Federal Reserve
Bank of Dallas

Discussion of “Pirates without Borders” & the Cyber Resilience of Banks

Jill Cetina, Vice President

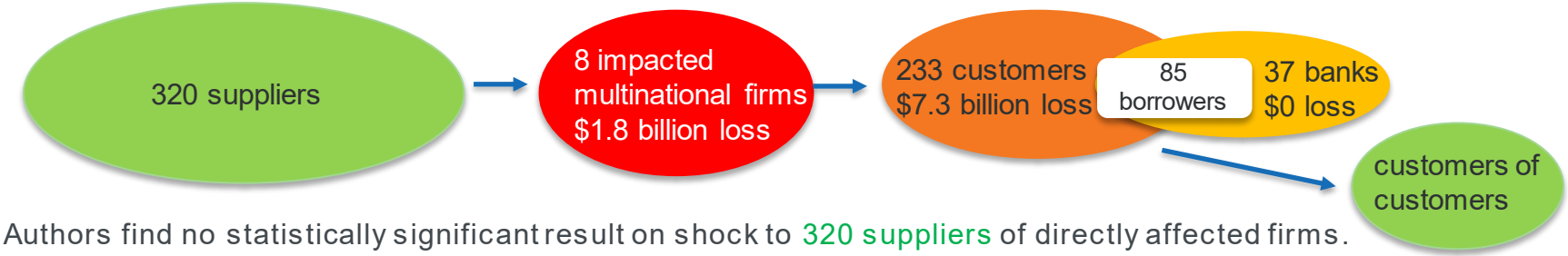
Federal Reserve Stress Testing Conference

October 8, 2021

The views expressed are my own and do not necessarily reflect official positions of the Federal Reserve System.

"Pirates Without Borders" - Overview of Main Characters

- **Natural experiment using an extreme cyber event – Not Petya** (June 27, 2017) - impacts on customers and suppliers of eight large firms directly impacted by NotPetya – extended disruption event.



- Authors find no statistically significant result on shock to 320 suppliers of directly affected firms.

- Authors find large negative and statistically significant downstream profitability impacts to 233 customers of directly impacted firms– but no evidence of further shock propagation (i.e., customers of customers). Additionally, following the NotPetya attack the 233 customers drew down on their internal liquidity and increased external borrowing more than peers who were not in the supply chain.

  - Customers of directly affected firms whose inputs are less substitutable experienced larger effects.

- Authors find 85 affected customers drew down on existing commitments at banks; but didn't obtain new loans.
- Authors find banks charged affected customers higher interest rates and applied higher default probabilities; but no evidence of impact on credit loss, loan maturity or collateral extended to these firms.

"Pirates Without Borders" – More About Banks, Please…

- **Impact of bank exposures to directly effected firms not considered; focus is on customers common to the supply chain and banks.**

- **Post dummy variable specification** for bank lending (Tables 6 & 7) – Q317 to Q418; NotPetya on 6/27/17; should Q217 (6/30/2017) be used?

- **No impact on non-performing loans:** Too strong conclusions drawn about lack of credit loss using six quarters? Paper also notes banks charged higher interest rates, increased their internal probabilities of default for these borrowers and ***"banks' perceptions about higher credit loss."***

- **Impact on bank liquidity:** What was the aggregate and individual size of the liquidity shock to banks from drawdowns both directly impacted firms and customers?

- **Impact on bank capital:** How were banks' regulatory/internal capital measures impacted as exposures and probability of default of these customers increased?

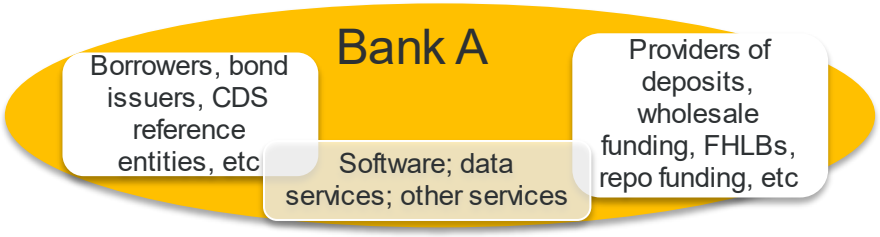
- **Conclusion on no new lending:** Total commitments do not increase; drawdowns of existing commitments only. Could smaller banks outside the Y-14 data set extend new credit?

"Pirates Without Borders" – More about Persistence/Time; First vs Second Round Effects; Directly Impacted Firms

- **Customers**
  - **Post dummy variable specification:** 2017 to 2018; when do customer profitability, liquidity, and leverage effects from the event peak and dissipate? Could you vary the dummy variable specification to gain insight on the time profile of cyber spillovers?
- **Directly effected firms**
  - **Direct losses seem understated:** Paper suggests NotPetya indirect loss 4x direct loss; but $1.8 billion in direct losses seems to be an understatement.
    - For example, Table 1 cites Merck losses of $670 million in 2017; but reports show Merck claims against cyber insurance policy for NotPetya totaled $1.3 billion. Insurer refused to pay citing the policy's war exclusion clause; Merck still remains in litigation with 20 insurers and re-insurers who wrote the policy, incurring further costs.
  - **Long run impacts on directly effected firms:** Could use difference-in-difference set up to estimate long run impacts on profitability, liquidity, and leverage of directly impacted firms relative to peers.

Could Seeing The Problem Differently Help Banks' Cyber Resilience?

- Banks are exposed to loss from a cyber event via **four channels:**



  - **Indirect**
    - **Asset channel:** Cyber attacks on banks' borrowers who were targeted or borrowers who were customers of direct targets
    - **Liability channel:** Cyber attacks on providers of bank funding
    - **Technology channel:** Cyber attacks on banks' own supply chain/service providers
  - **Direct**
    - Cyber attacks on banks

- **Three items for bank cyber resilience agenda:**
  1) development of metrics to incorporate cyber into credit assessment of entities connected to a bank on both the asset and liability sides of the balance sheet;
  2) development of approaches to analyze risks from banks' service provider relationships; and
  3) evaluation of tying banks' own material internal IT control deficiencies more closely to bank capital requirements.