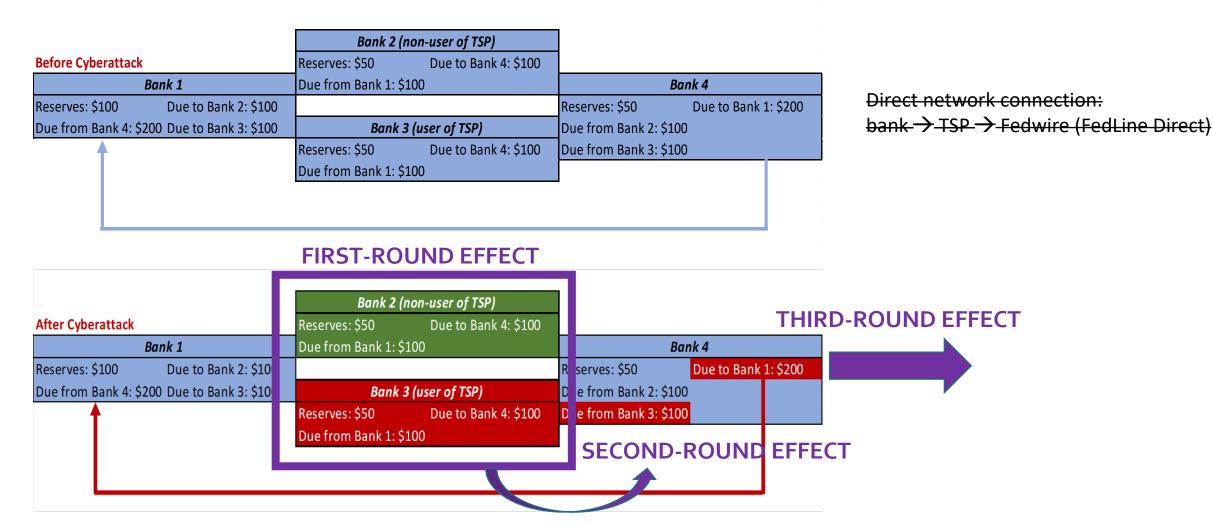


Direct network connection:

bank → TSP → Fedwire (FedLine Direct)

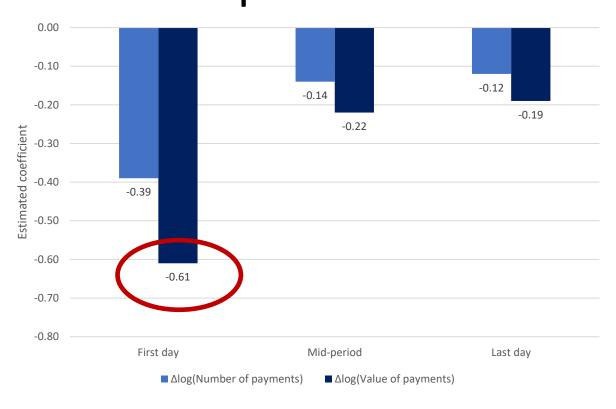


## Conceptual framework



# First-round effect

# First-round effect – including responses by the official and private sectors



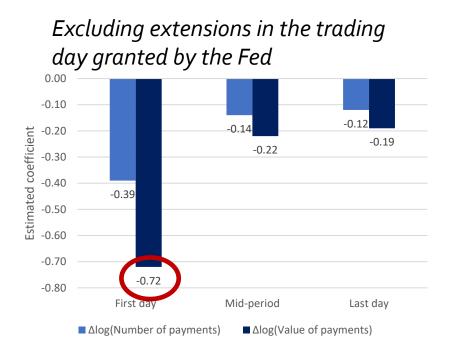
 What share of all Fedwire payments would have been lost had zero payments gone through?

-> **0.7**% = 0.7% (share of users' value of payments) \* 1

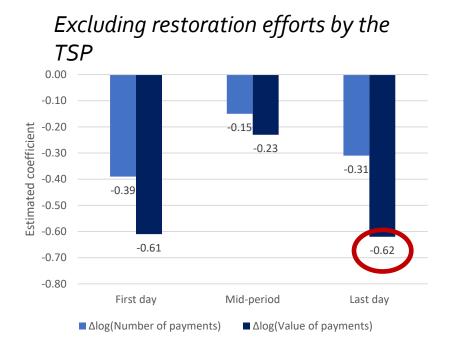
 Responses by the official and private sectors cut this effect almost by half

-> 0.42% = 0.7% (share of users' value of payments) \* 0.61

# First-round effect – excluding responses by the official and private sectors



-> 0.5% = 0.7% (share of users' value of payments) \* 0.72



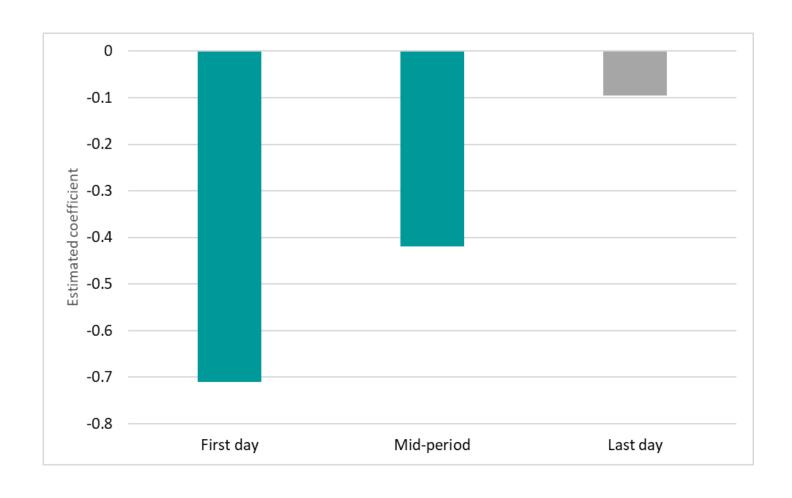
-> 0.43% = 0.7% (share of users' value of payments) \* 0.62

#### Second- and third-round effects

#### Second-round effect: contagion to receiver-banks

- If there is a second-round effect, it is on receiver-banks that were non-users of the TSP themselves. We ask:
  - Was there a drop in payments non-users received? (second-round effect)
  - If so, how did they respond? Did they send fewer payments themselves? (third-round effect)

#### Incoming payments of receiver-banks dropped



- Especially on the first day
- The drop was less severe on subsequent days

#### How did receiver-banks address the liquidity shortfall?

- Small receiver-banks were more likely to borrow from the discount window
  - ...especially those with no alternative sources of funding (FF=0)
  - ...especially those with relatively fewer reserves
- For large receiver-banks:
  - The larger ones with more reserves relied on those reserves, especially on the first day
  - The rest of the large receiver-banks increased fed funds borrowing
    - ...especially those with relatively fewer reserves
- → These responses were sufficient to avoid a third-round effect (i.e. no drop in these banks' outgoing payments) and broader financial instability

#### Policy lessons

- Official and private sectors' responses matter
  - Bank users switched to alternative methods in sending payments, which allowed them to send payments after business hours using Fed's extension of the trading day
  - However, they did not switch to them quickly enough to avoid contagion
  - As a result, bank non-users had a material drop in payments received
  - Restoration of services by the TSP helped mitigate some of the effects
- Liquidity buffers matter
  - Banks non-users with sufficient reserves could use those reserves to send their own payments
  - Those without sufficient reserves borrowed funds
- Federal Reserve support matters
  - Fed's traditional tools are effective in mitigating the impact of non-traditional shocks, such as cyberattacks
  - Extending time mitigated the first-round effect
  - Extending liquidity mitigated the second-round effect

Thank you!