Cyberattacks and Financial Stability: Evidence from a Natural Experiment

Antonis Kotidis and Stacey Schreft

Federal Reserve Bank of Cleveland and Office of Financial Research (OFR)
Financial Stability: Frontier Risks, a New Normal, and Policy Challenges
November 17-18, 2022

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)
- *Academics* 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)
- *Industry participants* 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)

Cyberattacks and the financial system

However, the financial system has yet to experience a cyberattack with systemic consequences

- Considerable preparation and contingency planning for a cyberattack by government and financial institutions

- Financial institutions frequently rehearse responses to cyberattack scenarios and highlight their contingency planning to provide continuity in the sector in the wake of a cyberattack (e.g., Hearing at the House Committee on Financial Services, 2015)

Cyberattacks and the financial system

How well might these contingency plans work in practice? Difficult to gauge their importance, because one needs:

1. An actual cyber event with potential financial stability effects
   - Most known events are hours-long events with no implications for financial stability

2. Ability to identify who was impacted and, as a result, forced to use contingency plans
   - Confidential Supervisory Information

3. Access to high-frequency data
   - Data within and across days to capture the effect of the common shock, contagion to the rest of the financial system as well as the effect of mitigants

Our contribution

We study a unique event with all those features:

A multi-day cyberattack on a major technology service provider (TSP) that serves thousands of financial institutions globally → *given its size and scale of operations, potentially a financial stability event*

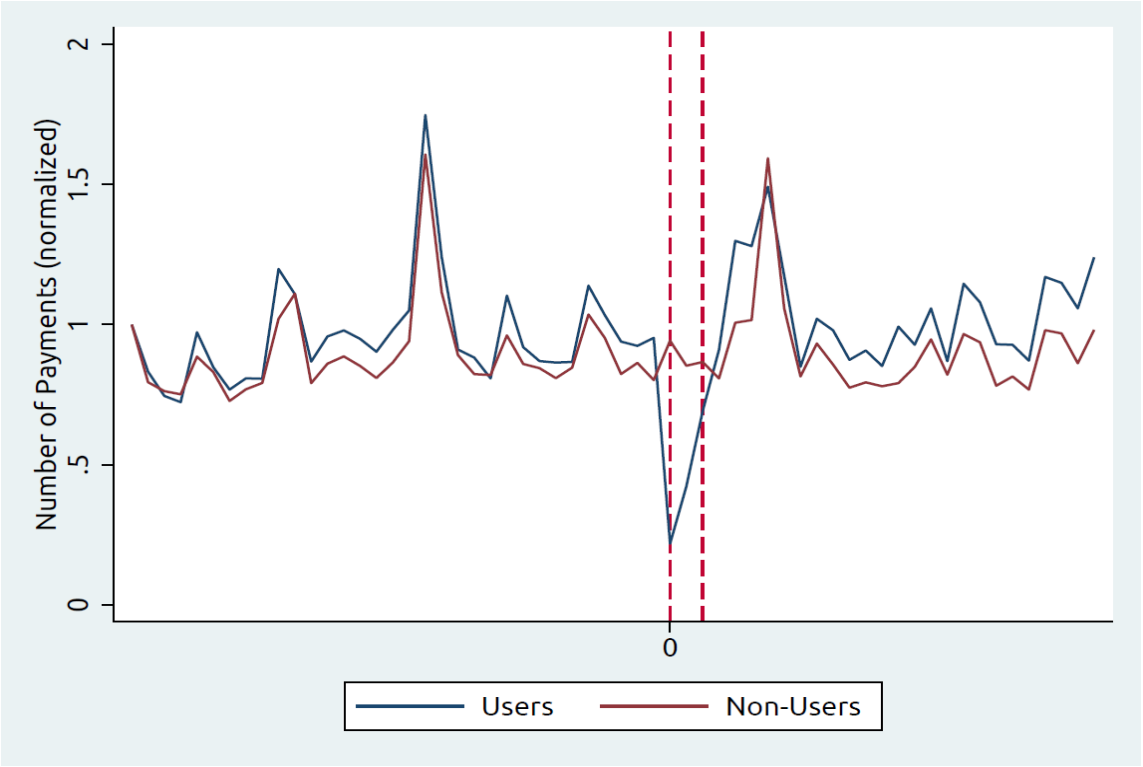
Background

- 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
- Excluding G-SIBs, which were non-users, users were relatively larger than non-users

- 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…

Number of Payments

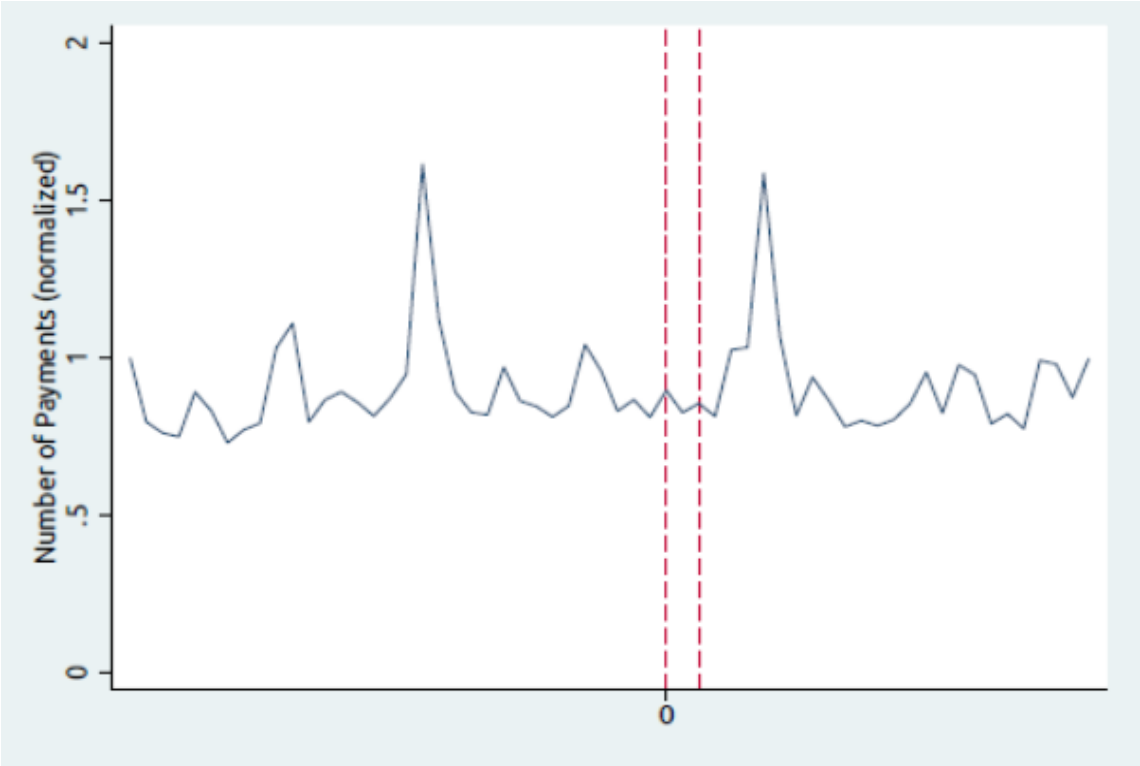


Value of Payments

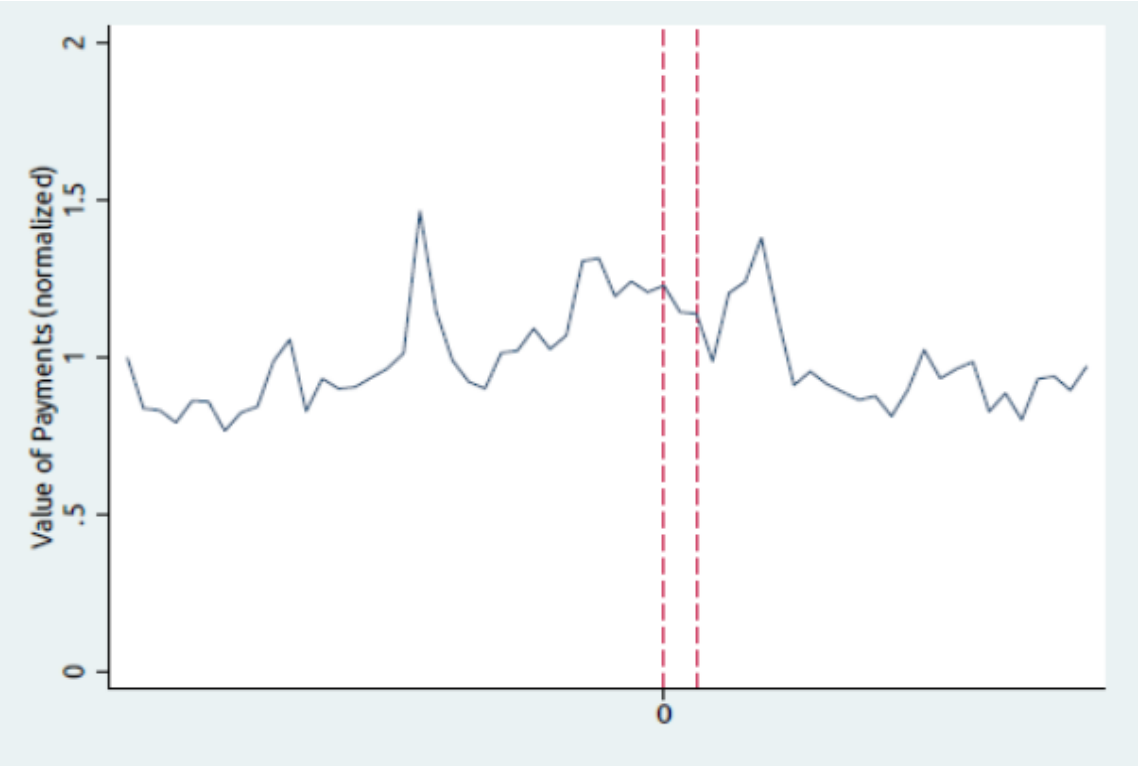
- Greatest disruption on the first day of the attack (first red vertical dashed line)
- Improvement the next days as TSP gradually restored services
- Similar trends before and after the cyberattack

…but no disruption in aggregate!

Number of Payments



Value of Payments



Questions we are ultimately interested in

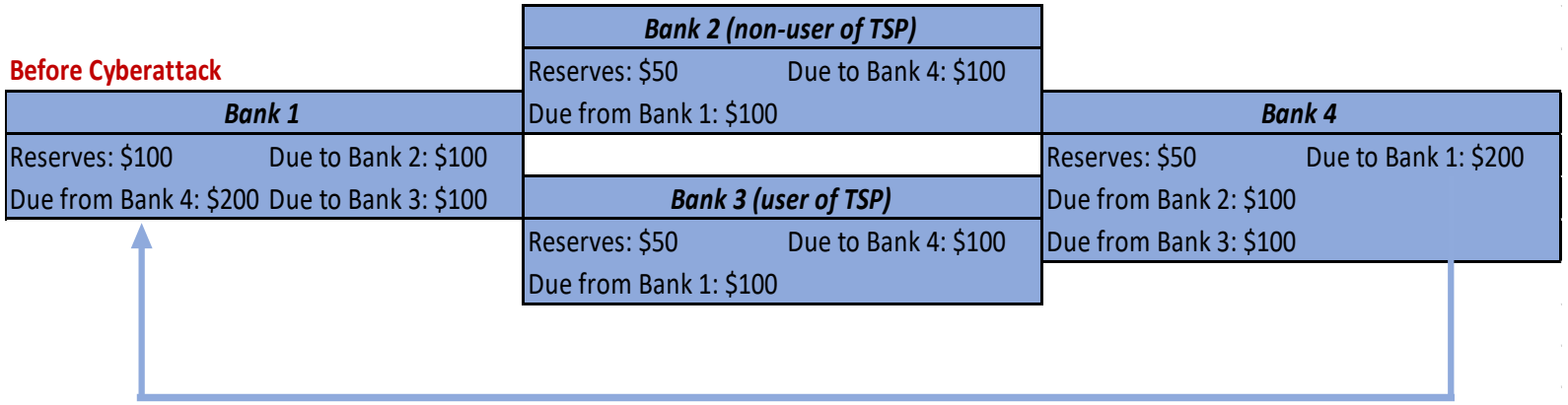
1. Why was there so little effect in the aggregate? Why were there no financial stability effects?

2. Did banks adapt to the shock? If so, how?

3. Did the Fed take steps to mitigate the impact of the cyberattack? If so, what kind of steps?

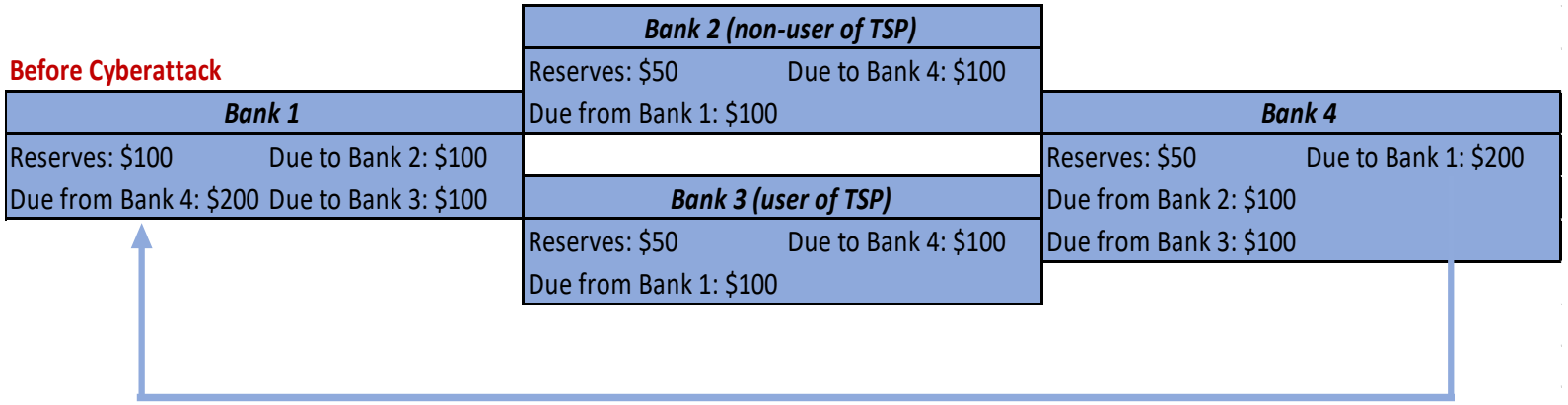
→Important for policymakers to have answers to those questions because it's a matter of "when" a cyberattack hits, not "whether." Need to know what works and what doesn't

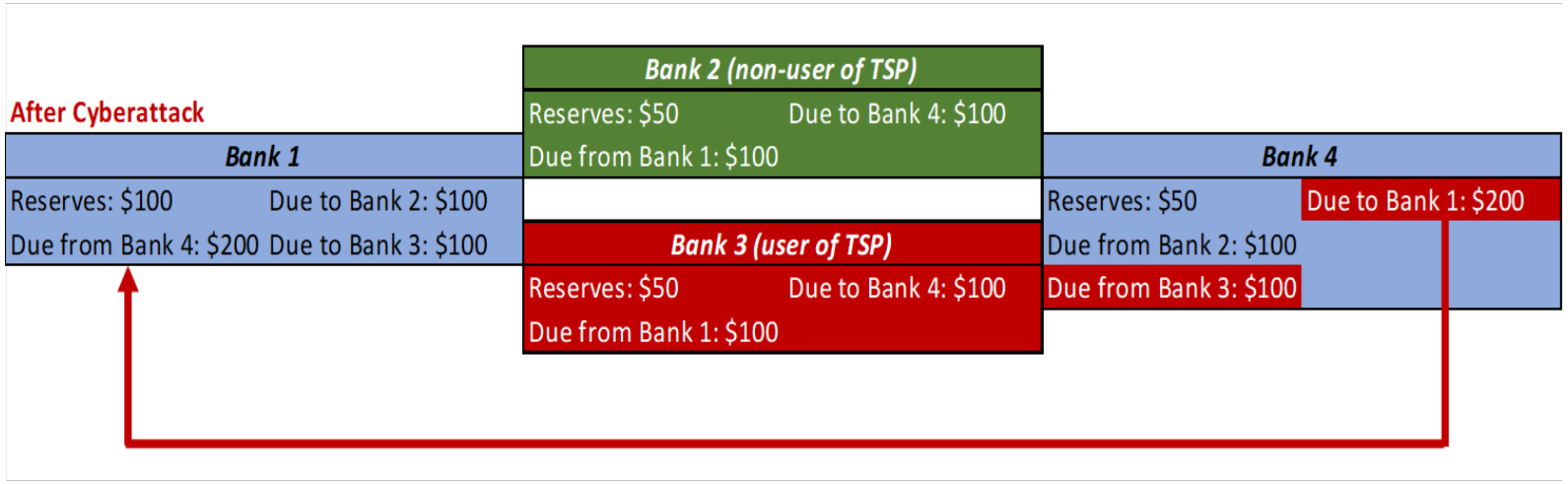
Conceptual framework



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

Conceptual framework



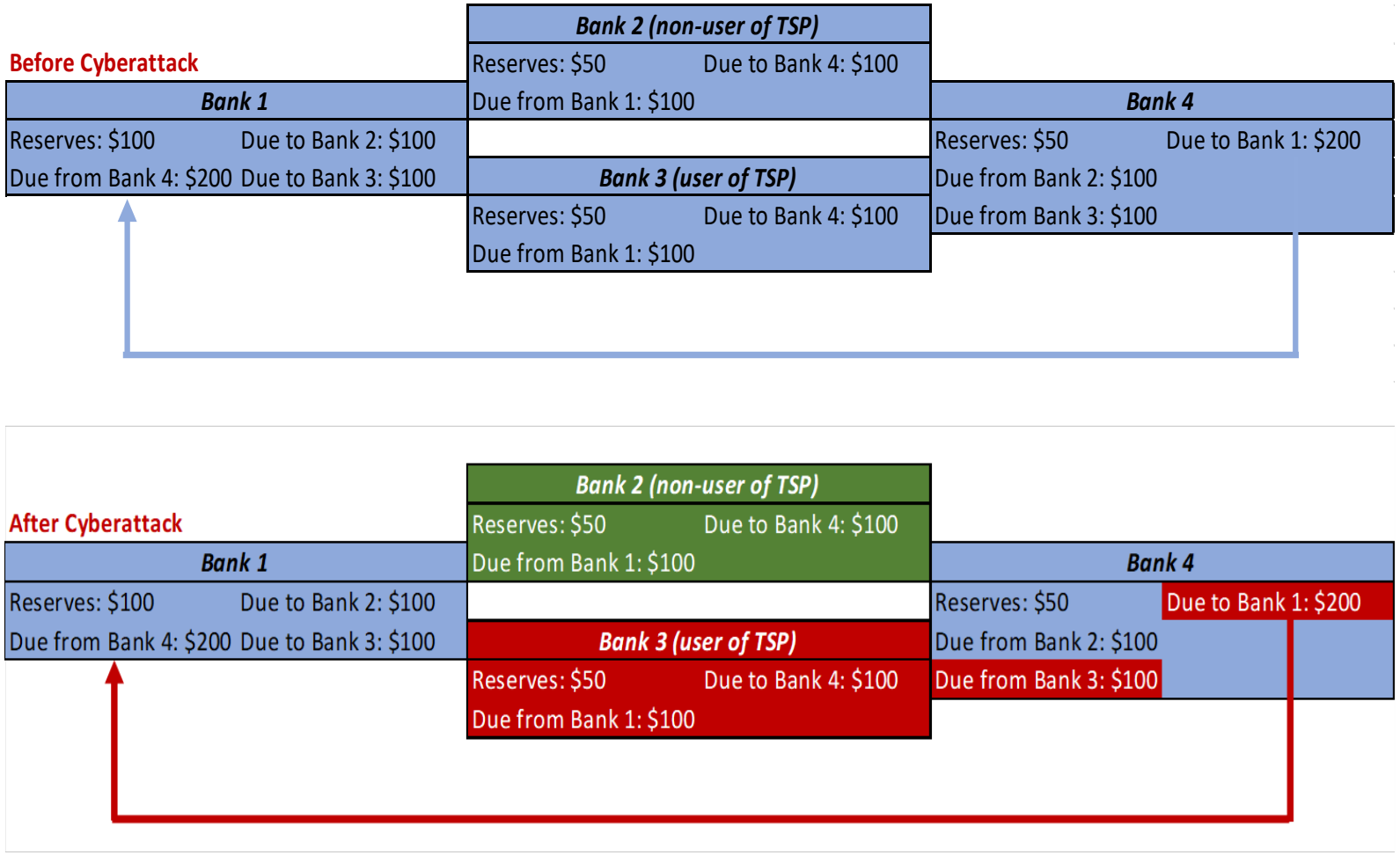


~~Direct network connection:~~
~~bank → TSP → Fedwire (FedLine Direct)~~

Contingency plans

1. Upload an Excel file with information to send payments (FedLine Advantage) – a partly manual process
2. By phone – Bank staff call Fedwire staff with the information to send payments; FR banks allow 3 transactions per call

Conceptual framework



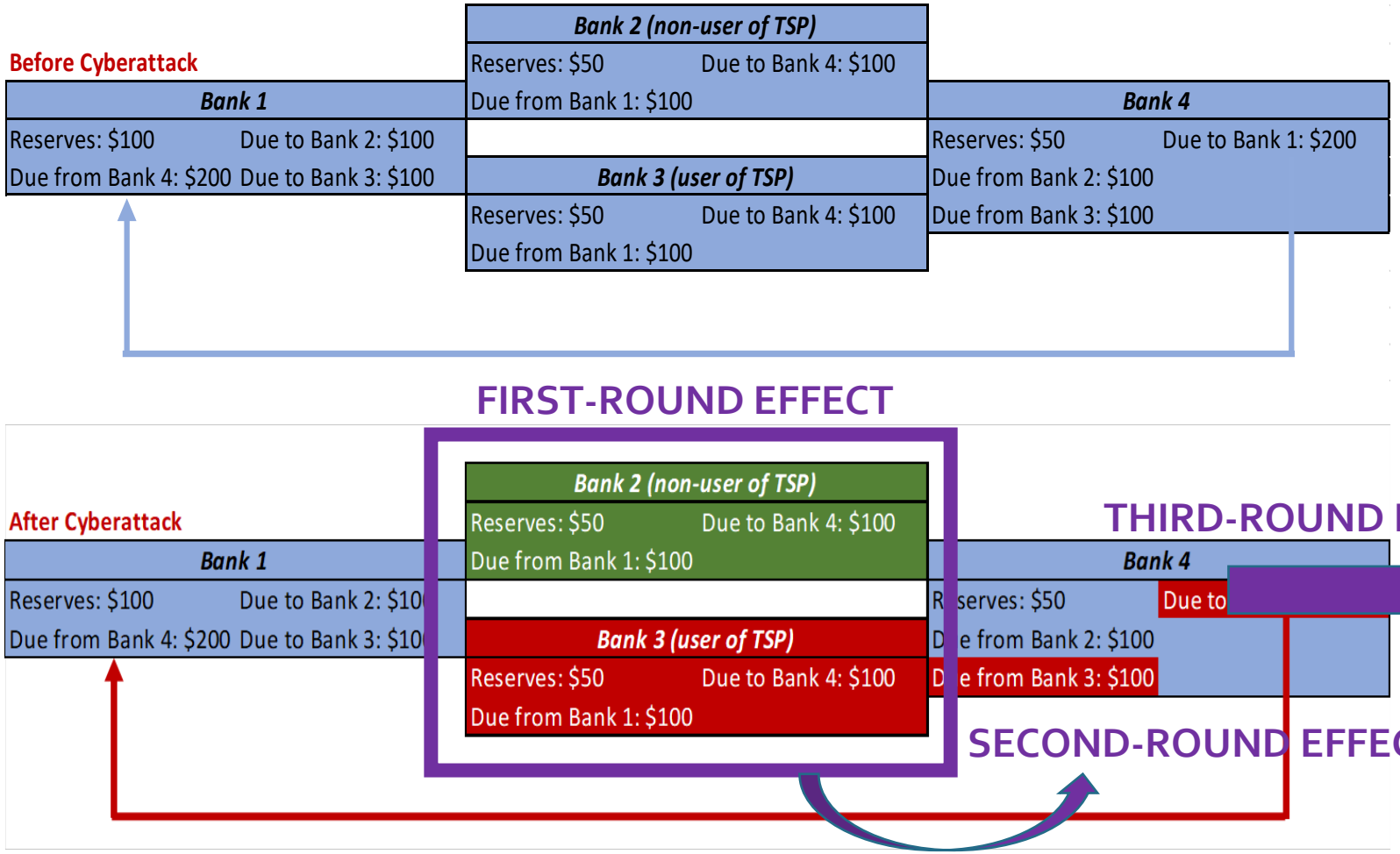
~~Direct network connection:~~
~~bank → TSP → Fedwire (FedLine Direct)~~

Contingency plans

1. Upload an Excel file with information to send payments (FedLine Advantage) – a partly manual process
2. By phone – Bank staff call Fedwire staff with the information to send payments; FR banks allow 3 transactions per call

- **In contingency situations, the Fed recommends banks *"prioritize transactions to those that the institution has identified as the most critical, particularly later in the business day"***

Conceptual framework



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

Contingency plans

1. Upload an Excel file with information to send payments (FedLine Advantage) – a partly manual process
2. By phone – Bank staff call Fedwire staff with the information to send payments; FR banks allow 3 transactions per call

- **In contingency situations, the Fed recommends banks *"prioritize transactions to those that the institution has identified as the most critical, particularly later in the business day"***

First-round effect

Empirical model

$$\Delta Log(Value/Number\ of Payments)_{srt} = \beta_1 \times Users_{\ s} \times First - Day_t + \beta_2 \times Users_{\ s} \times Mid - Day_t + \beta_3 \times Users_{\ s} \times Last - Day_t + FE + \varepsilon_{srt},$$

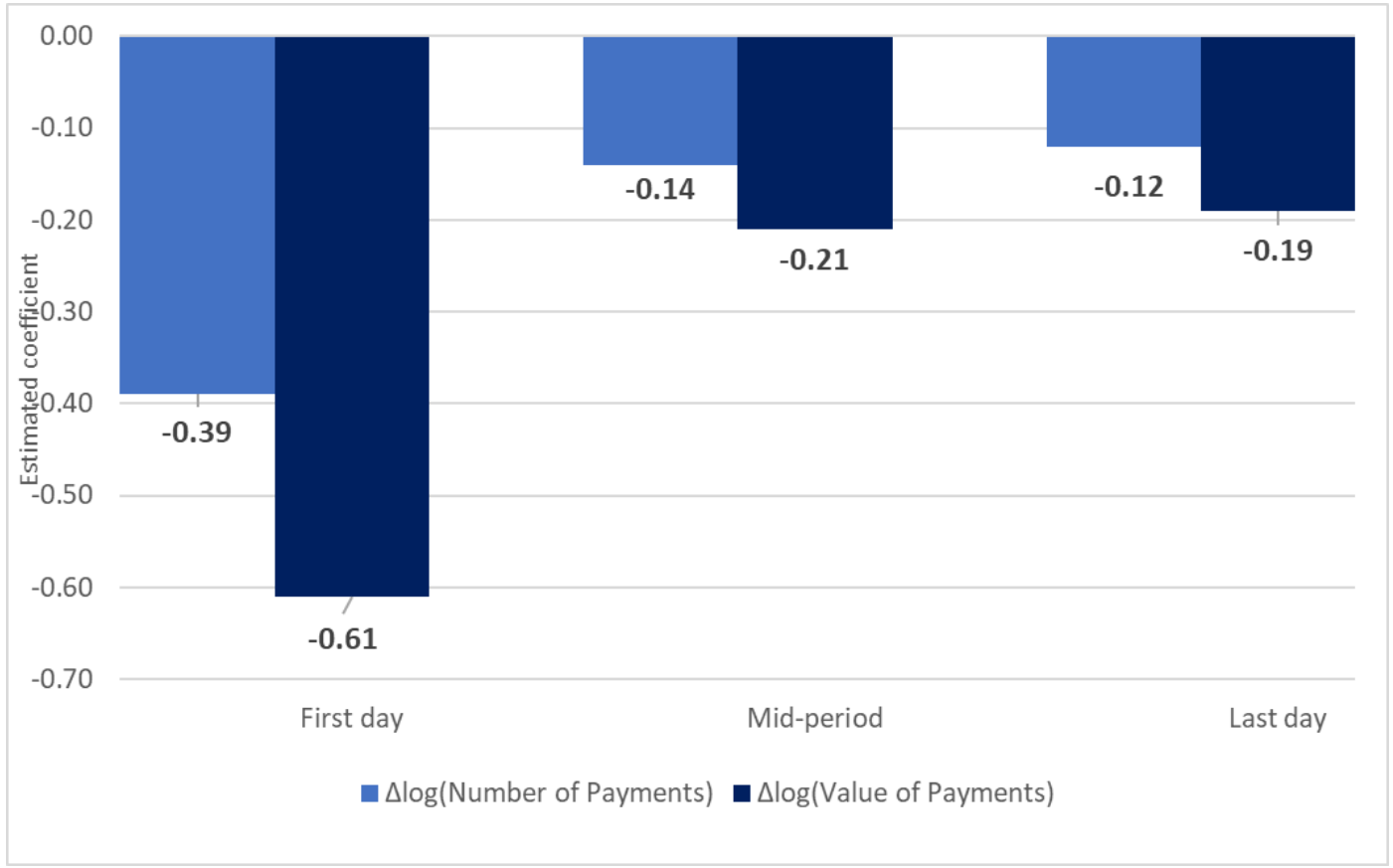
- Fedwire payments are initiated by the sender, so first-round effect is on a user bank's ability to send payments

- Variables of interest: the change in the number and value of payments compared with the same day a week before to account for seasonality in payment flows (e.g., Treasury settlement days)
  - Aggregate Fedwire's transaction-level data at the sender-bank–receiver-bank–day level:
  - (i) count the number of transactions for each pair of banks on each day
  - (ii) take the sum of the value of all transactions for each pair on each day

- *Users* is a dummy variable that takes value one if a sender-bank was a user and is zero otherwise. *First-/Mid-/Last-Day* are dummy variables that take value one on the first-/mid-/last-day respectively, zero otherwise.

- Conservative standard errors double-clustered at the sender and day level
  - #clusters > 50 in both dimensions – errors not biased downwards

First-round effect – with contingency plans



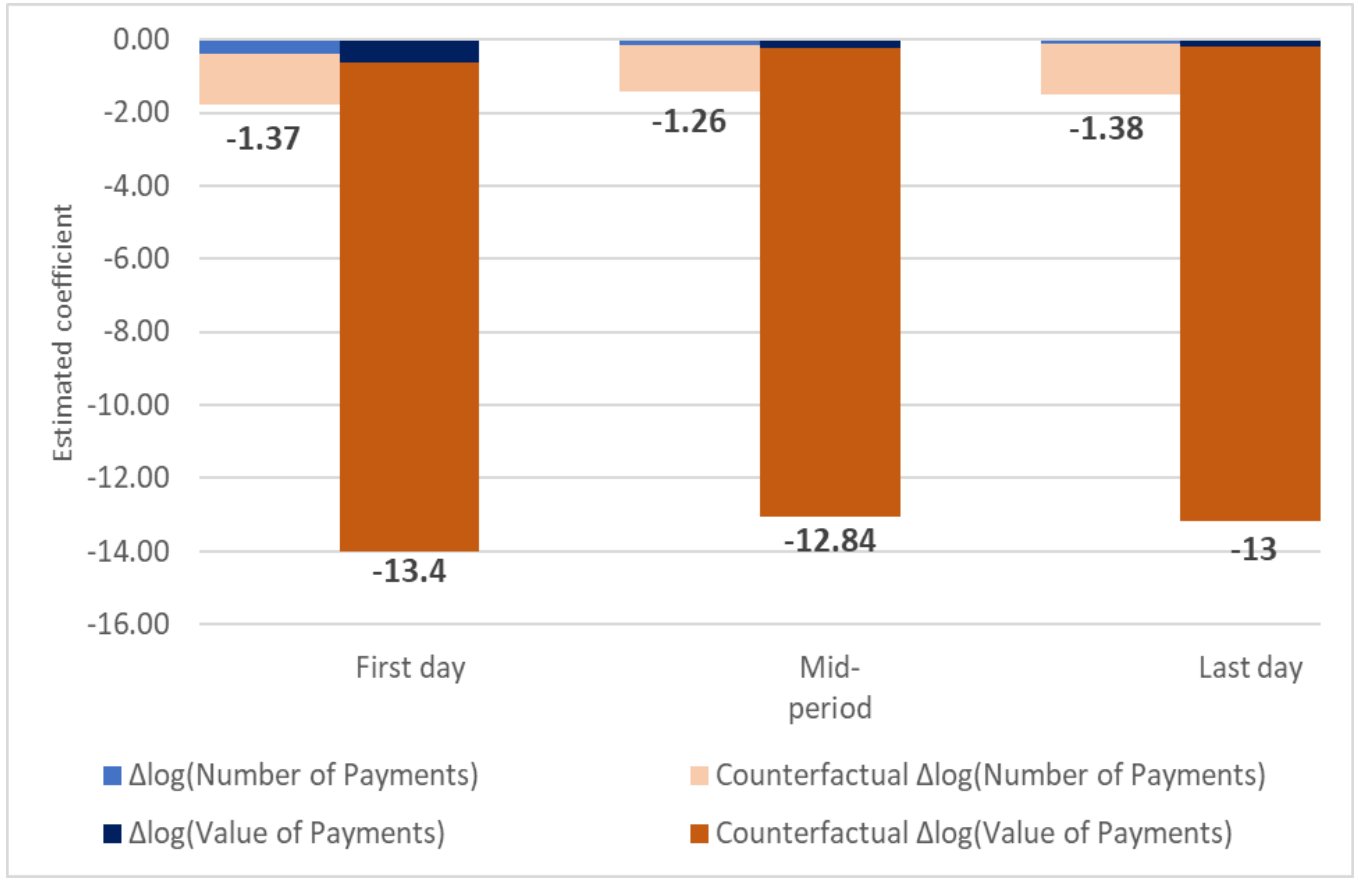
- Bank users (i.e., bank 3) of the TSP sent fewer Fedwire payments

- **Economic significance on first day: what share of all Fedwire payments was lost due to cyberattack?**

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

- **Why is the effect so small?** Did banks switch to alternative methods in sending payments?

First-round effect – without contingency plans



- Since it is unobservable how banks switched, we assume users sent zero payments
  - Same case as if cyberattack had hit banks directly

- **Economic significance of the counterfactual**

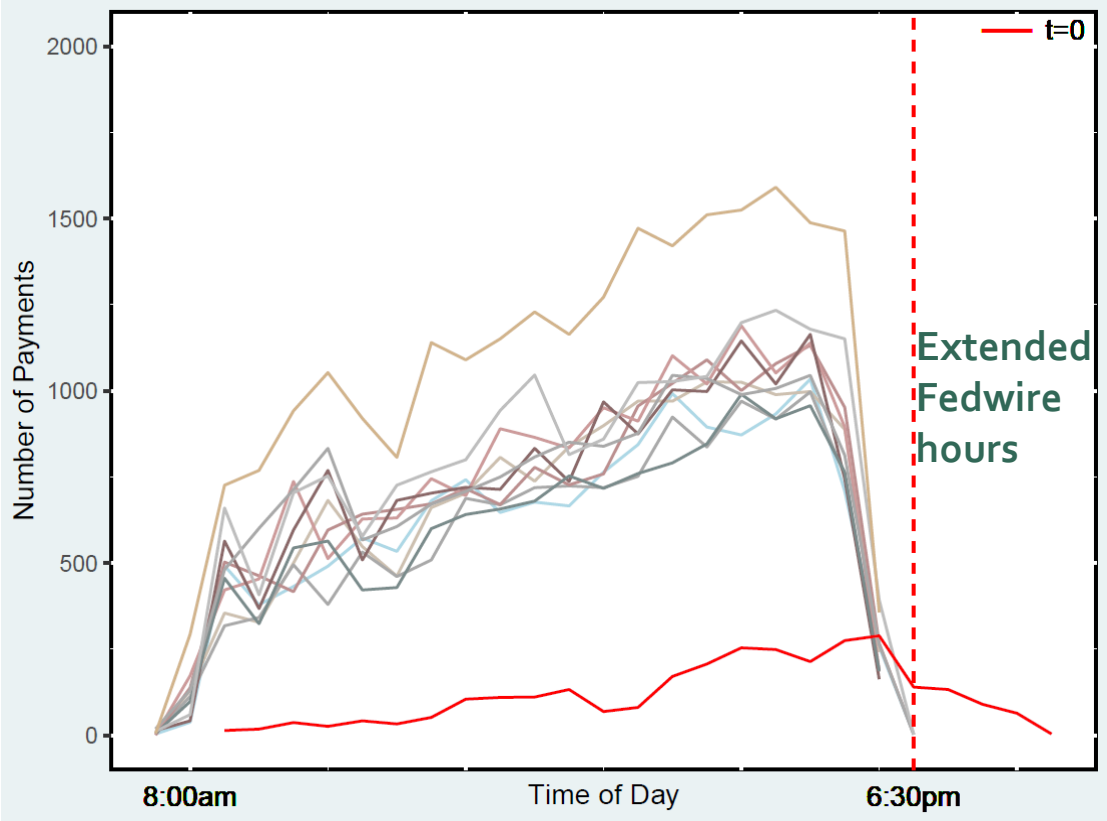
-> 9.4% = 0.7% (share of users' value of payments) * 13.4

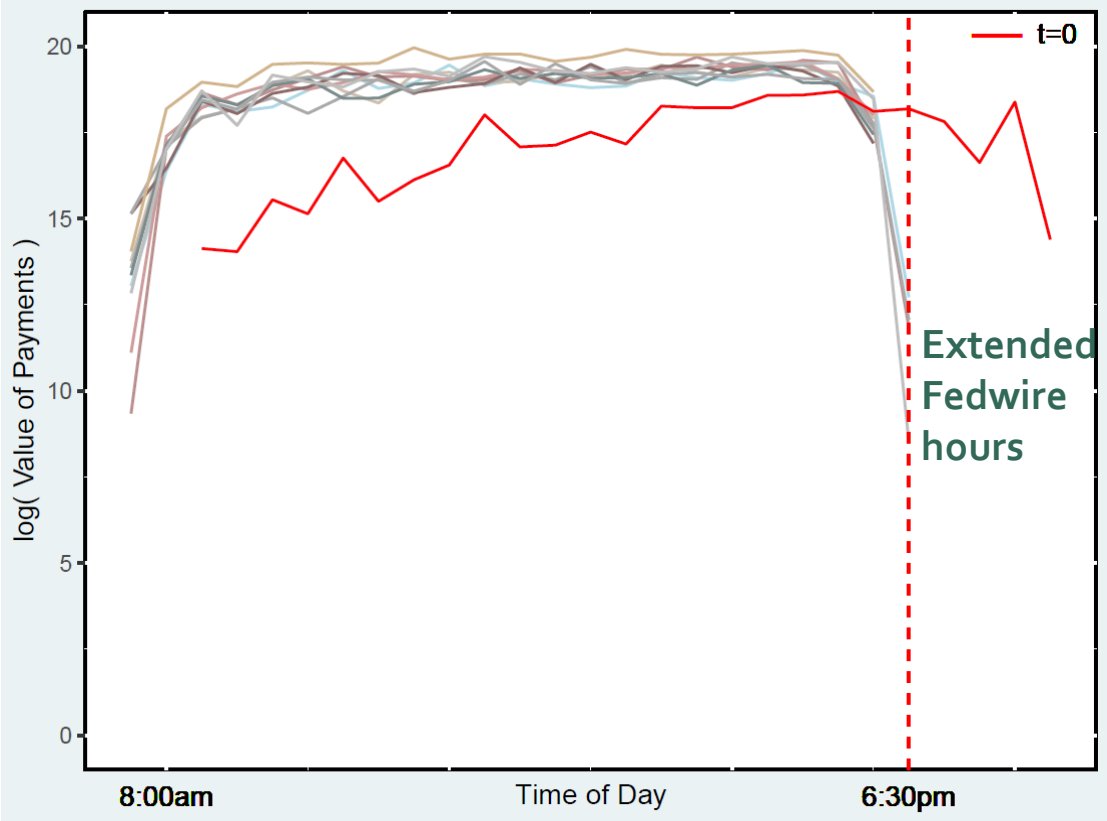
- **Is this a big effect?**

Yes, it's **1/3 of the 9/11 effect**

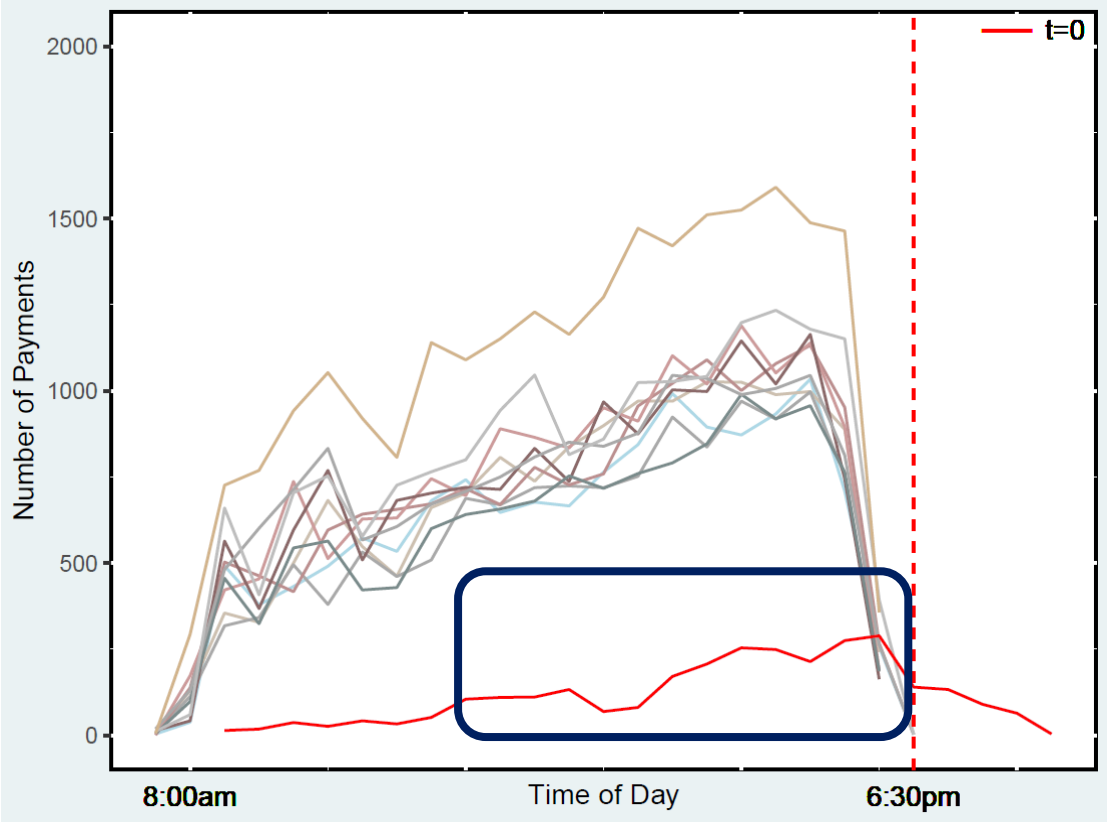
Recall: no GSIBs were directly affected by the cyberattack

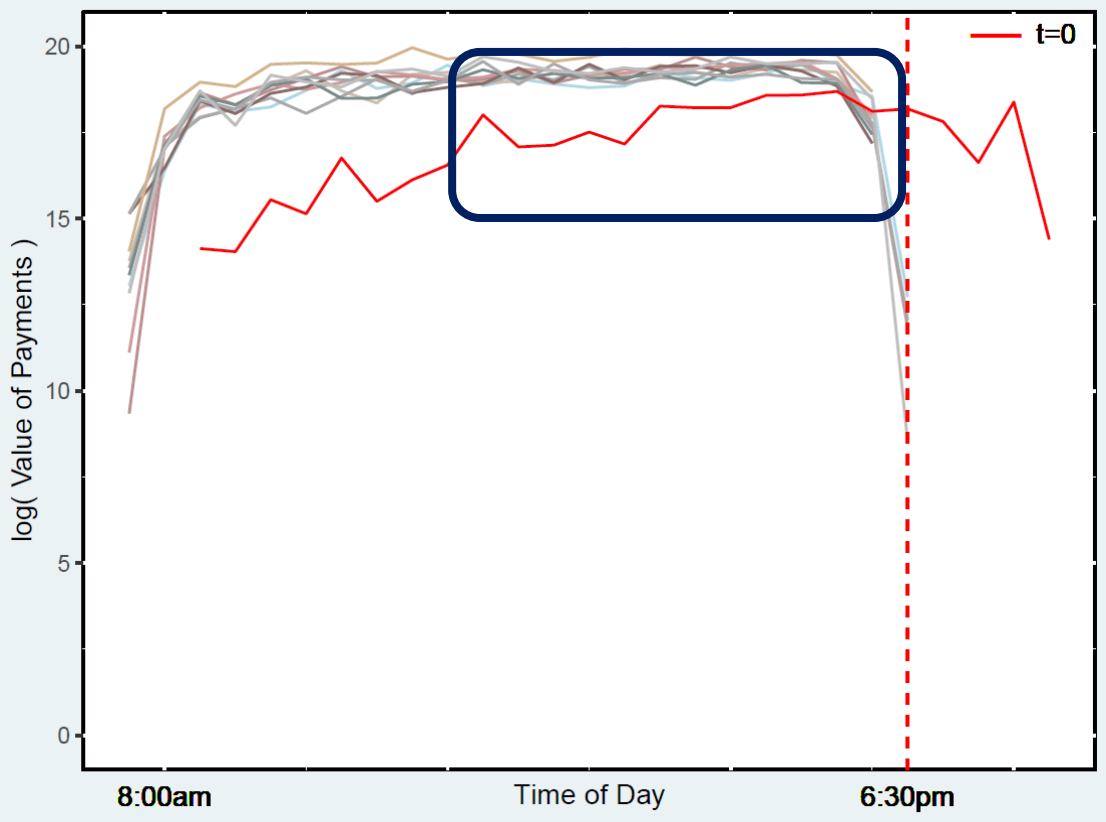
Given switching, did they prioritize larger payments and use extended Fedwire hours?





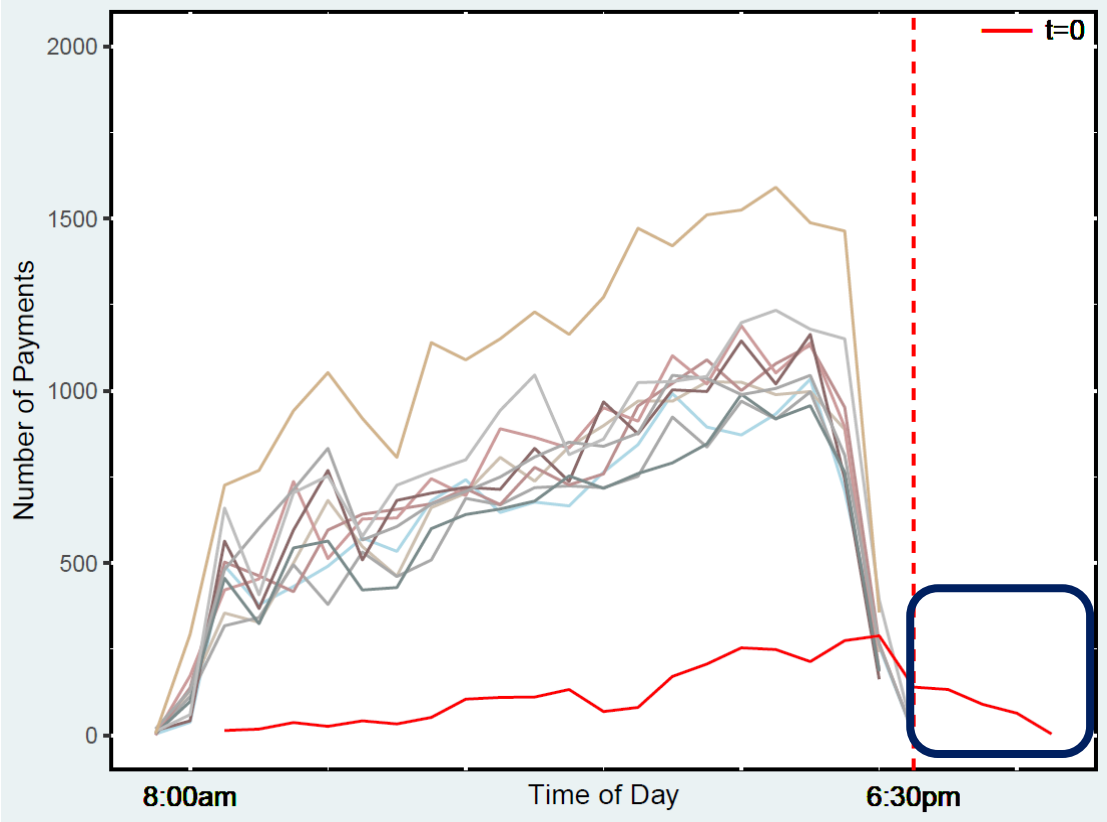
Given switching, did they prioritize larger payments and use extended Fedwire hours?

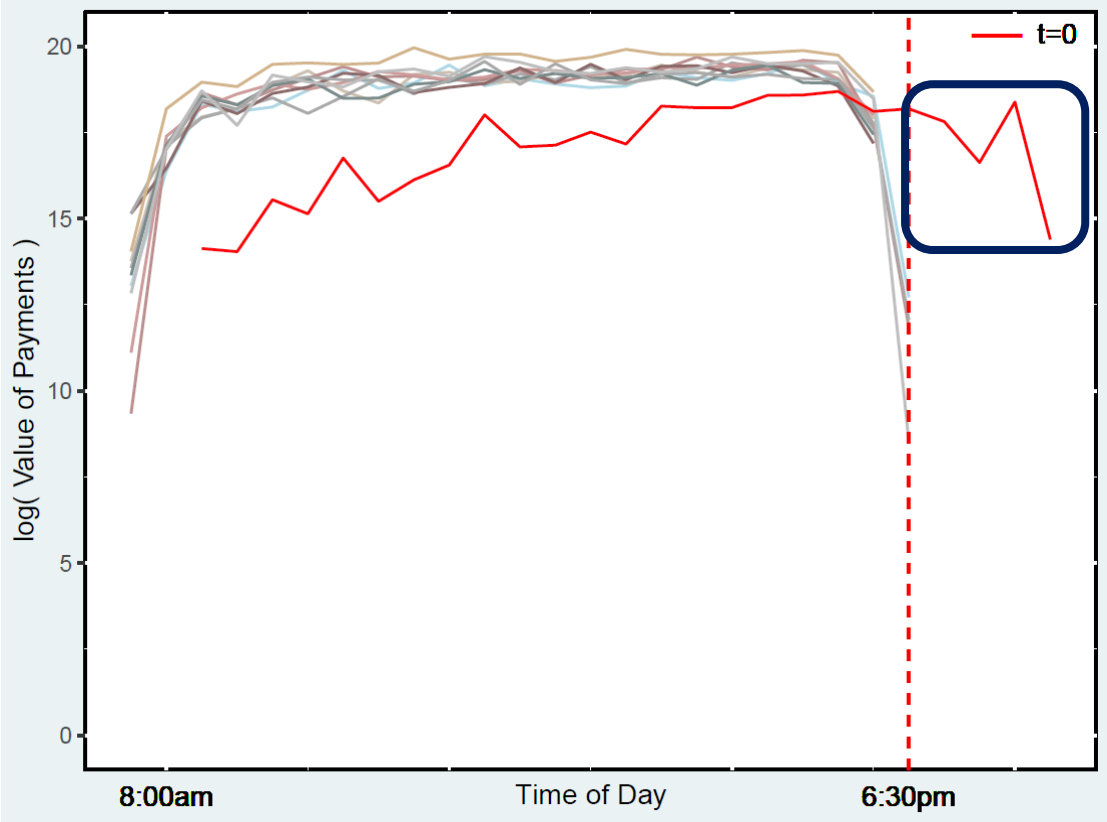




- **On the first day:**
  - the average payment users sent in the afternoon (12pm-6:30pm) was 86% larger compared to the morning

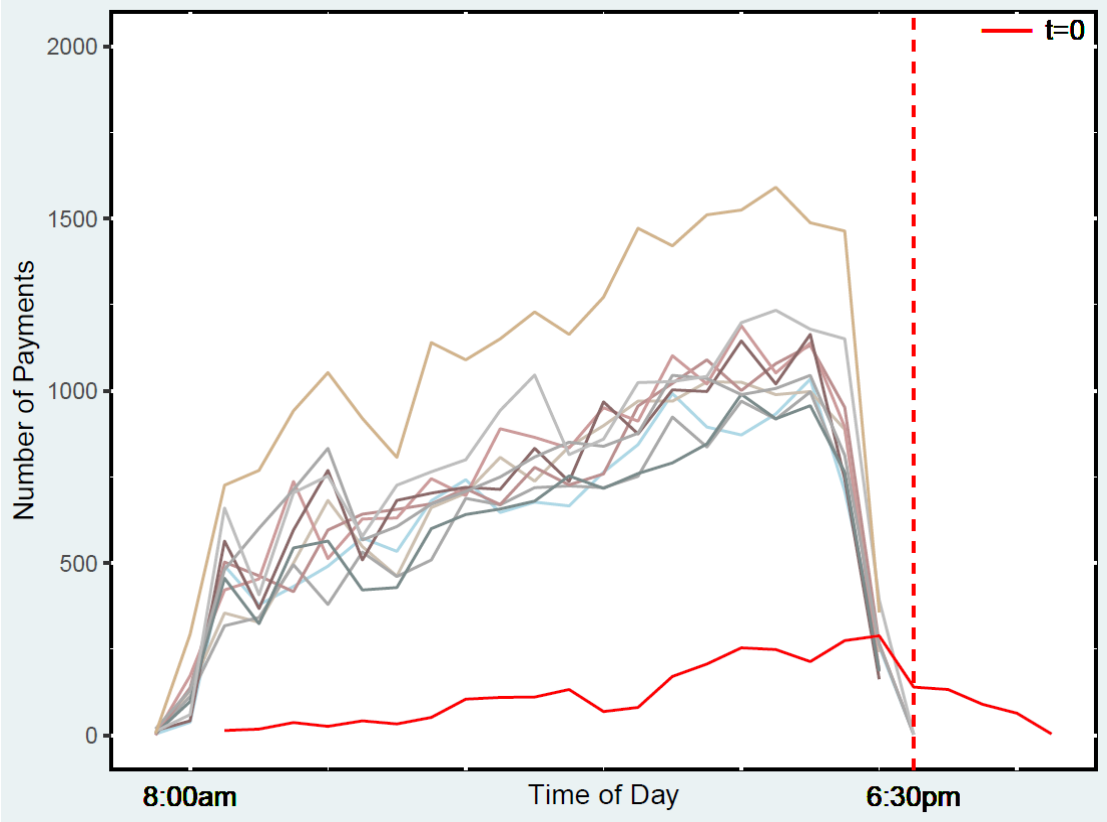
Given switching, did they prioritize larger payments and use extended Fedwire hours?

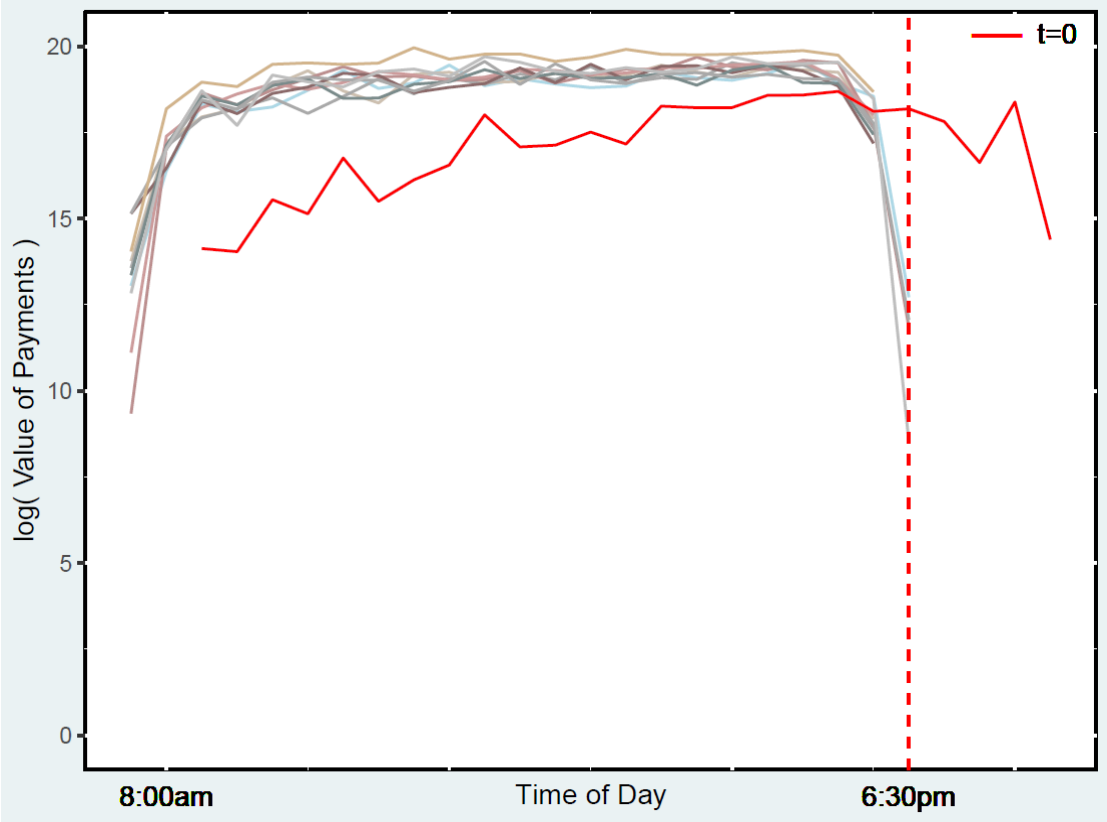




- **On the first day:**
  - the average payment users sent in the afternoon (12pm-6:30pm) was 86% larger compared to the morning
  - the average payment users sent in the evening (after 6:31pm) was 64% larger compared to the morning

Given switching, did they prioritize larger payments and use extended Fedwire hours?





- **On the first day:**
  - the average payment users sent in the afternoon (12pm-6:30pm) was 86% larger compared to the morning
  - the average payment users sent in the evening (after 6:31pm) was 64% larger compared to the morning
- **No intra-day trends before or after the cyberattack**

Second- and third-round effects

Second-round effect: contagion to receiver-banks

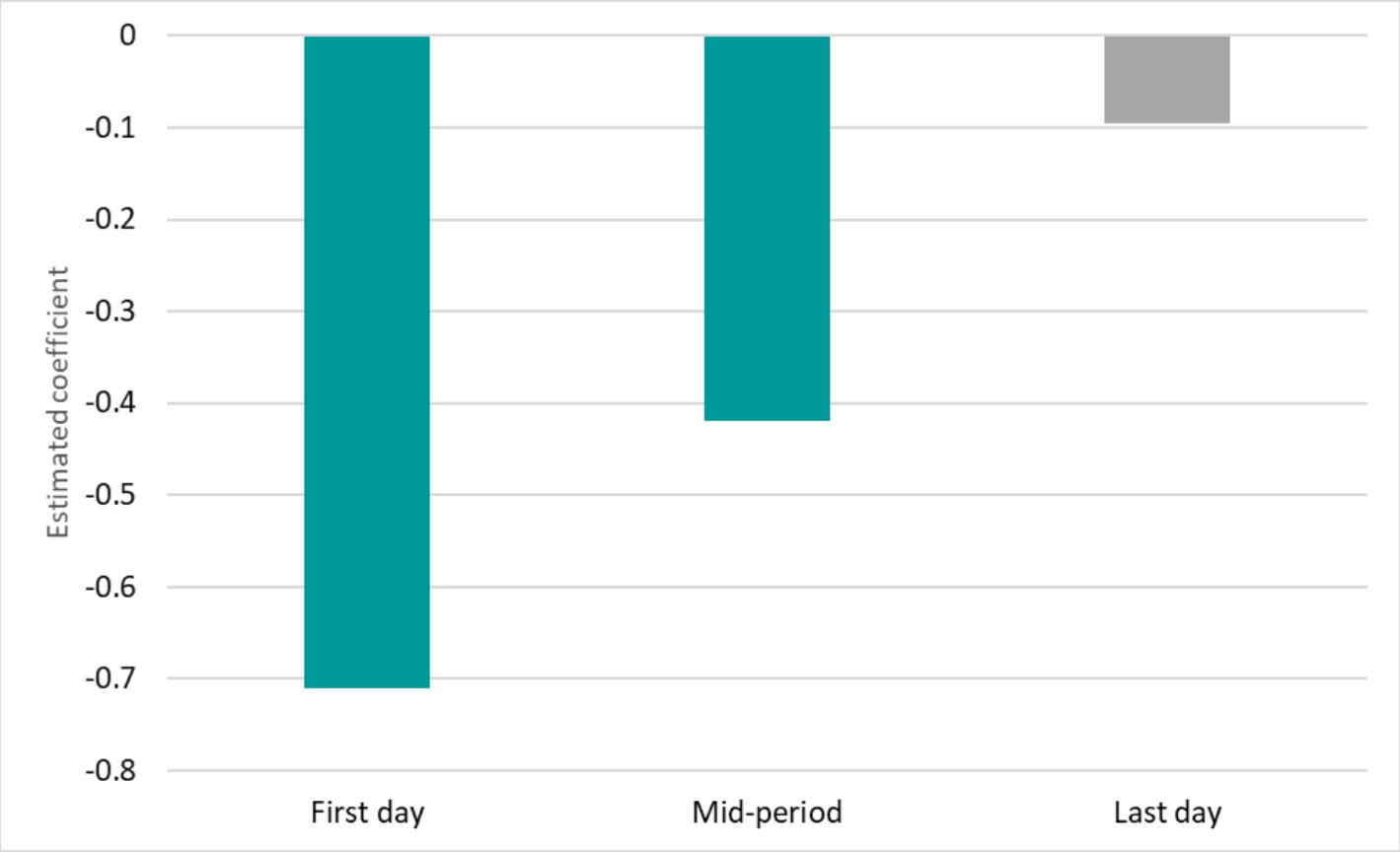
- If there is a second-round effect, it is on receiver-banks that were non-users of the TSP themselves. We ask:
  - Was there a drop in payments non-users received? *(second-round effect)*
  - If so, how did they respond? Did they send fewer payments themselves? *(third-round effect)*

Was there a drop in payments receiver-banks received?

$$\Delta \log(Payments)_{rt} = \beta_1 \times exposed\ receiver - bank_r \times Day\ Dummies_t + FE + \varepsilon_{rt}.$$

- "Exposed receiver-bank": the weighted average of a receiver bank's incoming payments from sender-banks before the attack; the weights are the share of a receiver-bank's total incoming payments sent by sender-banks, with user-senders' payments weighted by one and non-user-senders' payments weighted by zero
  - E.g., assume total incoming payments of $100 over a two-month window before the cyberattack, of which $20 was from user sender-banks and $80 was from non-user sender-banks. The exposure to the shock of the receiver-bank would be 20% (= 0.2*1 + 0.8*0)

Incoming payments of receiver-banks dropped

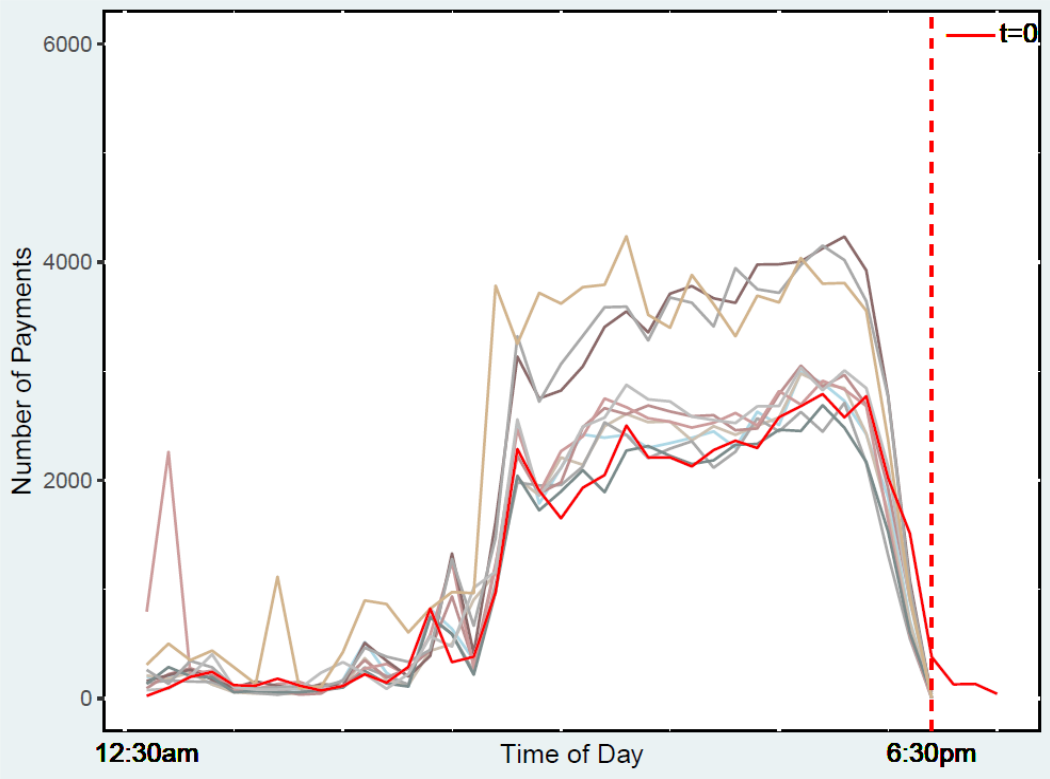


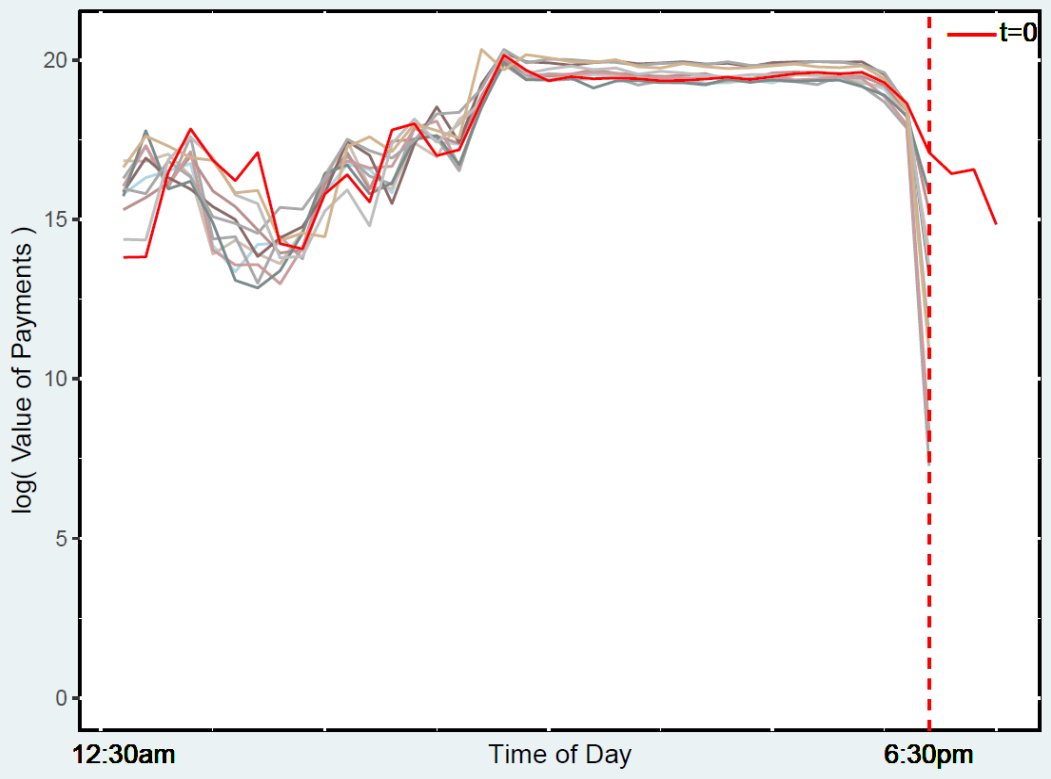
- **First-Day:** a one standard deviation (0.185) increase in the exposure of receiver-banks was associated with a decrease in incoming payments of 13%

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
- All responses were largest on the first day and smaller thereafter

Third-round effect: outgoing payments of exposed receiver-banks





- **On the first day:**
  - Very similar pattern in number and value of payments compared with “normal” days
  - Exposed receiver-banks exploited the extension of the trading day
  - No evidence of liquidity hoarding, so no third-round effect or broader financial instability

Policy lessons

- Contingency plans matter
  - Bank users had, and used, contingency plans
  - 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
- 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!