Fraud Exposure and Precautionary Credit Market Behavior

Nathan Blascak
Consumer Finance Institute
Federal Reserve Bank of Philadelphia

Ying Lei Toh
Federal Reserve Bank of Kansas City

System Applied Micro Conference, June 2020

Disclaimer

The views expressed here are solely those of the presenters and not necessarily those of the Federal Reserve Bank of Philadelphia, the Federal Reserve Bank of Kansas City, or the Federal Reserve System.

Introduction

- Large-scale data breaches involving sensitive personally identifiable information (PII) are increasingly common
- These breaches can lead to identity (ID) theft and fraud, which can be costly to victims
- To mitigate the risks of ID theft and fraud, consumers can take precautionary credit market actions:
  - Freeze their credit reports
  - Close down unused accounts
  - Sign up for credit monitoring

Introduction

- In this paper, we examine:
  1. Whether consumers affected by a data breach take precautionary actions in response to the breach, and
  2. How past exposure to fraud (ID theft) or a heightened risk of fraud (data breach) affect their responses.

Introduction

- Prior exposure may affect consumers' responses via learning:
  - Better informed about types of precautionary actions available
  - Practical experience of taking action
- Our hypotheses:
  - Prior ID theft or data breach victims are more likely to take precautionary actions than non-victims.
  - Prior ID theft victims are more likely to take precautionary actions than prior breach victims.
- Test hypotheses in the context of the 2017 Equifax data breach using a standard differences-in-differences (DID) empirical framework

Preview of Results

- Main findings:
- Consumer respond to the news of the breach:
  - increase in the likelihood of having a credit freeze
  - decrease in the number of retail trades held
  - no change in the number of bank cards held
- Previous ID theft victims are more likely to respond to the breach than non-victims
- Previous ID theft victims are more likely to respond than prior breach victims

Background

- Prior research has shown that individuals respond to **data breaches** by freezing their credit reports and/or using credit monitoring (Mikhed and Vogan, 2018)
  - No evidence that individuals changed their credit market behavior
  - Response is short-lived
- Individuals do respond to **identity theft** in credit markets (Blascak et al, 2019)
- Data breach disclosure laws can be effective in reducing identity theft (Romanosky, Telang, Acquisti, 2011)

A Stylized Model of Precautionary Action

- Consumer's decision problem: whether to adopt a protective measure to reduce potential fraud losses in the future.
- Consumer i adopt measure j if

$$p_i L_i > C_{ij} + \epsilon_i$$

  - pi, L_i: perceived probability of fraud and perceived losses from fraud
  - C_{ij}: cost of adopting measure j (monetary + non-monetary)
  - ϵ_i: idiosyncratic cost shock, i.i.d. with mean zero.
- $\Longrightarrow \uparrow p_i$, then consumers will take action

A Stylized Model of Precautionary Action

- "Baseline" scenario (no prior exposure): tendency toward inaction
  - Lack of knowledge or awareness of measures available (Zou et al, 2018)
  - Cost and hassle associated with adopting precautionary measures (Zou et al, 2018)
  - Decision errors due to present-biased preferences and underweighting of fraud risks $\rightarrow$ Status quo bias (Zou et al, 2018; Romanosky et al, 2011).

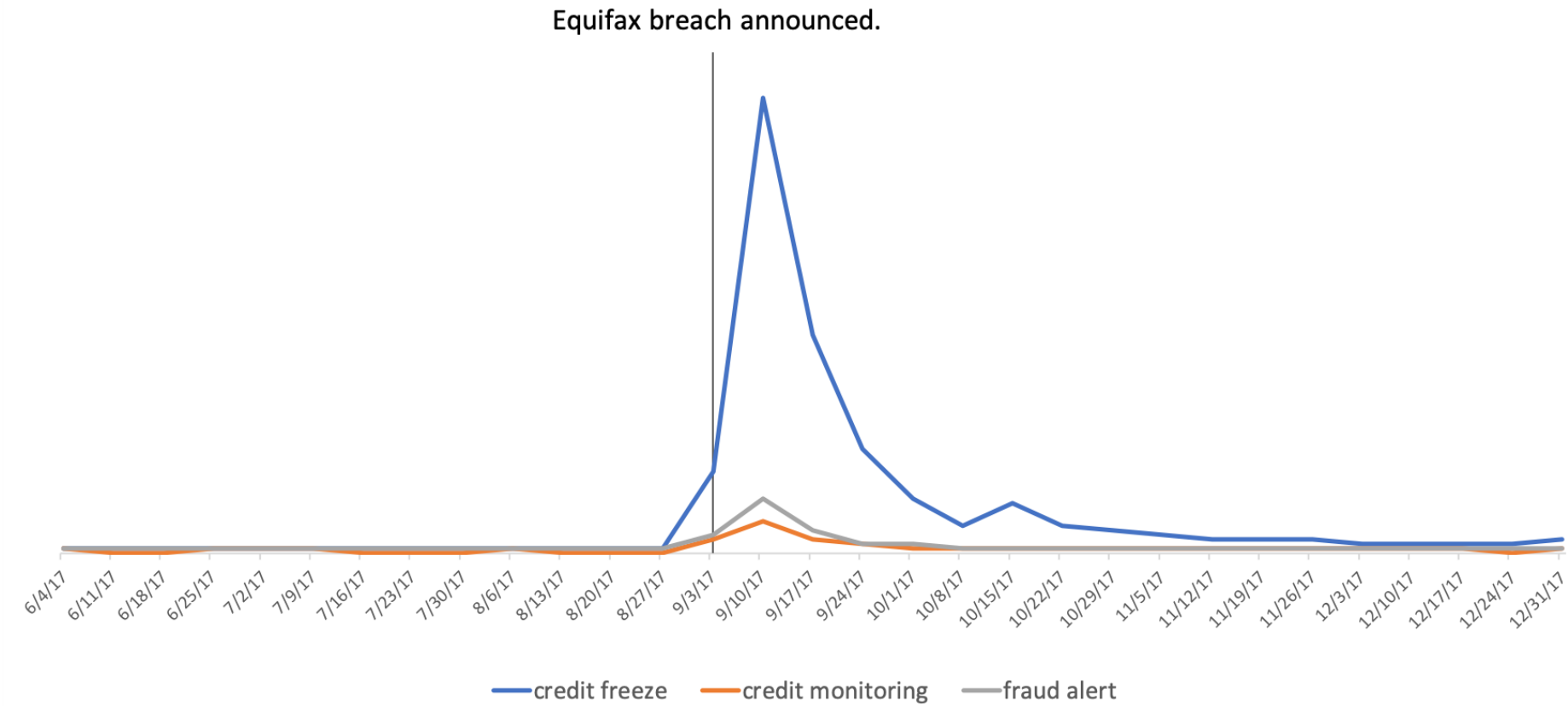
A Stylized Model of Precautionary Action

- Past exposure to fraud or a heightened risk of fraud may affect consumers precautionary behavior by:
  - Increasing their awareness of possible protective measures $\rightarrow$ Lower cost of taking action
  - Reinforcing or counteracting the decision errors via the availability heuristic
- Availability heuristic: assign probability to an event occurring based on how easily instances of such events can be brought to mind.
- Prior fraud exposure $\rightarrow$ Easily think of instances of fraud $\rightarrow$ Overestimate of fraud risks and risk aversion
- Prior exposure to a heightened fraud risks that did not result in fraud $\rightarrow$ Likely to recall the non-occurrence of fraud $\rightarrow$ Further underestimate or neglect fraud risks.

Background: The 2017 Equifax Breach

- Announced on September 7, 2017
- One of the largest and most severe data breaches ever recorded
  - Up to 147 million people affected
  - Information accessed included names, social security numbers (SSNs), birth dates, and home addresses
- Equifax responded by offering free credit monitoring to affected consumers and eventually free credit freezes

Equifax Breach: Did People Respond?



Notes: Authors' calculations using data from Google Trends.

Data

- Federal Reserve Bank of New York/Equifax Consumer Credit Panel (CCP)
  - 5% random sample of quarterly anonymized U.S. consumer credit bureau data
  - 11,848,960 individuals from Q1:2013-Q4:2018
- Merge the CCP will additional data from Equifax on credit freezes and fraud alerts
  - Credit freezes can be placed on a consumer's credit report, restricting access to outside parties
  - Fraud alerts requires businesses to verify a consumer's identity before issuing credit

Data

- Measures of precautionary behavior:
- Credit freezes
- Holding fewer accounts
  - We focus on retail trades
  - More fungible than a bank card

Identifying Prior Victims

- Identify two groups of prior victims:
  1. Prior fraud victims
     - Follow Blascak et al (2019) and use the placement of extended fraud alert flag as a proxy for being a victim of server identity theft
  2. Prior breach victims
     - Identify individuals in living in states that were highly likely exposed to the 2015 Anthem data breach
     - Major data breach where PII of individuals affiliated with Anthem and its subsidiaries were exposed to criminals
     - Exposure to the data breach is geographic
     - We will compare individuals living in IN (most highly exposed state, 68% of residents affected) to individuals in living in IL (1.67% of residents affected)

Empirical Framework

- Estimate the following event study DID regression

$$y_{it} = \alpha_0 + \mathbf{\Pi} T_t \times D_i + \alpha_1 D_i + \mathbf{\Psi} T_t + \mathbf{X}_{it}\mathbf{\Omega} + \delta_i + \gamma_c + \epsilon_{it} \quad (1)$$

- D_i is a dummy variable $= 1$ if an individual is a prior fraud or ID theft victim
- T_t is a vector of quarter dummy variables
- $X_i t$ includes county-level controls for unemployment rate, population, percent minority, and age dummy variables
- Also include individual fixed effects, δ_i, and county fixed effects, γ_c
- $\mathbf{\Pi}$ contains DID coefficient estimates for each quarter

Discussion and Conclusion

- Response greater and more persistent for prior identity theft victims
- Relative to other consumers, former ID theft victims were more likely place credit freezes by 0.1%; for former breach victims, this increase was only 0.05%
- Decline in retail trades small, but persistent
- Implies that increasing information for victims and keeping costs low may improve consumers' ability to take precautionary actions after a breach