# Identity Theft as a Teachable Moment

Slava Mikhed

with Robert Hunt, Julia Cheney,
Dubravka Ritter, and Michael Vogan

Payment Cards Center
Federal Reserve Bank of Philadelphia

* The views expressed in this paper are those of the authors and do not necessarily reflect the views of the Federal Reserve Bank of Philadelphia or the Federal Reserve System.

# Identity Theft Is Costly

- Nearly 17 million victims in 2012
  - 7 % of adults
  - 1 million had new accounts opened
- Out-of-pocket losses are uncommon
  - 85 % lose nothing; 7 % lost less than $100
  - But over a million lost $100+
- Increased exposure to collections, time costs, emotional distress

Source: National Crime Victimization Survey (Harrell and Langton 2013)

# Why Should We Care?

- ID theft exposes sensitive consumer information
- Existing remedies (fraud alerts) provide some protection
- Alerts allow consumers to receive free credit reports
- Shock to the salience of credit files
- May induce consumers to monitor their files

# What To Do Right Away

Did someone steal and use your personal information? Act quickly to limit the damage.

- Step 1: Call the companies where you know fraud occurred.
- Step 2: Place a fraud alert and get your credit report.
- Step 3: Report identity theft to the FTC.
- Step 4: File a report with your local police department.

# What To Do Next

Take a deep breath and begin to repair the damage.

- Close new accounts opened in your name.
- Remove bogus charges from your accounts.
- Correct your credit report.
- Consider adding an extended fraud alert or credit freeze.

# Research Questions

- How do people respond to identity theft?
- How does their behavior change over time?
- What are the consequences of identity theft on credit bureau attributes?

# Main Results

- Subprime consumers experience:
  - Persistent increase in risk score after alert
  - Higher % of cards in good standing
  - Fewer accounts in collections
  - More responsible use of credit
- Prime consumers:
  - Transitory effect on scores and other credit variables

# Analysis of New Data

- The PCC obtained
  - Extended fraud alerts on credit reports
  - Linked to the NY Fed Consumer Credit Panel / Equifax data
- We study likely victims of identity theft
  - We measure immediate effects and their persistence

# ID theft protection

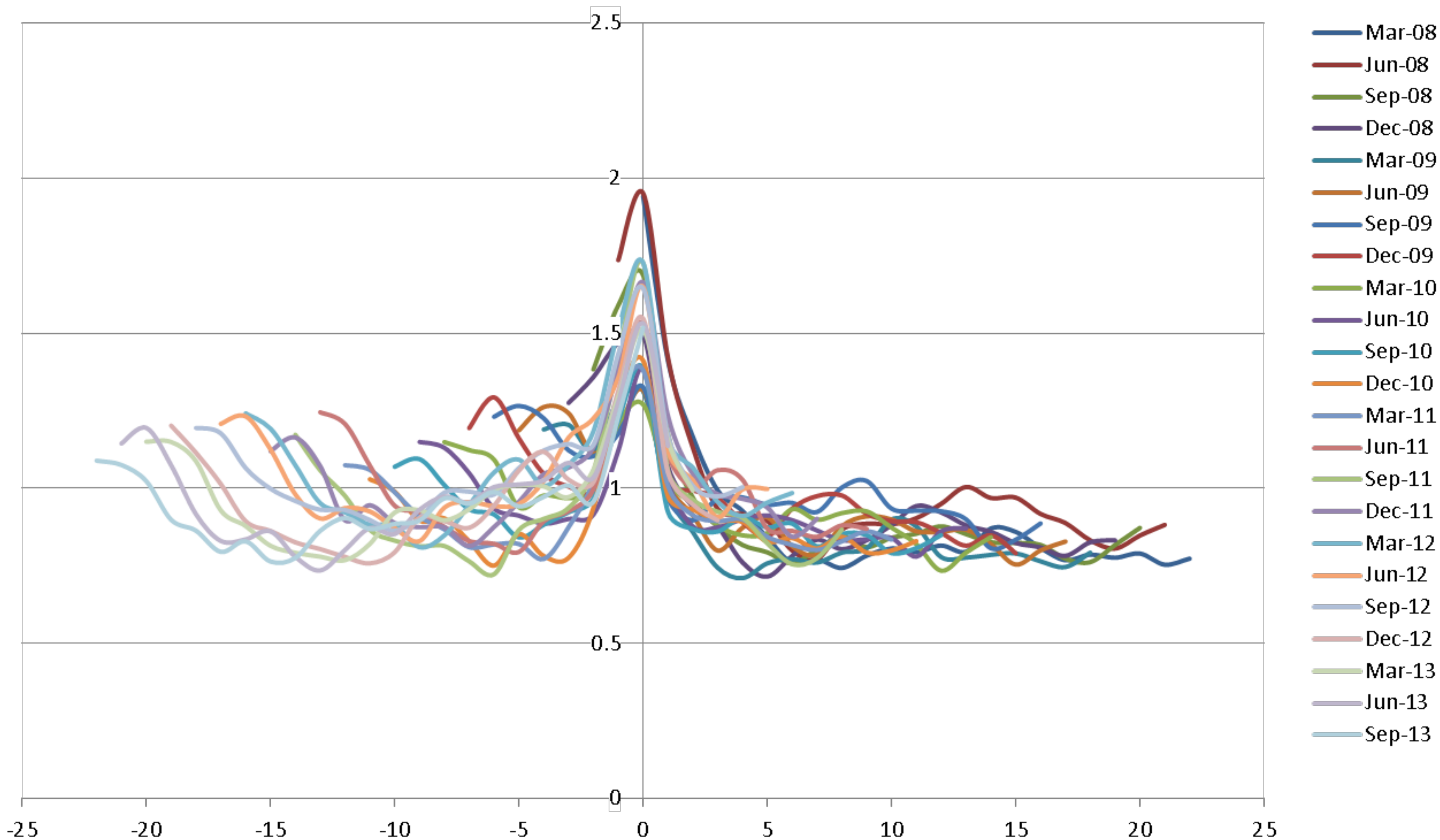
- Extended alerts*
  - Last 7 years
  - 5-year opt-out of prescreened solicitations
  - No cost to the consumer
  - Require a police report alleging fraud
  - Provide free credit reports

*Codified in the Fair and Accurate Credit Transaction Act of 2003

# Indications of ID theft

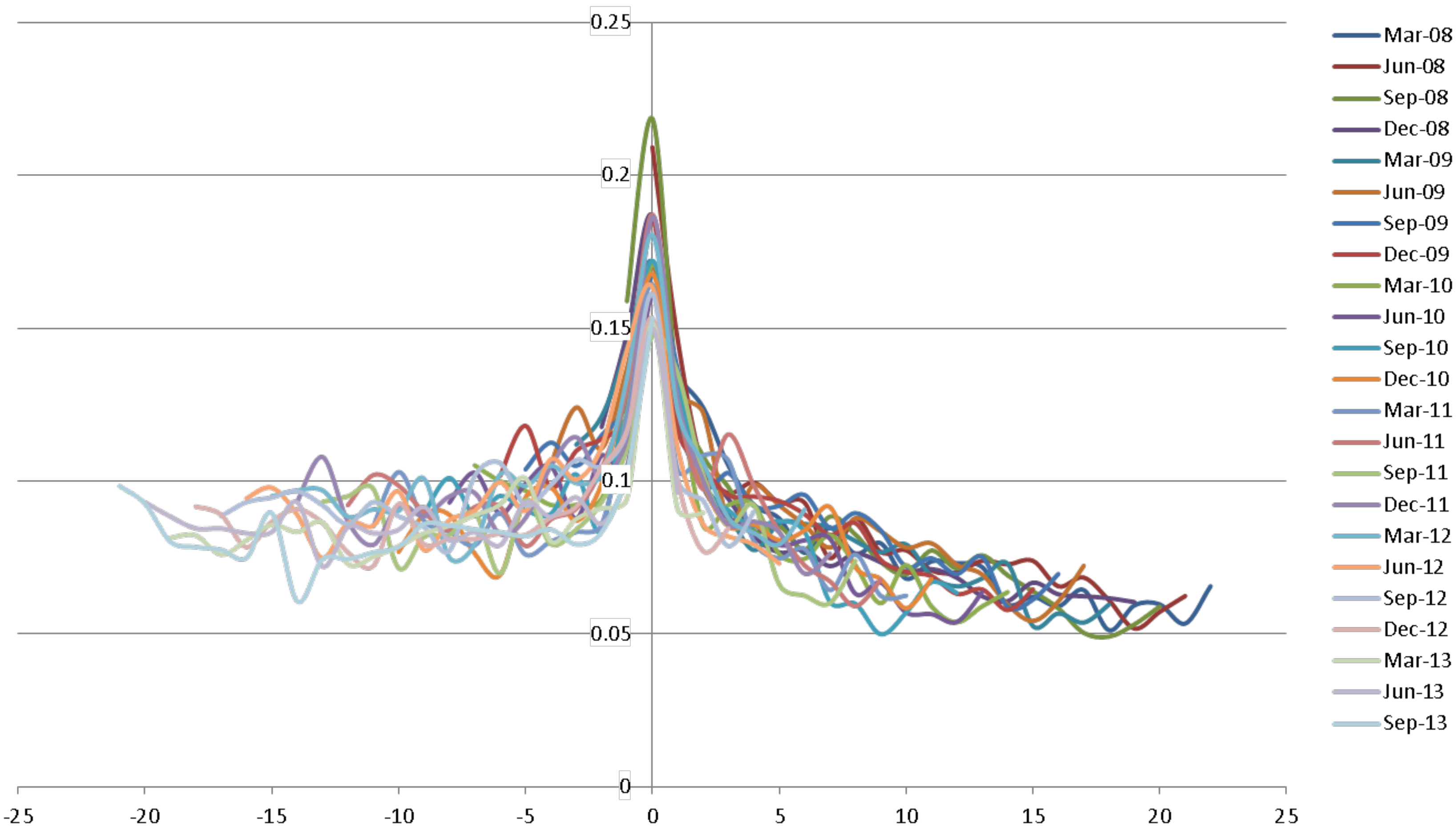
- Credit applications
- Address change
- Risk score change

# Credit Applications Spike upon Filing



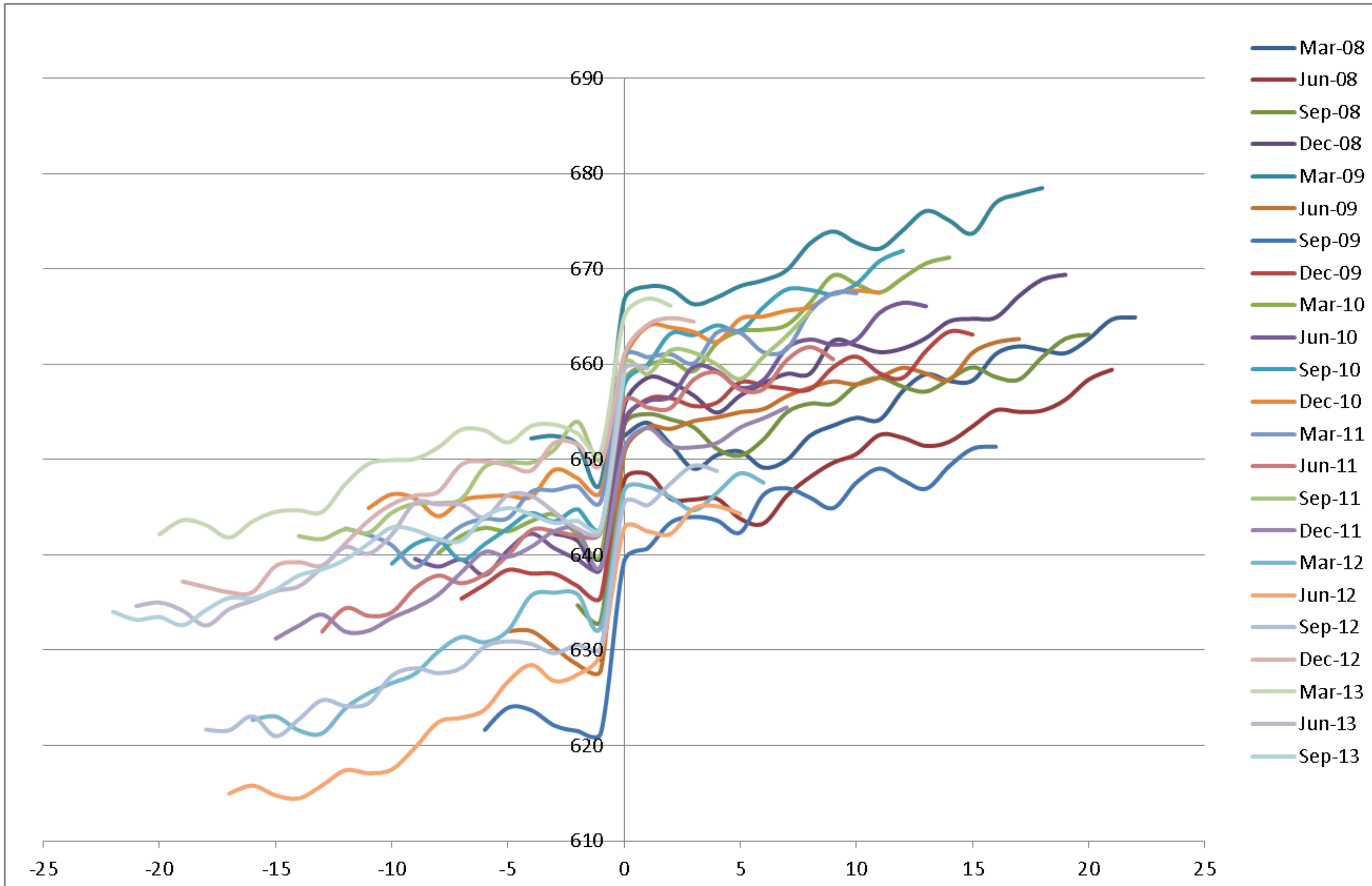

Source: Cheney et al. (2014b) using data from the FRBNY CCP, augmented with variables acquired by the Payment Cards Center

# Address Changes also Spike




Source: Cheney et al. (2014b) using data from the FRBNY CCP, augmented with variables acquired by the Payment Cards Center

# Risk Score Jumps at Extended Alert

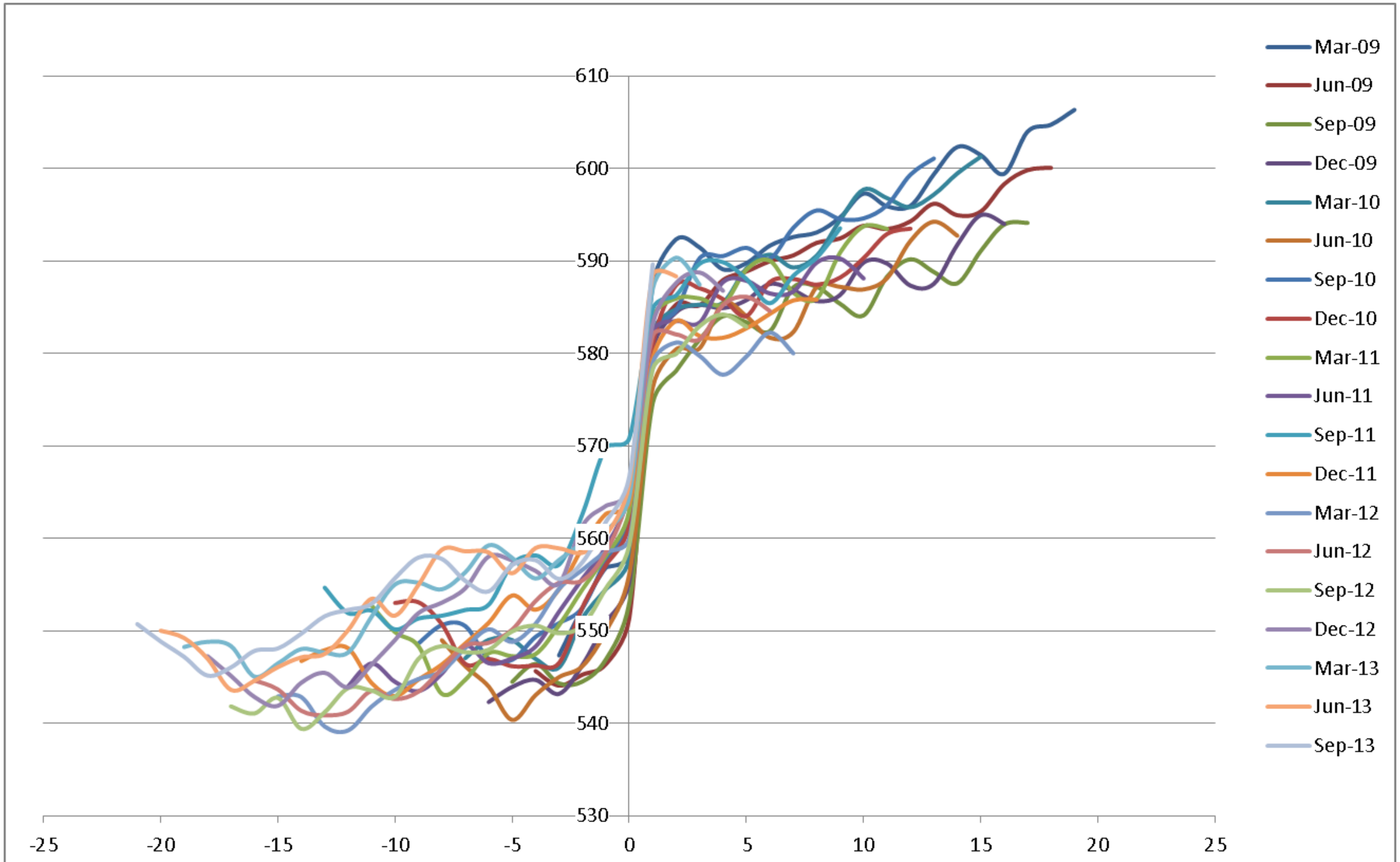



Source: Cheney et al. (2014b) using data from the FRBNY CCP, augmented with variables acquired by the Payment Cards Center

# Differences by Segment

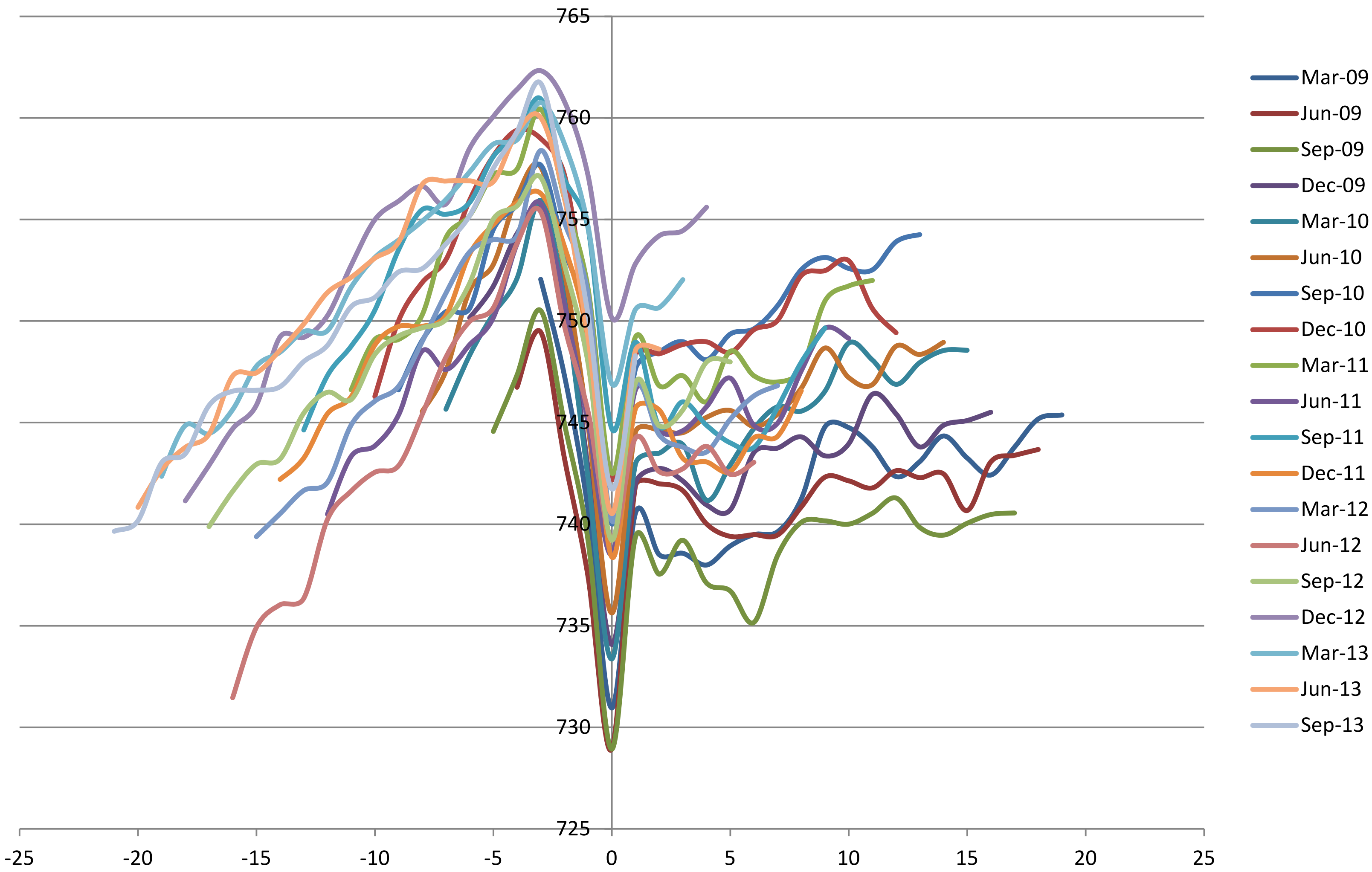
- Filers’ risk scores are low
- Subprime use extended alerts more
- Look at prime and subprime separately

# Risk Score for Subprime Consumers




Source: Cheney et al. (2014b) using data from the FRBNY CCP, augmented with variables acquired by the Payment Cards Center

# Risk Score for Prime Consumers




Source: Cheney et al. (2014b) using data from the FRBNY CCP, augmented with variables acquired by the Payment Cards Center

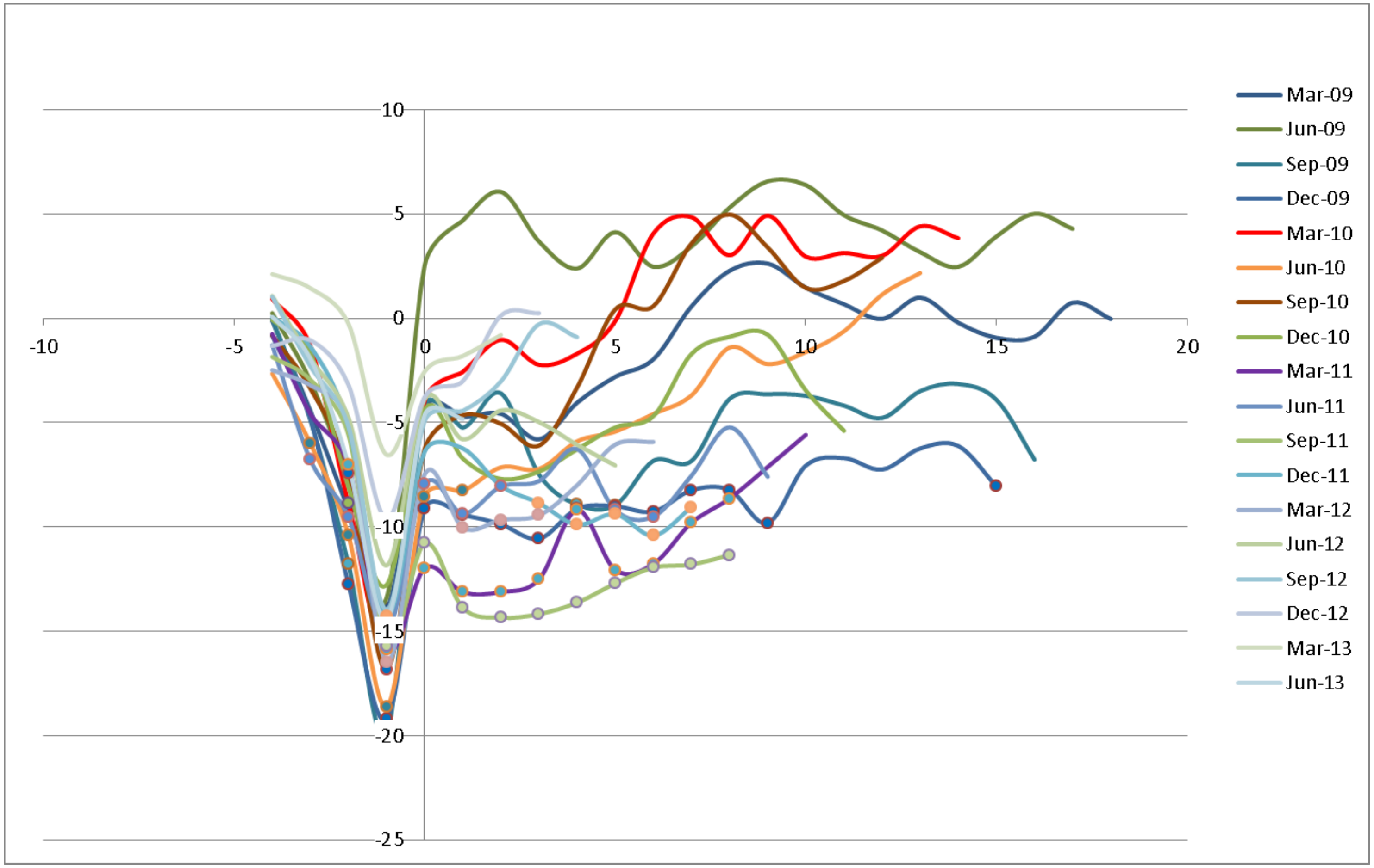
# Data Issues

- Extended fraud alert filers need evidence of identity theft to file, cannot "self-select" based on worries
- Criminals may select victims based on profitability
- Not all victims file alerts:
  - Only 9 % of victims check their reports and 70 % of those file an alert or freeze (Harrell and Langton, 2013)
  - We find choice of alert is affected by lags of credit bureau variables (Cheney et al 2014)
- We use propensity score matching to select a control population
  - Sets a higher bar than simply comparing identity theft victims with population trends

# Propensity Score Methodology

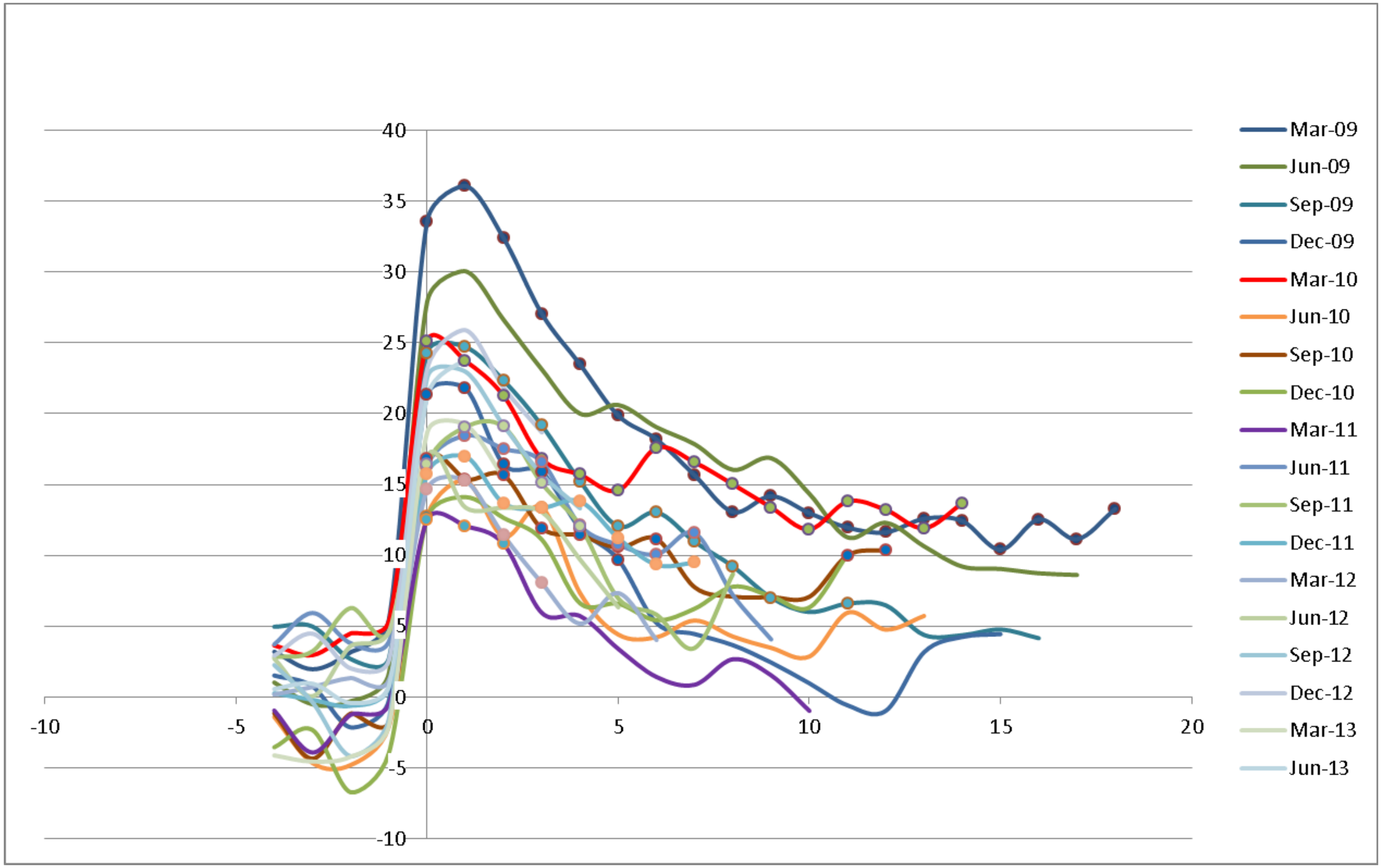
- Victims are allocated to cohorts based on the timing of their alert
  - Allows us to separate business cycle effects
  - Allows for heterogeneity in breaches
- We estimate two models for each cohort
  - One each for prime and subprime consumers
  - Models use a four quarter lag of characteristics:
    - Age, risk score, inquiries, number of accounts, utilization, etc.
- We test for differences in outcome variables

# Prime Consumers: Transitory Effect on Risk Score



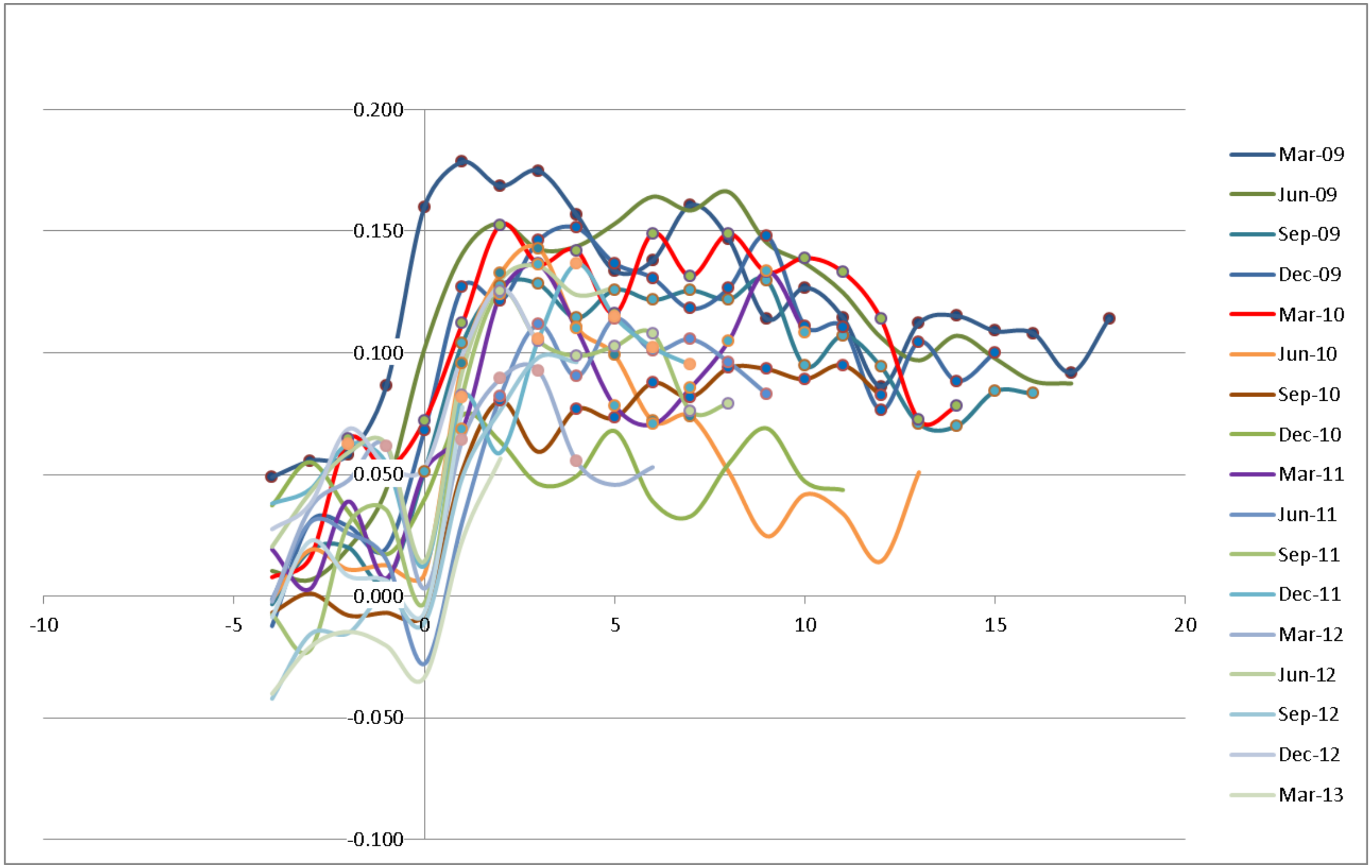

Source: Cheney et al. (2014b) using data from the FRBNY CCP, augmented with variables acquired by the Payment Cards Center

# Subprime Consumers: Persistent Effect on Risk Score




Source: Cheney et al. (2014b) using data from the FRBNY CCP, augmented with variables acquired by the Payment Cards Center

# More Accounts in Good Standing for Subprime Consumers




Source: Cheney et al. (2014b) using data from the FRBNY CCP, augmented with variables acquired by the Payment Cards Center

# Summary

- Credit bureau outcomes for ID theft victims
  - For prime consumers, the effects of identity theft are transitory
  - For subprime consumers, there are persistent, positive effects
- We believe this difference is due to consumer inattention before the event
  - A fraud event may be a “teachable moment” for some consumers