FEDERAL RESERVE BANK
PHILADELPHIA

Working Papers
RESEARCH DEPARTMENT

Does Experience Matter? Past Fraud Exposure, Data Compromises, and Credit Market Behavior

Nathan Blascak
Federal Reserve Bank of Philadelphia
Consumer Finance Institute

Ying Lei Toh
Federal Reserve Bank of Kansas City

WP 26-10

PUBLISHED
February 2026

FRB CFI
PHILADELPHIA

ISSN: 1962-5361

Disclaimer: This Philadelphia Fed working paper represents preliminary research that is being circulated for discussion purposes. The views expressed in these papers are solely those of the authors and do not necessarily reflect the views of the Federal Reserve Bank of Philadelphia or the Federal Reserve System. Any errors or omissions are the responsibility of the authors. Philadelphia Fed working papers are free to download at: https://www.philadelphiafed.org/search-results/all-work?searchtype=working-papers.

DOI: https://doi.org/10.21799/frbp.wp.2026.10

Does Experience Matter? Past Fraud Experiences, Data Compromises, and Credit Market Behavior*

Nathan Blascak[†] Ying Lei Toh[‡]

February 2026

Abstract

We study how past experiences with fraud affect individuals' likelihood of taking precautionary action in credit markets when faced with a new shock that raises their fraud risks. We focus on two kinds of past experiences with fraud: direct experience with fraud and a "near-miss" experience that increased fraud risk but did not directly lead to fraud. Using the 2017 Equifax data breach announcement, we show that individuals with either type of prior experience with fraud were more likely to take a precautionary action — freezing their credit report — than individuals with no prior experience with fraud. We also find that individuals with past direct experience with fraud were more likely to freeze their credit report than individuals who had a past near-miss experience. The individuals who froze their credit report had fewer total accounts and credit inquiries than those who did not, but this reduction in credit did not reduce their credit scores.

Keywords: Equifax data breach, consumer credit, credit freeze

JEL Classification: D14, D80, G51

[*] The authors would like to thank Alessandro Acquisti, Julia Cheney, Fumiko Hayashi, Mallick Hossain, Bob Hunt, Thanh Lu, the anonymous reviewers for WEIS, and seminar participants at the APPAM Fall Research conference, the CEPR Household Finance seminar series, Boulder Summer Conference on Consumer Financial Decision Making, the Consumer Finance Round Robin, WEAI Conference, the Federal Reserve System Applied Micro Conference, Carnegie Mellon University, and the Federal Reserve Bank of Kansas City for their helpful comments. Ian McGroarty and Bryant Wright provided excellent research assistance.

[†] Consumer Finance Institute, Federal Reserve Bank of Philadelphia (email: nathan.blascak@phil.frb.org)

[‡] Federal Reserve Bank of Kansas City (email: yinglei.toh@kc.frb.org)

Disclaimer: This Philadelphia Fed working paper represents preliminary research that is being circulated for discussion purposes. The views expressed in this paper are solely those of the authors and do not necessarily reflect the views of the Federal Reserve Bank of Philadelphia, the Federal Reserve Bank of Kansas City, or the Federal Reserve System. Any errors or omissions are the responsibility of the authors. No statements here should be treated as legal advice. Philadelphia Fed working papers are free to download at https://philadelphiafed.org/research-and-data/publications/working-papers.

1 Introduction

Data compromises, incidents where an individual's personal information is exposed to unauthorized parties, are an increasingly common source of shocks to an individual's privacy. In 2024 alone, the Identity Theft Resource Center recorded 3,158 data compromises, with 80% of the incidents involving sensitive personal identifiable information (PII), which can place affected individuals at heightened risks of fraud. Although fraud imposes significant financial and psychological costs on victims,[1] prior studies have shown that few individuals affected by a data compromise adopt precautionary measures, such as ID theft protection services or credit report freezes, to reduce their risk of experiencing fraud (Mayer et al., 2023; Zou et al., 2018; Institute, 2014; Romanosky et al., 2011; Brodkin, 2007). Understanding the factors that influence an individual's decision to adopt precautionary measures can help inform policies to promote greater adoption of these measures.

In this paper, we examine individuals' past experiences with fraud as a potential factor that influences their precautionary response when faced with a new threat of fraud. We first propose a conceptual framework for analyzing individuals' decision to adopt a precautionary measure and use the framework to examine the channels through which past experiences with fraud may affect individuals' responses to a future threat. We then test the predictions of our framework empirically by leveraging the 2017 Equifax data breach, which unexpectedly exposed sensitive PII of 147 million U.S. consumers, over 70% of the U.S. adult population.

Our conceptual framework draws insights from the literature on individuals' precautionary behavior in hazard domains and the literature on individual judgment and decision making under risk. In our framework, individuals evaluate fraud risk *cognitively* and *affectively*. The cognitive evaluation involves assessing the probability of the occurrence of fraud and the magnitude of harm. We assume that individuals rely on judgment heuristics to assess risk and therefore are susceptible to cognitive errors and biases.[2] The affective evaluation is driven by negative feelings associated with fraud, such as anxiety and fear, which can lead to higher perceived risk. Based on their risk assessment, individuals then decide whether to incur a cost to adopt a precautionary measure that reduces the risk of fraud.

We then propose that past experiences with fraud serve as an important source of risk information that affects individuals' cognitive and affective risk evaluations when faced with a new threat of fraud. They may also affect individuals' cost of adopting a precautionary measure through learning. Based on these past experiences, we group individuals into three categories: past direct experience with fraud, past 'near-miss' experience with fraud (i.e.,

[1] According to the US Department of Justice, in 2021, the mean direct financial loss for fraud victims was $880, and the 10% of victims were severely distressed by the fraud (Harell and Thompson, 2023).

[2] For example, the availability heuristic documented by Tversky and Kahneman (1973).

faced fraud risks but did not experience fraud in the past), and no prior experience with fraud. We hypothesize that individuals with prior fraud experience are more likely than individuals in the other two groups to adopt a precautionary measure in response to a data compromise since they have the highest perceived fraud risk and the lowest cost of adopting a precautionary measure. However, we are unable to hypothesize whether individuals with a previous near-miss experience would be more or less likely to adopt a precautionary measure than those who have no prior experience with fraud. Our conceptual framework suggests that the near-miss group may have lower perceived fraud risk, which lowers their likelihood of adopting a precautionary measure, but also has a lower cost of adopting a precautionary measure, which raises the likelihood.

To test our hypotheses empirically, we analyze how individuals' past experiences with fraud affects their precautionary response to the 2017 Equifax data breach. Specifically, we examine individuals' placement of credit report freezes – a tool that restricts lenders' access to credit reports, subsequently preventing the opening of new credit accounts. We utilize a large nationally representative data set of anonymized credit bureau records that also contains information on credit report freezes and fraud flags. The detailed nature of this data allows us to empirically identify the three groups of individuals with recent fraud experiences[3] that correspond to our conceptual framework: (1) individuals who placed an extended fraud alert in their credit report, an indicator of experiencing severe fraud in the past; (2) individuals who likely had their information exposed during the 2015 Anthem data breach, which corresponds to the experience of 'near-miss'; and (3) individuals with no observable recent exposure to fraud risk. To simplify our exposition, we refer to these groups of individuals as prior fraud victims, prior breach victims, and prior non-victims, respectively.

With this data, we estimate a series of difference-in-differences (DID) regression models to compare how each of our prior experience groups responded to the Equifax data breach announcement relative to the non-victims. Consistent with our hypothesis, we find that prior fraud victims are 0.1 to 0.25 percentage point more likely (a relative 25% increase) to place a credit freeze than non-victims in the quarters after the Equifax breach announcement. For prior breach victims, we find that they are 0.1-0.3 percentage point more likely (a relative 30% increase) to place a credit freeze than non-victims. The result for prior breach victims is consistent with exposure to the Anthem breach having a greater effect on the cost of adopting a measure than on the perceived risk of fraud. We then compare the

[3] We focus on recent experiences because we do not observe the full set of experiences of individuals, and recent experiences tend to have disproportionately strong effects on individuals' perceptions and actions (Hertwig et al., 2004).

precautionary responses of prior fraud victims and prior breach victims to the Equifax breach announcement. Prior fraud victims placed fewer new freezes than prior breach victims in the quarter of the announcement, but prior fraud victims placed more new freezes overall (from the second quarter following the announcement until the end of our sample). These results indicate that the likelihood of taking a precautionary action in the credit market varies by prior fraud experience.

Finally, we examine the impact of the placement of a new credit report freeze on individuals' financial outcomes. While credit report freezes help prevent criminals from accessing a consumer's personal information to fraudulently open new accounts, it also introduces a friction into the process of acquiring new/additional credit for individuals who decide to freeze. We divide each prior experience group into two categories: individuals who froze their credit report in response to the Equifax data breach and individuals who did not freeze. Our results show that regardless of fraud exposure type, individuals who froze their credit report had fewer credit inquiries and a lower total number of accounts than non-freezers in the quarters after the breach announcement. For prior breach victims and non-victims, freezers had lower balances on all their accounts and lower total credit limits than non-freezers. Despite this reduction in credit market activity, credit scores are not different for freezers and non-freezers. In total, our results suggest that while placing a new credit report freeze does reduce the accumulation of new credit, it does not harm financial health through a decline in credit scores.

The remainder of this paper is structured as follows. Section 2 discusses related literature. Section 3 presents our conceptual framework for examining how past experiences with fraud risk may affect precautionary response to a new data compromise. Section 4 provides a brief background of the Equifax data breach and initial evidence of adoption of precautionary credit market measures following the announcement. In Section 5, we describe our data and sample construction, and in Section 6, we present our empirical specifications and our findings. Section 7 discusses the effect of credit report freezes on financial outcomes, and Section 8 concludes.

2 Related Literature

Our work primarily contributes to three bodies of literature. First, our paper contributes to the literature on consumer responses to data breaches. Prior research has found that some individuals adopt precautionary measures after becoming a data breach victim in a number of different contexts, such as choosing different payment methods (Agarwal et al., 2024), removing potentially identifying information such as profile pictures (Turjeman and

Feinberg, 2019), and placing fraud alerts and credit freezes in their credit reports (Mikhed and Vogan, 2018). Mayer et al. (2023) conducted two surveys to investigate individuals' responses to data breaches and found that some individuals took steps such as changing their passwords and reviewing their credit and financial reports after becoming aware that they had been affected by a data breach.

Researchers have also identified several factors that may affect individuals' response to a data breach. These factors include the effectiveness with which the breached entity communicates the breach and available protective measures, individuals' knowledge of available protective measures, the presence of overlapping protective measures, the cost of adopting these measures, and behavioral factors, such as the underestimation of the probability of falling victim to fraud (optimism bias), the preference for remaining in the status quo, acting only after fraud has occurred (status quo bias), and the desensitization to data breaches due to breach or notification fatigue (Mayer et al., 2023; Zou et al., 2019, 2018; Lillian et al., 2016; Romanosky et al., 2011).

Our work also contributes to the literature on how past hazard experiences affects the adoption of protective actions against a future hazard. Many studies have found that direct experience with a past hazard that led to adverse outcomes is positively correlated with the adoption of protective or preventative action against the hazard. This result has been found in studies on natural disaster hazards (e.g., Lindell and Hwang (2008); Siegrist and Gutscher (2006); Peacock (2003); Zaleskiewicz et al. (2002); Dooley et al. (1992); Jackson (1981)), illnesses and diseases (e.g., Nowak et al. (2015); Andersson et al. (2009); McKenna et al. (2004); Fein et al. (1995); Cody and Lee (1990)), and crime (e.g., Averdijk (2011); Dugan (1999); Rountree and Land (1996)). We find a similar effect of past victimization in our study: Individuals who were likely victims of severe fraud in the past were more likely to place a credit freeze.

We extend this literature by exploring how individuals' past experiences with fraud affects their precautionary responses to a (future) data compromise. Our conceptual framework draws from protective action adoption models from other hazard domains (Lindell and Perry, 2012; Rogers, 1975). In those models, an individual's cognitive evaluation of perceived hazard risk depends on their perception of the probability of the hazard's occurrence and the severity of the outcomes. In our model, we also include the affective evaluation of risk as a component of perceived risk, as various studies find that an individual's feelings of risk is an important driver of their risk perception (Siegrist and Gutscher, 2008; Zaleskiewicz et al., 2002; Finucane et al., 2000). In addition to examining the effect of past victimization, we also examine the experience with the non-occurrence of the hazard or a near miss, which in our setting corresponds to exposure to a data compromise that did not lead to fraud.

The few studies that have examined the effects of near misses on the adoption of protective action have found that individuals who experienced or were provided information about a prior near-miss are less likely to adopt protective actions than those without such experience or information (Bogani et al., 2023; Dillon et al., 2011). In contrast to existing studies, we find that the individuals in our near-miss group were more likely to have adopted a protective action. We provide a few possible explanations for the difference based on our conceptual framework.

Finally, our paper contributes to the literature on the effect of fraud on households' finances. Though the majority of studies in this area focus on fraud in financial markets (e.g., Giannetti and Yue Yang (2016); Gurun et al. (2018); Knüpfer et al. (2024)), there are few studies that focus on identity theft (Blascak et al. (2025); Hamdi et al. (2024)). Our study complements this research by examining how past fraud affects households' decisions to protect themselves financially from future fraud.

3 Conceptual Framework

To examine how different types of past experiences with fraud may affect individuals' response to a new threat of fraud, we propose a behavioral model of protective measure adoption that draws on existing models of individual precautionary behavior and the literature on judgment and decision making under risk. In our framework, an individual has to decide whether to adopt a protective measure to mitigate their risk of experiencing fraud, and their decision depends upon their risk perceptions and protective action perceptions, similar to the Protection Motivation Theory proposed by Rogers (1975).

We assume that individuals do not know their objective risk of fraud and form risk perceptions based on the risk information available to them. The information may come from public authorities, the compromised entity (e.g., in the form of a breach notification letter), their social network, as well as relevant past experiences with fraud. Drawing on the theories proposed by Loewenstein et al. (2001) and Slovic et al. (2004), we consider two channels through which risk information may affect risk perceptions: cognitive (risk as analysis) and affective (risk as feelings).[4] The cognitive evaluation of risk involves assessing the probability of fraud, p_i, and the magnitude of the associated loss, l_i. We assume that individuals make their probability judgment intuitively by relying on heuristics. The affective evaluation of risk is based on feelings that individuals experience when they learn that they are at risk of fraud victimization. Based on findings in the literature on affect and risk

[4] Several studies have found that risk perceptions models that include both cognitive and affective components provide the best fit for data (Van der Linden, 2014; Holtgrave and Weber, 1993).

perceptions, we posit that having stronger negative feelings (e.g., fear, shock, dread, and anxiety) about the risk of new account fraud leads to a higher perceived risk of fraud. We let e_i be a measure of the intensity of negative affect experienced by individual i, where higher e_i corresponds to a stronger negative affect.

Individuals' cognitive evaluation of risk may influence their affective evaluation of risk, and vice versa. Similar to Finucane and Holup (2006), we are agnostic about how individuals combine their cognitive and affective evaluations of risk to form their risk perceptions. We let $x_i = h(p_i, l_i, e_i)$ be the joint outcome of the cognitive and affective risk evaluations. We call x_i the *as-if* expected fraud loss of individual i; i.e., individual i assesses the benefit of adopting the protective measure *as if* the expected fraud loss is x_i. The as-if expected loss is increasing in p_i, l_i, and e_i and may deviate from the expected loss based on individual i cognitive evaluation of risk, $p_i l_i$, because of the affect experienced by the individual.

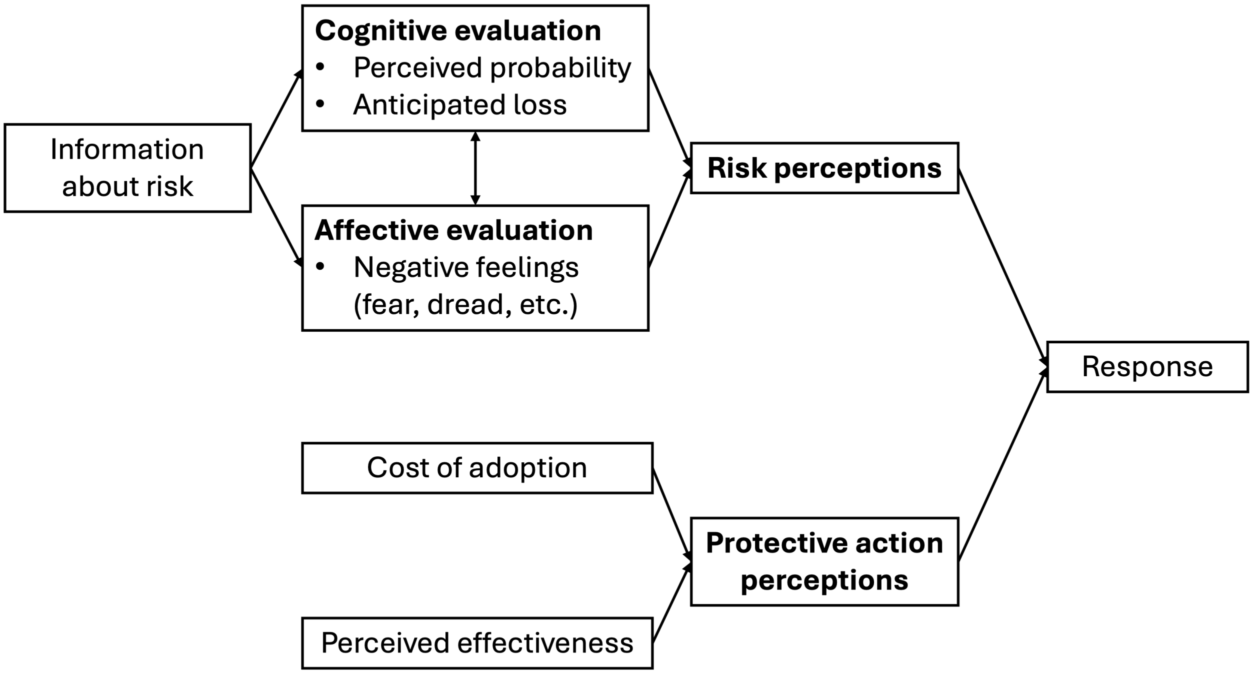
Individuals' perceptions of the protective action consist of their perceived cost, c_i, and perceived effectiveness, τ_i, of the protective action, where τ_i is the share of expected loss that individual i believes that the protective measure would help reduce. Individuals' perceived cost of adopting the protective measure comprises both pecuniary and non-pecuniary (e.g., time and effort) components. The non-pecuniary component depends in part on the information the individual possesses about the protective measure. The lack of awareness of the protective measure can be captured in our model by setting the cost of the protective action to infinity. Figure 1 illustrates our proposed framework.

We assume that individuals decide whether to adopt the protective measure by weighing the benefit (i.e., the reduction in (as-if) expected fraud loss) against the cost of adopting the measure. More precisely, individual i chooses to adopt the protective measure if $\tau_i x_i > c_i$.

3.1 Effects of Past Fraud Experiences on Precautionary Behavior

Past experiences with fraud may affect individuals' decision to adopt a protective measure through both their risk perceptions and protective action perceptions. First, past experiences with fraud may affect individuals' cognitive assessment of risk through the availability heuristic, where individuals judge the probability of an event based on the ease with which they are able to recall instances of the event's occurrence (Tversky and Kahneman, 1973). Direct personal experience of an event increases the availability of the event in an individual's mind. The use of the availability heuristic implies that individuals who have personally experienced fraud in the past are more likely to recall instances of fraud occurring and thus perceive the probability of fraud following the data compromise to be higher. In contrast, individuals who were exposed to fraud risk in the past (e.g., as a result of a data compro-

Figure 1: Behavioral Framework of Protective Action Adoption



Notes: This figure presents a flow diagram representation of our conceptual framework.

mise) but did not experience fraud are likely to recall instances of the non-occurrence of fraud and thus perceived the probability of fraud arising from the (new) data compromise to be lower. Further, we postulate that individuals who have not previously experienced fraud may underestimate the loss, particularly the non-pecuniary aspect (e.g., time and energy required to resolve resulting financial and credit problems).

Second, past experiences with fraud may also affect individuals' affective evaluation of risk. Although all individuals affected by a data compromise may experience some level of negative affect, studies on other types of hazards suggest that individuals who have previously experienced fraud are likely to have the strongest affective response to the data compromise (Becker et al., 2017; Siegrist and Gutscher, 2008). Further, studies have found that individuals who have been previously exposed to a hazard risk, but did not experience the hazard (i.e., individuals who experienced a near miss), may experience less negative affect than individuals without such past experiences (Tinsley et al., 2012; Dillon et al., 2011).

Finally, past experiences with fraud may affect individuals' awareness and knowledge of the protective actions available (Weinstein, 1989). Zou et al. (2018) interviewed individuals following the 2017 Equifax data breach and found that most respondents were either unaware of or misunderstood common protective actions (e.g., placing fraud alerts and credit freezes); only individuals who were offered these protective services in *previous* data breaches were able to correctly describe these measures.[5] This finding suggests that exposure to fraud or fraud risk in the past may lower the amount of time and effort required to adopt a protective measure; i.e., lower the non-pecuniary cost of adoption. We further postulate that prior fraud victimization may be associated with an even greater level of knowledge and awareness than fraud risk exposure, as past fraud victims are more likely to have adopted the protective action in the past in response to their victimization.

The above discussion suggests that individuals may differ in their likelihood of adopting a protective action in response to a new data compromise if they have previously experienced fraud (F), previously experienced a near miss (M) (i.e., exposed to fraud risks but did not experience fraud), or no previous experience with fraud (N). Suppose for simplicity that within each group, individuals only differ in their non-pecuniary cost of adopting the protective action, which captures the heterogeneity in individuals' cost of time and effort. Based on the above discussion, we expect $p_F > p_N > p_M$, $l_F > l_N = l_M$, and $e_F > e_N > e_M$. Thus, we conjecture that the perceived fraud risk resulting from the data compromise should be highest for the individuals who previously experienced fraud and lowest for those who previously experienced a near miss; i.e., $x_F > x_N > x_M$. We expect the time and effort needed to adopt the precautionary measure to be lowest for individuals who have previously experienced fraud and highest for those who have not previously been exposed to fraud risk. We capture these differences in our framework by assuming that the distribution of the cost of adopting the precautionary measure for individuals previously exposed to fraud, G_F, is first-order stochastic dominated by that for individuals who previously experienced a near-miss, G_M, which is first-order stochastic dominated by that for individuals with no previous experience with fraud risk, G_N; i.e., $G_F \succeq_1 G_M \succeq_1 G_N$. We assume that the perceived effectiveness of the protective measure is the same across the three experience groups, as we do not have a strong prior on how they might vary.

In all, our analysis suggests that the probability of adopting a protective measure in response to a data compromise, $Pr(c_ij < \tau x_j) = G_j(\tau x_j)$ where $j \in \{F, M, N\}$, is highest among individuals who have previously experienced fraud: $G_F(\tau x_G) > G_M(\tau x_M)$, $G_N(\tau x_N)$. However, we are unable to predict *a priori* whether individuals with a near-miss experience would be more or less likely to adopt a protective measure than individuals with no prior fraud risk experience, owing to the opposing effects of a prior near-miss experience on perceived fraud risk and the cost of adopting the protective measure. Individuals with a near-miss experience would be less likely to adopt the protective measure than those without previous fraud risk experience if the effect on perceived fraud risk dominates, while

[5] Studies in the preventative health-care literature have also found similar effects of learning from past exposure to an illness personally or via a first-degree relative (Baer et al., 2010; Mouchawar et al., 1999).

the reverse would be true if the effect on the cost of adopting the precautionary measure dominates.

We test our predictions empirically by examining individuals' responses to the 2017 Equifax data breach, a massive data compromise that exposed sensitive PII of the vast majority of U.S. adults. The next section describes the Equifax data breach in more detail.

4 The Equifax Data Breach

4.1 Background

Equifax is one of the three major credit bureaus (also known as credit reporting agencies) in the United States. Credit bureaus collect information about individuals' credit accounts (for example, account balances, payment histories, credit limits, debt collections, and bankruptcies) from various third parties, including banks, credit card companies, telecommunications and utilities companies, and landlords. Each credit bureau then compiles and maintains the information it has collected on an individual in a credit bureau file (or a credit report), which creditors and lenders can access and use for evaluating the individual's creditworthiness. Any individual who has recently used a traditional credit product (for example, a credit card, student loan, auto loan, or mortgage) almost certainly has a credit report at one or more of the three major credit bureaus. According to a 2015 study by the Consumer Financial Protection Bureau, the vast majority of adults (approximately 89%) in the United States has a credit report.

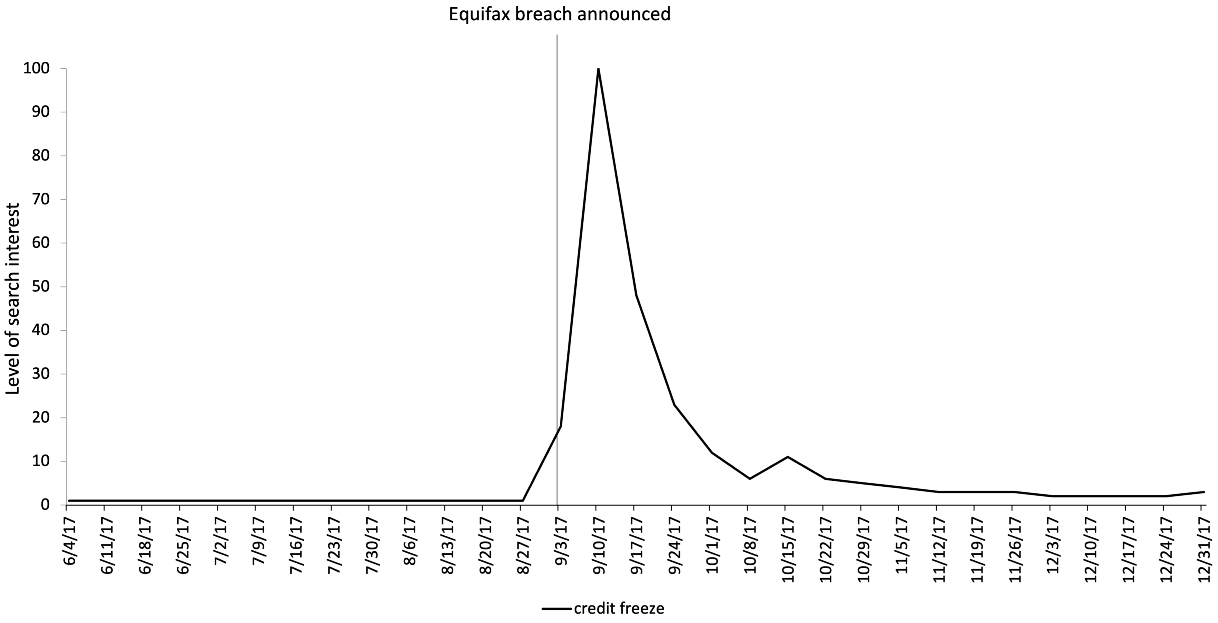
On September 7, 2017, Equifax publicly announced that it had suffered a data breach, potentially impacting 147 million individuals — the vast majority of adults — in the United States. Equifax revealed that hackers had gained unauthorized access to some of its data from mid-May through July 2017. The company detected the intrusion on July 29, 2017, and was able to identify and patch the vulnerability that the hackers had exploited to gain access to its system.[6] The information the hackers accessed included names, Social Security mumbers (SSNs), birth dates, home addresses, and, in some cases, driver's license numbers. Additionally, the hackers also obtained the credit card numbers of about 209,000 individuals and dispute documents with PII of about 182,000 individuals.

[6] Equifax describes their actions since 2017 in the Equifax 2020 Security Annual Report. The authors of this paper have not verified the accuracy of this report.

4.2 Individuals' Precautionary Behavior Following the Breach

Because the Equifax data breach exposed sensitive PII of individuals and the hackers' intentions were unknown at the time of the breach announcement, affected individuals were at a heightened risk of experiencing fraud in the credit market in the quarters after the breach. Following the announcement, many consumer protection groups, state attorneys general, and security experts recommended affected individuals adopt protective measures, particularly credit report freezes, to protect themselves against increased fraud risks. A credit freeze blocks access to an individual's credit bureau report and hence prevents fraudsters from successfully opening new credit accounts using the individual's identity.

Figure 2: Google Search Interest Over Time: Credit Freeze



Notes: Authors' calculations using data from Google trends from June 2017 to December 2017. Scale represents search interest relative to the highest point on the chart for the given time period.

Google search trend data indicate an increase in search interest in the search term *credit freeze* following the Equifax breach announcement, suggesting many individuals were considering placing credit report freezes. Figure 2 shows the Google search trends for *credit freeze* in the U.S. between June and December 2017. Search interest for the term increased sharply in the week following Equifax's breach announcement and began falling the week after. The timing of the rise and fall in the level of search interest for *credit freeze* strongly suggests that the spike in interest for the term was induced by the breach announcement.

5 Data and Sample Selection

5.1 Data Description

To empirically examine how individuals with different past experiences with fraud reacted to the Equifax breach announcement, we use data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax (CCP). The CCP data set is an anonymized 5% random sample of all U.S. individuals with a credit bureau record. To be included in the data set, individuals must have a Social Security number and at least one public record or credit account.[7] The CCP is an unbalanced panel that follows individuals at a quarterly frequency and is constructed so that (1) new individuals are included over time as they open their first credit account or gain their first public records and (2) are dropped from the sample when they die or experience a prolonged period of credit market inactivity. The sample is designed in this way to mirror the entry and exit dynamics in the general credit bureau data population (Lee and van der Klaauw, 2010).

The CCP data are then merged with a unique data set of anonymized fraud alert information obtained by the Consumer Finance Institute from Equifax. These data contain detailed information on the type of fraud alert filed, the status of the alert, and utilization of other services such as credit freezes and opt outs from prescreened credit offers. Importantly, we also observe the month and year of the placement of both the fraud alerts and credit freezes, allowing us to more precisely measure when individuals take these measures.

To study the adoption of precautionary measures, we use the information on the date of placement of credit report freezes to create a variable that identifies when individuals place a *new* freeze on their credit report. Using the information in the fraud alert data, we create a dummy variable that is equal to one if either: (1) the date of the freeze placement is not equal to the freeze placement date in the previous quarter and (2) if the date of freeze placement is missing in the previous quarter. This allows us to identify if individuals with no prior credit freeze decide to freeze their credit report or an individual with an existing credit freeze un-freezes and re-freezes their credit report.[8]

To study the financial impacts of taking a precautionary measure, we examine credit inquiries, the total number of accounts, the total debt balance on all accounts, the total credit limit on all accounts, and credit scores.[9] The account, balance, and limit variables cover all types of accounts, including credit cards, auto loans, and mortgages.

[7] Public records include adverse events such as bankruptcy declarations or tax liens.

[8] For more details on fraud alert data, see Blascak et al. (2025).

[9] Our credit score measure is the Equifax Risk Score, which is a proprietary credit score produced by Equifax. The Equifax Risk Score is similar to other risk scores used in the industry.

5.2 Sample Construction

To form our analytical sample, we merge the data sets from the years 2014 to 2018. We drop any observations for individuals under the age of 18 or over the age of 80. We also drop all observations for any individual who is recorded as being deceased at any point during our sample period. We also drop any individual with fewer than four total observations across the sample period to mitigate any problems due to "fragment" files in the credit bureau data.[10] After these restrictions, we are left with approximately 12 million unique individuals.

To test our hypotheses on how *prior* exposure to fraud affects individuals' credit market behavior, we identify three sets of individuals in the CCP data. The first two groups are our treatment groups: (1) individuals who have previously experienced fraud and (2) those individuals who have faced heightened risks of fraud due to their exposure to the 2015 Anthem data breach (which we will elaborate on shortly). The third group is our control group, which comprises individuals who were not exposed to either severe ID theft or the Anthem data breach. We describe in detail how we identify our treatment groups in the following subsections.

5.2.1 Prior Fraud Exposure: Fraud Victims

To identify past victims of fraud, we use the extended fraud alert flags in the CCP data supplement, which is a strong indicator of being a victim of severe fraud. Under the Fair and Accurate Credit Transactions Act (FACTA), the presence of an extended fraud alert on an individual's credit report requires potential creditors to perform stringent identification verification requirements before extending credit to that individual. When filing an extended fraud alert, the individual must specify a telephone number or other reasonable contact method as part of the alert documentation; all creditors must contact the individual by the method specified in the alert to verify the individual's ID when receiving an application for credit. Once placed, the extended fraud alert remains on the individual's credit reports for seven years (unless the individual chooses to remove it beforehand) instead of one.[11]

The placement of an extended fraud alert flag in an individual's credit file is an excellent proxy for severe fraud victimization. Placing an extended fraud alert in a credit bureau file is an elaborate filing process, as the alert filer is required to submit either a police report or an ID Theft Report (ITR) to place the alert in their credit file. An ITR requires detailed information on the accounts that were compromised and accompanying evidence of ID theft

[10] Fragment credit bureau records occur when new records are created and then subsequently merged with preexisting records when a credit bureau discovers that the two records belong to the same individual.

[11] Additionally, an extended fraud alert removes the individual's credit file from lists of prescreened credit and insurance offers for five years.

or fraud. Providing such evidence entails both time and effort, and individuals face criminal penalties for falsifying information in these reports. Because of these requirements, filers of extended alerts are unlikely to place alerts in their credit bureau files based simply on worries or as a precaution.[12]

5.2.2 Prior Exposure to the Risk of Fraud: 2015 Anthem Data Breach Victims

Anthem (Anthem Inc.) is one of the largest health insurers in the United States. Anthem offers private insurance plans through the Blue Cross (BC) and Blue Cross Blue Shield (BCBS) networks, as well as managed care plans (Medicaid). As of the end of 2014, Anthem and its affiliates served over 71 million individuals from all across the country. It offered private insurance plans in 14 states, operating as Anthem Blue Cross, Anthem Blue Cross Blue Shield, Blue Cross Blue Shield of Georgia, or Empire Blue Cross Blue Shield, and provided managed care plans in 19 states and the District of Columbia through its subsidiaries, such as Amerigroup and UniCare.

In late January 2015, Anthem discovered that hackers had gained unauthorized access to one of its databases, which contained personal information, including names, dates of birth, Social Security numbers, home addresses, email addresses, and employment information of approximately 80 million customers and employees, dating back to 2004. On February 4, 2015, Anthem announced the data breach and began mailing out notification letters to individuals affected by the breach. In response to the breach, the company offered two-year free credit monitoring, child ID protection, and ID theft reparation services, which affected individuals could sign up for beginning on February 13, 2015.[13]

The likelihood of exposure to the Anthem breach varies by state, depending largely on Anthem's share of the insurance market in a given state. To identify how each state was affected by the breach, we gather data on the states where Anthem operated in 2015 (especially where it offered both BC or BCBS plans and Medicaid plans), and data on the number of individuals affected by the Anthem breach in each state.[14] Using this information,

[12] Using the same CCP data, Blascak et al. (2025) show that credit market behavior consistent with fraud, such as the opening of new accounts and changes of addresses, increases right before or concurrently with the placement of these flags.

[13] We chose to focus on the Anthem breach for a few reasons. First, it was one of the largest data breaches in the pre-Equifax breach period. Second, the Anthem data breach was still relatively recent at the time of the Equifax breach announcement and may therefore have a larger effect on individuals' precautionary behavior than older data breaches. Third, the types of data compromised in the Anthem breach are similar to those exposed in the Equifax breach, and thus individuals may be more likely to consider it as a relevant past experience to consider when they are assessing the fraud risk arising from the Equifax breach. Further, the knowledge and practical experience that individuals may gain from dealing with exposure to the Anthem breach are likely to be relevant in the case of Equifax's breach and may help to lower the cost of adopting a protective action in response to the Equifax breach.

[14] We collect data from news reports and press releases (whenever available). For states in which the victim

we identify a group of states that were most affected by the breach (defined as having more than 25% of the state's population having been a victim) and a group of states that were *least* affected by the breach (defined as having less than 5% of the state's population reported being a victim). Appendix Table A1 provides a breakdown of these states. We define individuals living in the most exposed states each as individuals affected by a prior data breach ("prior data breach victims").

In Appendix Section C, we provide event study results similar to those reported in Section 5.1 to demonstrate that individuals living in states that were most exposed to the Anthem data breach were more likely to respond to the announcement of the breach when compared to individuals living in states that were the least exposed.

5.3 Summary Statistics

Table 1 provides summary statistics for credit report freezes for prior fraud victims, prior data breach victims, and for the entire sample (including non-victims). The prevalence of having a credit freeze prior to the Equifax breach announcement is very low, with less than 1% of all individuals having an active freeze. This percentage increases by a factor of 4 (from 0.7% to 2.8%) after the breach announcement. We observe a similar difference in the fraction of individuals placing a new credit report freeze, where only 0.2% of individuals placed a new credit freeze in a given quarter in the pre-announcement period; this increases by a factor of 10 in the quarters after the announcement (0.2% to 2.3%). We observe relatively large differences in the means of our outcome variables of interest between our two groups of prior victims. These gaps are unsurprising given the differences in severity of the prior victimization.

We also show the total number of active credit report freezes and the number of new freeze placements for each exposure group over time in the raw data in Figure 3. The left-hand y-axis displays counts for non-victims and prior breach victims, while the right-hand y-axis displays the count for prior fraud victims; given the size of the prior fraud group, as shown in Table 1, the freeze count for prior fraud victims is orders of magnitude smaller than the counts for non-victims/prior breach victims. In panel A, we see that the number of new credit report freeze placements spikes in the quarter of the breach announcement for all groups, reaching approximately 80,000 for both non-victims and prior breach victims, and then subsequently declines in the following quarters, though the counts remain elevated relative to the pre-announcement period. Panel B shows that the number of active credit report freezes for each group sees a drastic increase in the quarter of the breach announcement

count was not publicly reported, we contacted the state's attorney general's office or insurance department to request the information.

Table 1: Credit Report Freeze Summary Statistics

	Pre-Breach	Post-Breach
Have Active Freeze Flag		
Full Sample	0.7%	2.8%
Prior Fraud	3.8%	6.4%
Prior Breach	1.0%	3.5%
New Freeze Placement		
Full Sample	0.2%	2.3%
Prior Fraud	1.0%	3.6%
Prior Breach	0.3%	2.7%
Number of Individuals		
Full Sample	12,062,42	
Prior Fraud	38,106	
Prior Breach	3,359,710	
Average freeze length: 5.6 quarters		
Average number of freezes per consumer: 1.2		

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Sample is from Q1:2016 to Q4:2018. The full sample consists of non-victims, prior breach victims, and prior fraud victims. Prior fraud victims are individuals who had filed an extended fraud alert any time between Q1:2010 to Q2:2017. Prior data breach victims are individuals living in states where at least 25% of the total population was affected by the 2015 Anthem data breach. We exclude individuals who fall in both victimization categories.

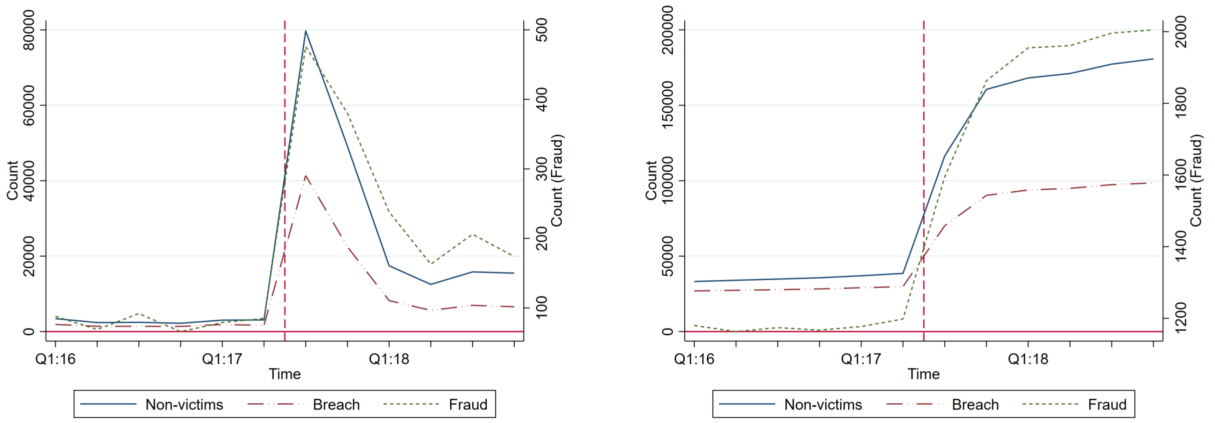
and then continues to grow over time, reflecting the elevated rate of new freeze placements in the post-announcement period.

To explore whether individuals took precautionary actions following the breach, we examine how our freeze variable evolved over time. To do so, we use a standard event study methodology to examine how individuals' adoption of credit report freezes changed in each time period before and after the breach announcement. Specifically, we estimate the following equation from the first quarter of 2016 to the fourth quarter of 2018:

$$y_{it} = \Pi_t + \mathbf{X}_{it}\boldsymbol{\Omega} + \delta_i + \gamma_s + \epsilon_{it}, \tag{1}$$

where y_{it} is the indicator variable for placing a new credit freeze and Π_t is a vector of time dummy variables extending from six quarters before to six quarters after the Equifax breach announcement. Our omitted period is the 2nd quarter of 2017, which means that the estimated effects of the time dummies are relative to the quarter before the breach was announced. We include the county unemployment rate, county share of non-White, county total population, and age bin dummy variables as controls in the vector X_{it}. We also include state fixed effects, γ_s, and individual fixed effects, δ_i. Standard errors are clustered at the

Figure 3: Credit Freezes by Victimization Type Over Time



Panel A: Number of New Freeze Placements

Panel B: Number of Active Freezes

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Prior fraud victims are individuals who had filed an extended fraud alert any time between Q1:2010 to Q2:2017. Prior data breach victims are individuals living in states where at least 25% of the total population was affected by the 2015 Anthem data breach. We exclude individuals who fall in both victimization categories. The left-hand y-axis represents the counts for non-victims and prior breach victims, while the right-hand y-axis represents counts for prior fraud victims.

individual level.

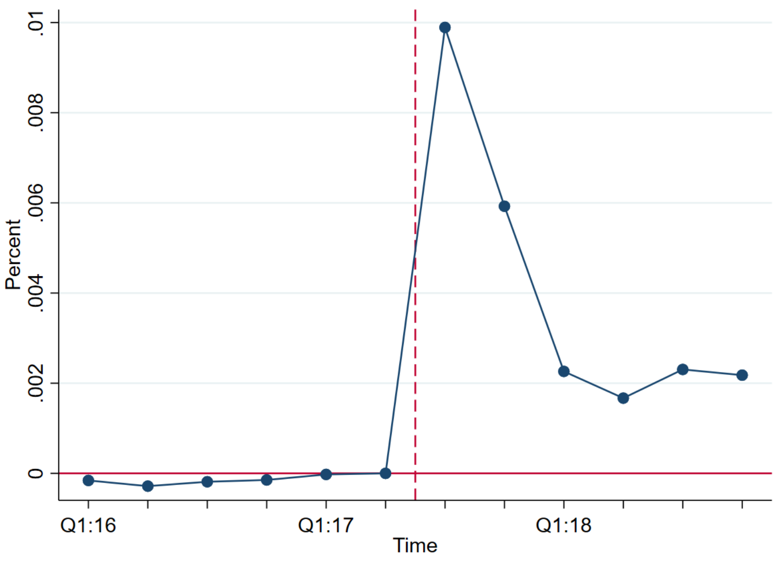
Figure 4 presents the results of our simple event study. The probability an individual would place a new credit freeze on their Equifax credit report increased sharply during the quarter of the breach announcement by 1 percentage point (a relative 142% increase) and remained elevated, though at a lower rate, from the fourth quarter of 2017 through the end of 2018. Overall, the figure shows that consumers took precautionary action in response to the Equifax breach. Interestingly, these general results differ from the prior literature in that we observe persistent, elevated effects for our precautionary effects after the breach announcement. For example, Mikhed and Vogan (2018) found that after a serious data breach in South Carolina in 2012, there was increased uptake of credit freezes, but this only lasted for two quarters after the breach announcement.

6 Past Fraud Exposure and Individuals' Response to the Equifax Breach

Having established that individuals, on average, took precautionary action following the Equifax breach announcement, we now examine how prior exposure to fraud or the risk of fraud (i.e., prior exposure to a data breach or prior fraud victimization) affects individuals'

Figure 4: Individuals' Response to the Equifax Breach

Probability of Having a New Credit Freeze



Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Analysis sample consists of all individuals (prior non-victims, prior breach victims, and prior fraud victims). Dots represent point estimates and bands show 95% confidence intervals.

responses. Specifically, we aim to (1) test if our hypothesis that prior *fraud* victims are more likely to adopt a precautionary measure than prior breach victims and non-victims and (2) examine if prior data breach victims are more or less likely to take up a precautionary measure than non-victims.

6.1 Estimating Effects by Prior Fraud Exposure

To estimate how different types of prior exposure affect precautionary credit market behavior, we examine how each prior exposure group responded to the Equifax data breach announcement relative to our control group of non-victimized individuals in a difference-in-differences (DID) framework. In addition to examining how each prior fraud exposure group responds to the breach announcement relative to non-victims, we also directly compare prior fraud victims to prior breach victims. Based on our conceptual framework presented in Section 3, we may expect prior fraud victims to take up a new precautionary measure at a higher rate than prior breach victims. Our DID estimating equation takes the following form:

$$y_{it} = \alpha_0 + (\mathbf{\Pi_t} \times D_i)\mathbf{\Psi} + \alpha_1 D_i + \Pi_t + \mathbf{X}_{it}\mathbf{\Omega} + \delta_i + \gamma_c + \epsilon_{it}, \tag{2}$$

where $D_i = 1$ if individual i belongs to the prior fraud exposure group and $\mathbf{\Pi_t}$, $\mathbf{X_{it}}$, δ, and γ are as defined in Equation (1). The vector $\mathbf{\Psi}$ contains the coefficients of interest on the interaction terms of the treatment indicator variable D_i and the time dummy variables $\mathbf{\Pi_t}$. We cluster our standard errors at the individual level. The identifying assumption for our DID specification is that absent the Equifax data breach, our outcomes of interest for the treatment and control individuals, conditional on our control variables, would have trended similarly over time. We provide evidence that our outcomes meet the parallel trends assumption in the form of event study plots in Figures 5 to 7. In Table 2, we also report estimates of DID coefficients where we pool the individual time periods into short-run and long-run dummy variables, with the short-run dummy variable equal to one for the two quarters immediately after the announcement and the long-run dummy variable equal to one for the year 2018, which is three to six quarters after the announcement.

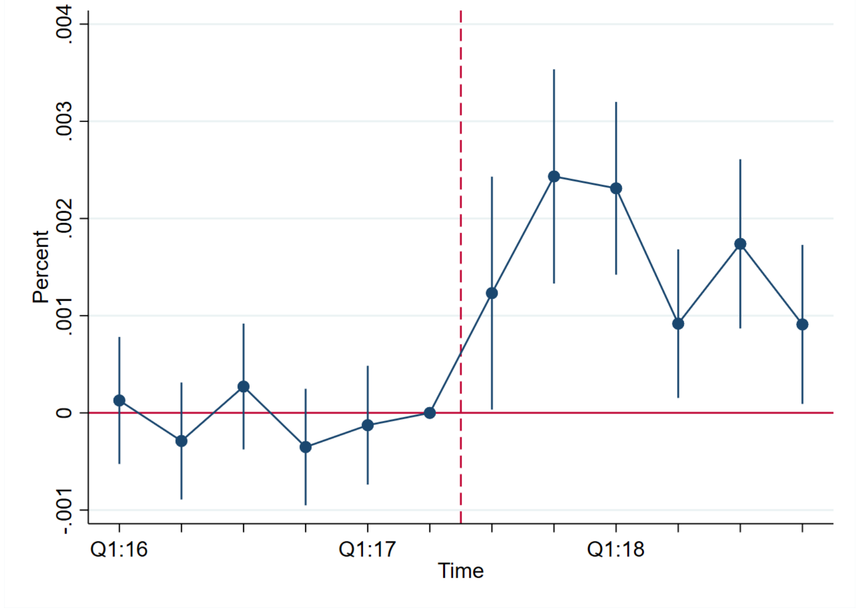
Results from estimating Equation (2) for individuals with prior exposure to fraud are presented in Figure 5. Compared to non-victims, previous fraud victims have a 0.1 percentage point higher likelihood of placing a new credit freeze in their credit report in the quarter immediately after the breach announcement, and this difference increases to 0.25 percentage point by the third quarter after the announcement. Relative to the pre-announcement mean, these estimates indicate that prior fraud victims were 2.6 to 6.6% more likely to place a new credit freeze than prior non-victims. Our DID results in the first column of Table 2 are consistent with these event study results, with the difference in likelihood of having a freeze increasing by a statistical significant 0.2 percentage point in the short-run period and by 0.15 percentage point in the long-run period.

Figure 6 shows the results for individuals who had been previously exposed to the 2015 Anthem breach relative to non-victims. We can see that the likelihood of placing a credit report freeze increases by 0.3 percentage point (a relative 30% increase) in the quarter of the breach announcement for prior breach victims relative to prior non-victims, which is three times larger than the estimate for prior fraud victims relative to prior non-victims. This increase in probability remains elevated for the following two quarters, but it returns to zero by the end of our sample period.

Our DID results in the second column of Table 2 show similar results. For prior breach victims, the likelihood of a new credit report freeze increases by 0.2 percentage point in the short-run period and increases by 0.01 percentage point in the long-run period. While prior breach victims have a higher likelihood of having a new credit freeze (relative to prior non-victims) by the same fraction of a percentage point as prior fraud victims in the short run, as shown in Panel A, the increase is of different economic magnitude for the two groups: The 0.2 percentage point increase represents an increase of an additional 130,000 new credit

Figure 5: Equifax Breach Results: Prior Fraud Victims vs. Non-Victims

Probability of Having a New Credit Freeze



Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Analysis sample consists of non-victims and prior fraud victims. Dots represent point estimates and bands show 95% confidence intervals.

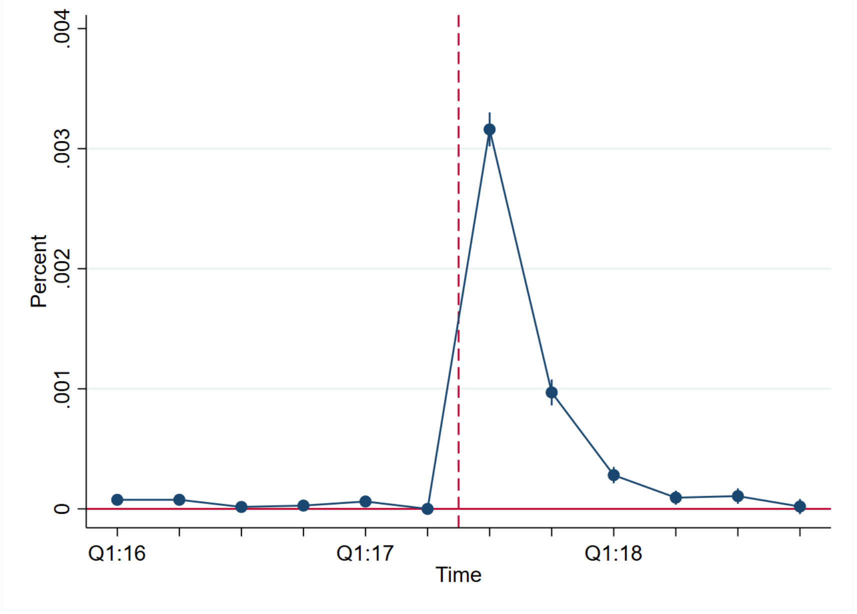
freezes for prior breach victims, whereas the 0.2 percentage point increase for prior fraud victims translates to approximately 1,500 new freezes.

In Figure 7, we directly compare prior fraud victims to prior breach victims to see if their responses to the Equifax breach are statistically different from each other. To do this, we redefine D_i in Equation (2) so that $D_i = 1$ if an individual was a prior ID theft victim and $D_i = 0$ if an individual was a prior breach victim. In the quarter of the announcement (Q3 2017), previous breach victims have a higher likelihood of placing a freeze relative to previous fraud victims by 0.2 percentage point. However, in the quarters after the announcement, the effect reverses and prior fraud victims have a relative higher likelihood of placing a freeze than previous breach victims until the end of our sample. This immediate reversal is consistent with the summary statistics, where prior fraud victims have a higher rate of freeze placement than prior breach victims.

Our short-run and long-run DID coefficients in the third column of Table 2, where we pool all post-breach time periods into two separate post-period dummy variables, are more precisely estimated and indicate that prior fraud victims have a 0.2 percentage point higher likelihood of having a credit freeze in the long-run period.

Figure 6: Equifax Breach Results: Prior Breach Victims vs. Non-Victims

Probability of Having a New Credit Freeze



Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Analysis sample consists of non-victims and prior breach victims. Dots represent point estimates and bands show 95% confidence intervals.

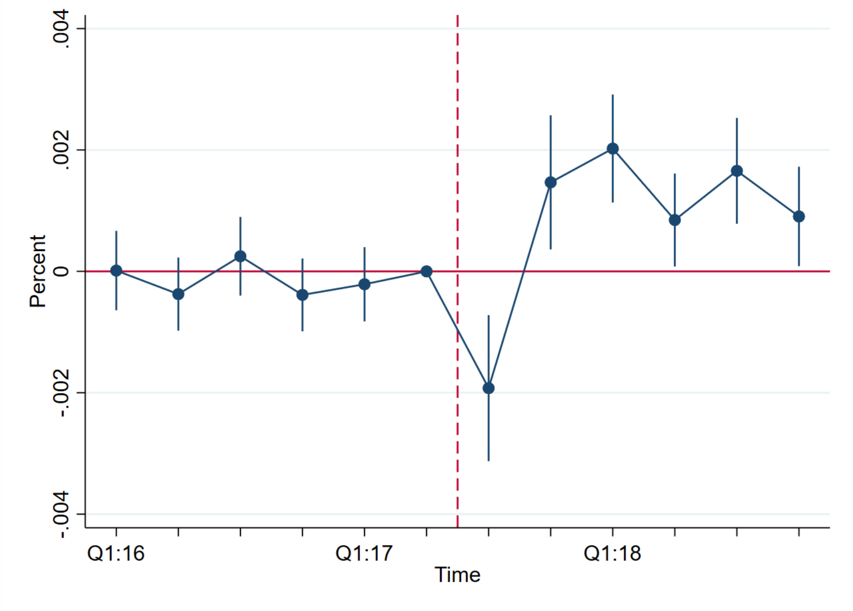
Our estimates from Figures 5 to 7 and Table 2 are consistent with our conceptual framework, which predicts that prior fraud victims are more likely to adopt a protective measure than prior breach victims and prior non-victims. Further, our estimates from Figure 6 show that prior breach victims are more likely to adopt a protective action than prior non-victims, which corresponds to the scenario where the effect of past data breach exposure on the cost of adopting the protective action outweighs the effect on perceived fraud risk.

Overall, the magnitudes of our effect sizes, while statistically significant, are also consistent with the previous literature that, in aggregate, many individuals do not take precautionary actions in response to data breaches. In addition, the persistence of our results, when compared to the previous literature (e.g., Mikhed and Vogan, 2018), shows that individuals with prior exposure to fraud had a more persistent precautionary response to the Equifax data breach when compared to prior data breaches.

6.2 Long-Run Effects of Exposure to the Equifax Breach

One notable result from Figure 4 and Table 2 is that the likelihood of placing a new freeze on a credit report persists multiple quarters after the announcement of the Equifax data

Figure 7: Equifax Breach Results: Prior Fraud Victims vs. Prior Breach Victims



Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Results are for prior fraud victims relative to prior data breach victims (the control group). Dots represent point estimates and bands show 95% confidence intervals.

Table 2: Difference-in-Difference Results; Probability of a New Freeze

	Prior Fraud vs. Non–Victims	Prior Breach vs. Non–Victims	Prior Fraud vs. Prior Breach
Treat × *Short–run*	0.0019***	0.0020***	-0.0001
	(0.0004)	(0.0000)	(0.0004)
Treat × *Long–run*	0.0015***	0.0001***	0.0015***
	(0.0002)	(0.0000)	(0.0002)
Pre-period sample mean = 0.007			
N	101,985,621	140,901,416	39,820,443

Note: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. *Short–run* = 1 for the time period Q3:2017 to Q4:2017 and *Long–run* = 1 for the time period Q1:2018 to Q4:2018. *** p<0.01, **p < 0.05, *p < 0.1.

breach. Given the results of previous studies (e.g., Mikhed and Vogan (2018), it is unlikely that individuals freeze their credit reports *in response* to the Equifax breach after so much time has elapsed. Instead, the persistence of the increased likelihood of freeze placement is consistent with a long-term change in individuals' precautionary behavior in credit markets.

Based on our theoretical framework, the Equifax data breach can be classified as a 'near-miss' experience for affected individuals: While individuals' information was exposed, it does not appear that the information has been used for fraud (Benner, 2020). As we discussed in Section 3, the experience of a near miss can have two opposing effects on individuals' precautionary behavior: It may simultaneously lower individuals' perceived fraud risks and their (non-pecuniary) cost of adopting the precautionary measure. The persistently higher likelihood of freeze placement suggests that the effect of the Equifax breach on the cost of placing a credit freeze is large relative to its effect on perceived fraud risks. We conjecture that the relatively large *decrease* in the cost of placing a credit freeze resulted from the extensive media coverage, especially outside of normal news channels, on the breach and the actions individuals could take to protect themselves from the fraud risks associated the breach, which increased the awareness of credit freezes among the general public.

In Figure 8, we plot Google search trends for "credit freeze" in the U.S. from January 2016 to July 2019. We omit the time around the Equifax breach for scaling purposes.[15] As can be seen from the figure, search intensity for "credit freeze" remains significantly elevated in the two years after the breach announcement, which supports our conjecture.

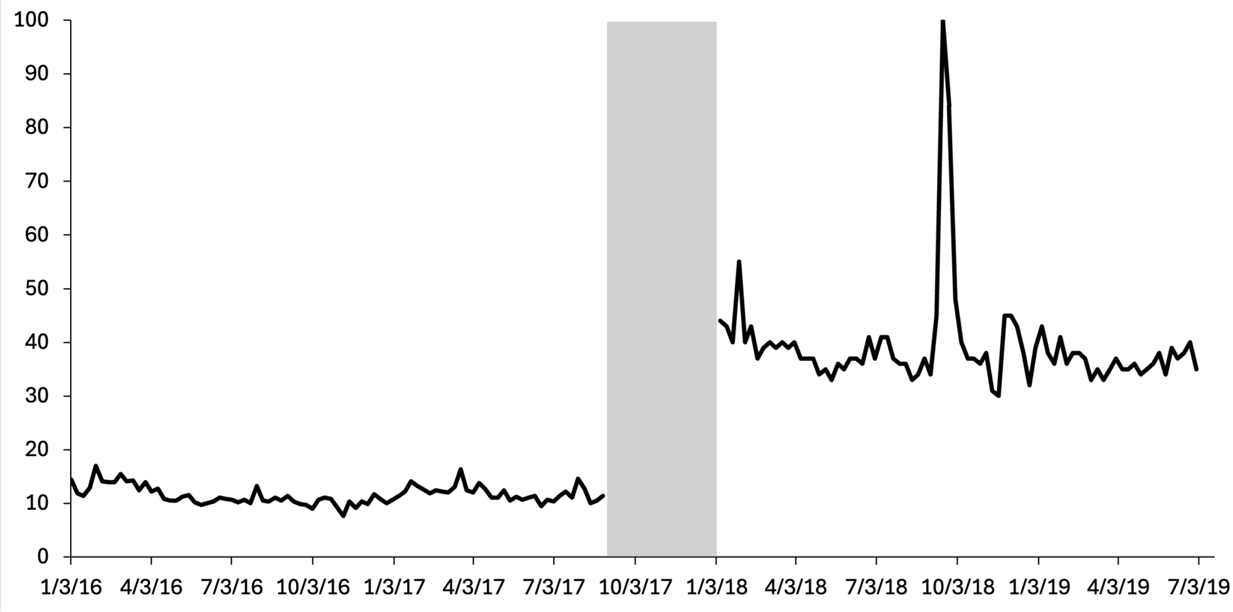
6.3 Other Types of Precautionary Measures

While credit report freezes prevent criminals from using individuals' credit information to open new accounts, they don't prevent criminals from using existing accounts. To reduce the likelihood of having an existing account misused, individuals may close or stop using certain accounts to reduce monitoring costs and/or exposing information online. While not a direct indicator of precaution by itself, changes in card closures could provide supporting evidence that individuals increased their precaution following the Equifax breach. To examine card closures, we construct a variable that counts the number of credit card accounts an individual closes in each quarter; details on the construction of the closed bankcard account variable are provided in Appendix B. Results for closed cards are presented in Appendix Figure A2.

Panel A of Figure A2 shows prior fraud victims and non-victims closed around the same number of accounts before and after the breach announcement. In contrast, panel B shows prior breach victims closed fewer accounts than non-victims after the breach announcement, with a decline of 0.002 account (a relative 5% decline) in the quarter immediately after the breach. This downward trend continues through the remaining five post-breach quarters. Panel C of Figure A2 shows that prior fraud victims and prior breach victims also closed

[15] Because of the large and sudden increase in Google searches for "credit freeze" following the Equifax breach (see Figure 8), including the time period around the breach masks variation across time in the search term.

Figure 8: Google Search Interest for the Term "Credit Freeze" over Time



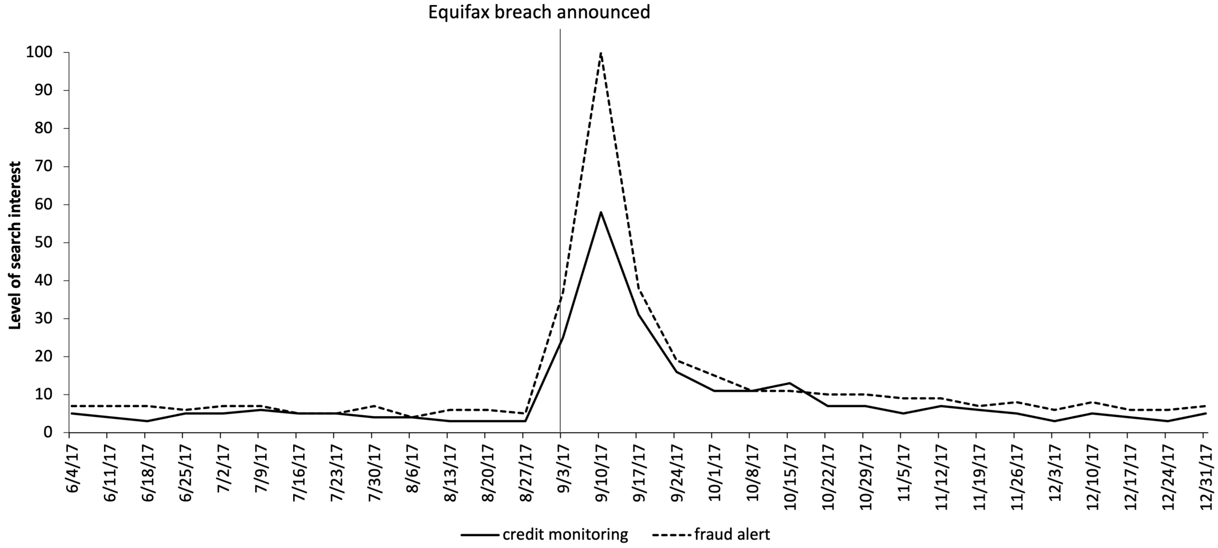
Notes: Authors' calculations using data from Google trends from January 2016 through June 2019. Data from September 2017 through December 2017 (gray region) have been omitted. Scale represents search interest relative to the highest point on the chart for the given time period. The spike in search interest that occurred around the end of September 2018 is likely attributable to the passage of the Economic Growth, Regulatory Relief, and Consumer Protection Act, which made credit freezes free for consumers.

about the same number of accounts in the quarters before the breach announcement but prior fraud victims closed 0.003 more account (a relative 7.5% increase) on average than prior breach victims in the quarters after the breach announcement. However, we note that our event study coefficients are estimated noisily, and we cannot rule out a zero effect.

In addition to direct actions that affect credit outcomes, individuals can adopt other types of precautionary measures, such as purchasing credit monitoring services or signing up for initial fraud alerts. These measures are more passive and do not prevent fraud from occurring: They are designed to report potentially suspicious activity, allowing individuals to take actions to prevent further fraud from occurring. This is in comparison to credit report freezes or closing credit card accounts, which are more proactive measures that can potentially prevent fraud from occurring in the first place. We provide more details on these two measures in Appendix C.

Although we are unable to analyze the adoption of credit monitoring services and initial fraud alerts in our paper, we find evidence that consumers may have adopted these measures using Google trends data. Figure 9 shows a spike in the volume of Google searches for the terms "credit monitoring" and "fraud alert" in the week following Equifax's data breach

Figure 9: Google Search Interest Over Time: Credit Monitoring and Fraud Alert



Notes: Authors' calculations using data from Google trends from June 2017 to December 2017. Scale represents search interest relative to the highest point on the chart for the given time period.

announcement. These search trends suggest that consumers were seeking information on these precautionary measures after the breach announcement and as a result may have implemented some of them.

6.4 Heterogeneity Analysis

Although a credit report freeze can help prevent fraud, having a frozen credit report is not costless. Freezes, by design, make it more difficult to open new credit accounts. Therefore, we may expect individuals who are shopping for credit or expect to need credit in the near-future to be less likely to freeze their credit report or to delay freezing their credit report until after they have obtained the credit they need. We may also expect this heterogeneity to differ by prior victimization status: Prior fraud victims may better anticipate the frictions imposed by credit freezes than prior breach victims and non-victims, as they are more likely to have placed credit freezes in the past. For those prior fraud victims who are seeking credit, we may expect them to delay freezing their credit report.

To examine how individuals in each prior exposure group differ in their likelihood of placing a credit freeze by credit shopping behavior, we divide the sample in two categories: Individuals who had at least one credit inquiry in the quarter prior to the Equifax announcement and individuals who did *not* have any credit inquiries in the quarter before the breach announcement. We then re-estimate our DID regressions from Equation (2) for each category and each prior exposure group. Results are shown in Figure A3.

In Panel A, we compare prior fraud victims to non-victims separately by inquiry status. It is clear that for the no inquiry group (the red dashed line), prior fraud victims have a relatively higher likelihood of placing a freeze compared to non-victims in the quarters after the breach announcement, similar to our main results. For individuals with inquiries, we observe no differences in the likelihood of freezing between prior fraud victims and non-victims except in the second quarter *after* the breach announcement. This implies that credit shopping behavior matters for prior fraud victims taking up precautionary action.

In Panel B, we compare prior breach victims to non-victims by inquiry status. Unlike the results in Panel A, the likelihood that prior breach victims place a credit freeze relative to non-victims is similar across inquiry categories. This suggests that credit shopping behavior does not impact take-up of precautionary measures for prior breach victims.

We then compare prior fraud victims to prior breach victims for each inquiry category in Panel C. For the inquiry group, prior fraud victims have a relatively lower likelihood of placing a credit report freeze than prior breach victims in the quarter of the breach announcement. However, in the quarters after the breach announcement, the likelihood of placing a freeze is relatively similar or higher for prior fraud victims than for prior breach victims. For the no inquiry group, we observe no difference in the likelihood of freezing between prior fraud victims and prior breach victims in the quarter of the breach announcement, but we see a relative increase in the freeze likelihood for prior fraud victims in all subsequent quarters. Overall, these results suggest that for prior fraud victims, credit demand leads to less take-up, at least initially, of precautionary actions.

7 Credit Market Consequences of Freezing

In the previous section, we provide clear evidence that some consumers placed credit report freezes in the quarters after the announcement of the Equifax breach, and that the response differed by prior victimization category. Because credit report freezes mechanically introduce a friction in the credit market, we may expect to see a difference in credit market behavior and outcomes between individuals who froze their credit reports (freezers) and those who did not (non-freezers) following the announcement. Further, the difference in credit market outcomes between freezers and non-freezers may vary across prior exposure group, as the type of prior exposure (or lack thereof) may affect the level of sophistication in managing the friction introduced by credit freezes.

To examine how consumers' credit market outcomes change after the breach announcement, we first estimate simple event study regressions similar to those in Section 5 for four broad measures of credit market activity. This allows us to compare these credit outcomes across our prior fraud exposure categories before and after the announcement. We then examine how these outcomes evolved separately for individuals who froze their credit report in response to the breach announcement and for individuals who did not freeze their credit report. While we cannot draw any causal conclusion as to why differences between freezers and non-freezers exist, we are able to document that the two groups have significantly different credit outcomes in the post-breach period.

7.1 Consumer Credit Outcomes After the Breach Announcement

To study how consumer credit outcomes were impacted by the Equifax breach announcement, we look at four broad measures of credit market activity: the number of credit inquiries, the number of all credit accounts, the total credit balance on all accounts, and the total credit limit on all accounts. Summary statistics for these variables are reported in Appendix Table A2. We first follow the empirical strategy outlined in Section 5.3 and estimate Equation (1) for each credit outcome. Results from the simple event study model for each exposure group are presented in Appendix Figures A4-A6.

Unlike the event study result for new freeze placements in Figure 4, each of the four credit variables, for each exposure group, exhibits clear secular trends over our sample period. Inquiries exhibit a downward trend across the three exposure groups, while the number of accounts, total balances, and total credit limits display consistent upward trends over time. We observe no evidence of a trend break in any of the four credit variables in the quarters after the breach announcement.

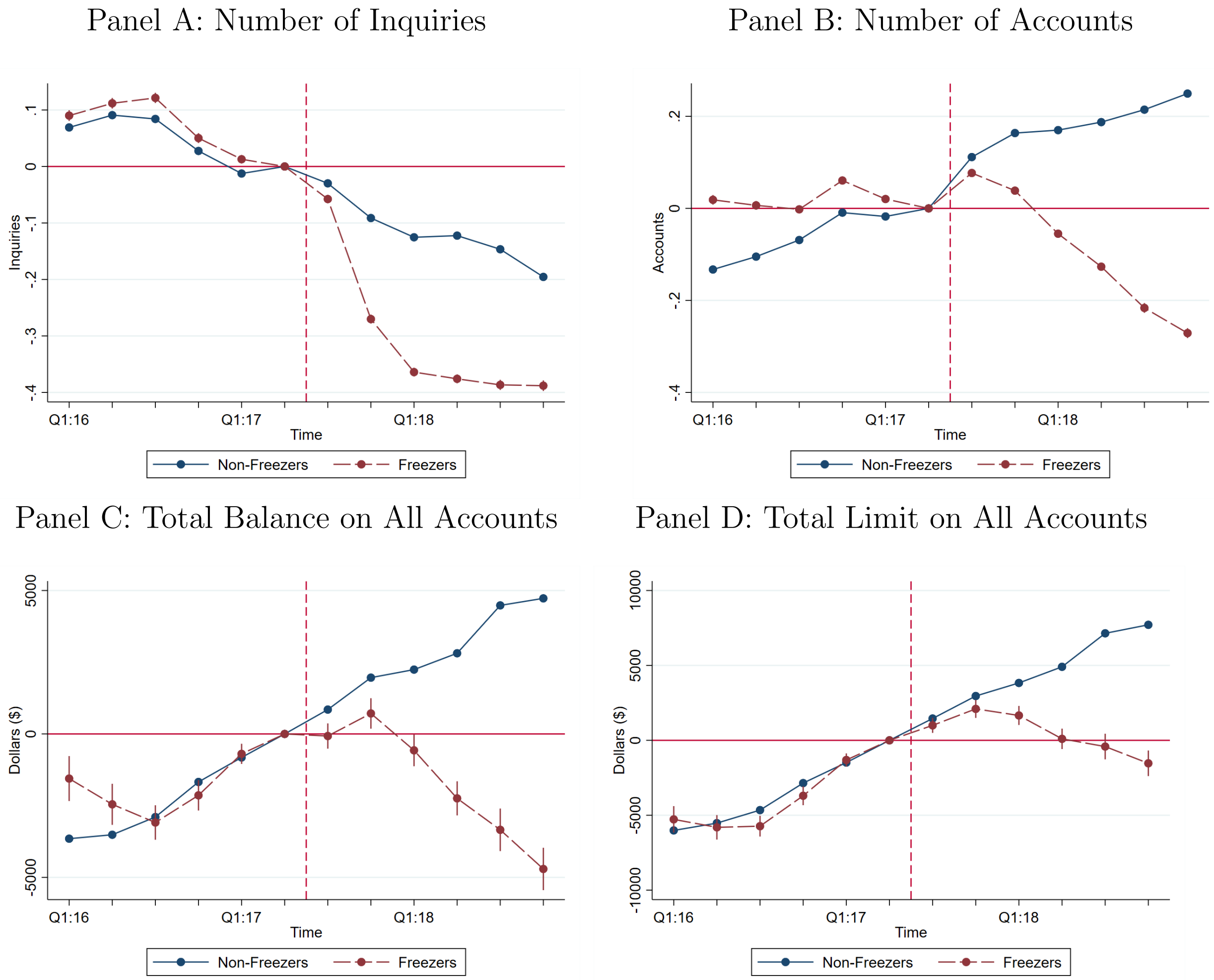
We also compare each prior victim group to prior non-victims and prior fraud victims to prior breach victims using the DID framework in Equation (2) to examine if there were any differences in our credit variables across groups. Results are shown in Appendix Figures A7-A9. None of the credit variables exhibit parallel trends in the pre-period, so we do not view any of these estimates as causal. We discuss the results of these regressions in further detail in Appendix D.

7.2 Consumer Credit Outcomes by Freeze Status

To illustrate the credit market consequences of a credit report freeze, we estimate Equation (1) for each of our four credit outcome variables separately for freezers and non-freezers. Event study results for each prior exposure group are presented in Figures 10-12.

We first examine the effect of credit report freezes for non-victims in Figure 10. We can see that non-victims who froze their credit reports have significantly fewer inquiries (panel A)

Figure 10: Equifax Breach: Freeze vs. Non-Freeze; Non-Victims



Panel A: Number of Inquiries

Panel B: Number of Accounts

Panel C: Total Balance on All Accounts

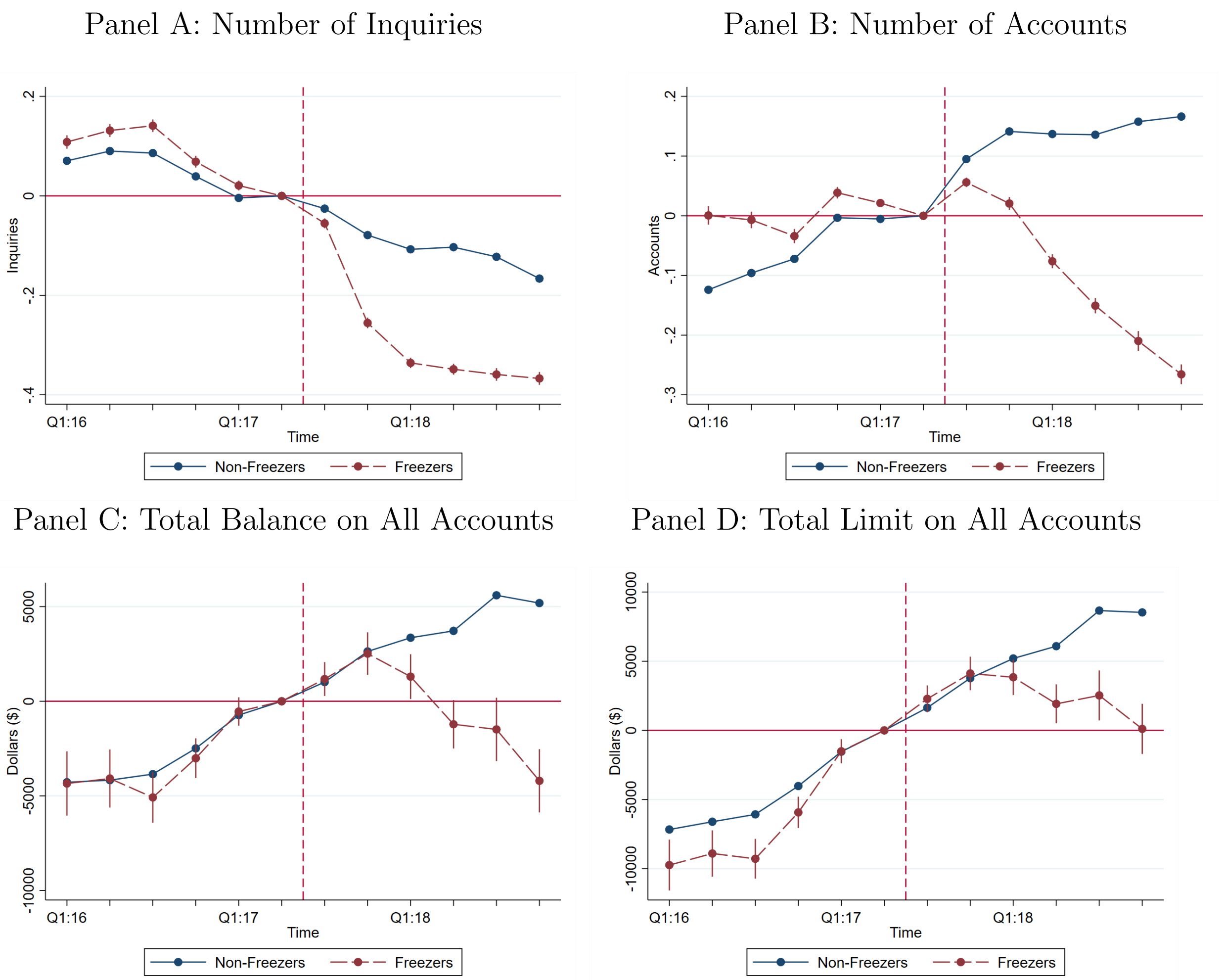
Panel D: Total Limit on All Accounts

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Freezers are individuals who froze their credit report in either Q3 or Q4 of 2017 and kept their freeze on for the remainder for the sample. Non-freezers never placed a credit report freeze during the same period.

and total accounts (panel B) than non-victims who did not freeze post-breach announcement. Within two quarters of the breach announcement, freezers have approximately 0.25 fewer inquiry and 0.28 fewer account than non-freezers. Along with fewer inquiries and accounts, freezers have lower balances (panel C) and credit limits on all accounts (panel D). By the end of our sample period in Q4:2018, freezers have approximately $9,000 less in total balances and total limits than non-freezers.

Results for prior breach victims are reported in Figure 11. Similar to prior non-victims, prior breach victims who froze their credit reports have fewer inquiries and fewer total accounts than non-freezers. Freezers have approximately 0.2 fewer inquiry within three quarters of the breach announcement and 0.3 fewer account. By the end of the sample

Figure 11: Equifax Breach: Freeze vs. Non-Freeze; Prior Breach Victims


Panel A: Number of Inquiries

Panel B: Number of Accounts

Panel C: Total Balance on All Accounts

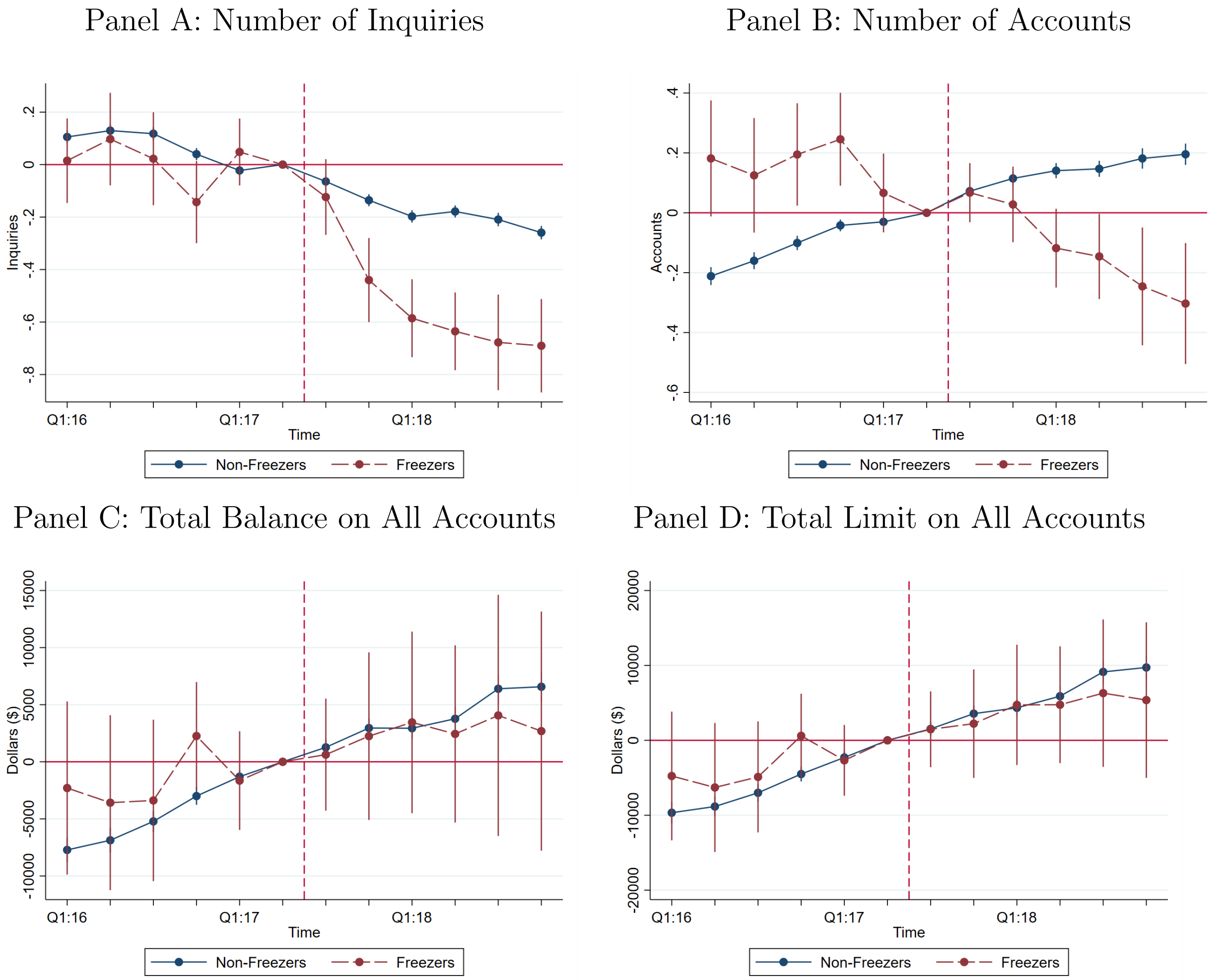
Panel D: Total Limit on All Accounts

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Freezers are individuals who froze their credit report in either Q3 or Q4 of 2017 and kept their freeze on for the remainder for the sample. Non-freezers never placed a credit report freeze during the same period.

in Q4:2018, the total number of accounts for freezers and non-freezers differ by over 0.4 account. Total account balance and total credit limit are also lower for freezers than non-freezers post-breach announcement. As can be seen in panels C and D, total balances and total credit limits were approximately $9,000 lower for freezers by the end of the sample period in Q4:2018. For both variables, the gap between freezers and non-freezers starts more modestly in Q1:2018, but grew significantly over the remainder of the sample period.

For prior fraud victims, we can see in Figure 12 that prior fraud freezers had significantly fewer credit inquiries (panel A) and fewer total accounts (panel B) than non-freezers. Within three quarters of the breach announcement, prior fraud victims who froze their credit report have 0.26 fewer inquiry and 0.22 fewer account than prior fraud victims who did not freeze.

Figure 12: Equifax Breach: Freeze vs. Non-Freeze; Prior Fraud Victims


Panel A: Number of Inquiries

Panel B: Number of Accounts

Panel C: Total Balance on All Accounts

Panel D: Total Limit on All Accounts

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Freezers are individuals who froze their credit report in either Q3 or Q4 of 2017 and kept their freeze on for the remainder for the sample. Non-freezers never placed a credit report freeze during the same period

Despite victims having fewer inquiries and total accounts, total debt balance and total credit limit do not differ by freeze status, with both variables growing over the sample period at similar rates for both groups.

We observe from Figures 10-12 that the differences in number of inquiries and number of accounts between freezers and non-freezers and their evolution over time post-breach announcement are qualitatively similar for all three prior exposure groups. These differences across the three exposure groups are mostly mechanical in nature—a credit report freeze, by design, prevents lenders from conducting hard inquiries on an individuals' credit report, which is necessary for opening new credit accounts. Therefore, it is natural for non-freezers to have more inquiries and acquire new accounts at a faster rate than freezers, contributing to a widening difference in the number of accounts between non-freezers and freezers. We note that a lower rate of account closures among non-freezers relative freezers could also contribute to the difference in the number of accounts we observe; however, in results not shown, we find no evidence that freezers and non-freezers close accounts at different rates, which suggests the difference in the number of accounts is largely a direct consequence of placing credit freezes.

For total balance and total limit, the differences between non-freezers and freezers in both the prior non-victim and prior breach victim groups widen in the quarters after the breach announcement, with both variables increasing over time for non-freezers and decreasing over time for freezers. These results are unsurprising, given the decline in the number of accounts for freezers over time in the post-breach announcement period. However, total balance and total limit for non-freezers and freezers in the prior fraud group do *not* differ significantly post-breach announcement; both variables grew over time for non-freezers and freezers. This is despite the fact that the difference in the number of accounts and inquiries between prior fraud freezers and non-freezers is similar to the differences between freezers and non-freezers for individuals in the prior breach victims and non-victims groups.

One possible explanation for why freezers in the prior fraud group differ from those in the prior non-victim and prior breach groups is their higher ability to manage their credit access around a credit freeze. As we conjectured in our conceptual framework, prior fraud victims are likely to have more knowledge of and practical experience with credit freezes. One way of demonstrating this is by identifying freezers in the prior fraud group are more likely to 'toggle' their credit report freeze—unfreezing (for instance, to apply for new credit) and then refreezing their credit report—which is a strong sign of consumer familiarity with credit report freezes. We calculate that approximately 56.7% of freezers in the prior fraud victim group toggle their credit freeze, as compared to 19.3% in the prior breach victim group and 16.7% in the non-victim group.

We further examine whether the differences in credit outcomes between freezers and non-freezers post-breach announcement affected their financial health by examining credit scores.[16] In Appendix Figure A10, we show changes in credit scores for freezers and non-freezers for each prior exposure group. For all three exposure groups, credit scores for freezers and non-freezers do not differ significantly across the sample period. This result is somewhat surprising for the prior non-victims and prior breach victim groups, as freezers in those groups experienced a decrease in total credit limit post-breach announcement, which would lower credit scores if credit utilization increased. A possible explanation for why credit scores of freezers in those groups did not decrease relative to credit scores of non-freezers

[16] The credit score we use is the Equifax Risk Score.

is that the effect of the fall in credit limits was offset by the fall in credit utilization, as indicated by the decrease in total balances.

Overall, regardless of prior fraud exposure status, individuals who freeze have fewer credit inquiries and total accounts than individuals who do not freeze post-breach announcement. However, the effect of having a credit freeze on total credit balances and limits does differ by prior fraud exposure status: Prior non-victims and prior breach victims who froze their credit reports have lower balances and limits than non-freezers, while prior fraud victims have similar balances and limits regardless of freeze status. Despite these differences in credit outcomes, individuals who freeze do not have worse financial health, as measured by credit scores, than individuals who do not freeze, despite the decline in available credit. This suggests that taking precautionary action, while reducing credit, does not harm individuals financially.

8 Conclusion

This paper examines the effect of prior fraud and data breach exposure on future precautionary behavior in credit markets by exploiting the 2017 Equifax data breach, which exposed sensitive information for over 70% of the U.S. adult population. To guide our analysis, we first develop a descriptive model of credit market precautionary behavior, which enables us to formulate theoretically founded hypotheses on how past experiences with fraud risk may affect individuals' precautionary responses to a future data breach. We test our hypotheses using a DID framework and large anoynomized data set of consumer credit records. We find that, consistent with our hypothesis, individuals who previously experienced fraud have a higher probability of placing a credit freeze following the announcement of the Equifax breach relative to individuals who had previously experienced a data breach and non-victims. Further, prior breach victims were more likely to have taken precautionary action than non-victims, which corresponds to the scenario where the reduction in the cost of adopting a precautionary measure due to learning outweighs the negative effect of the near-miss experience (i.e., experiencing the Anthem data breach but not fraud) on perceived fraud risk arising from the Equifax breach.

When analyzing the credit outcomes for individuals who take up a precautionary measure, we find that individuals who froze their credit reports in response to the Equifax breach announcement have less credit relative to individuals who did not freeze their credit reports. However, these results are not homogeneous across prior victimization types. While all freezers see fewer inquiries and total number of accounts after adopting a credit report freeze, non-victims and prior breach victims also see lower total credit balances and limits;

prior fraud victims who freeze, on the other hand, do not experience the decline in balances and limits. This is consistent with our conceptual framework, where prior fraud victims have the most experience dealing with credit bureaus and likely have the sophistication to 'toggle' their credit freeze so they can maintain the levels of credit they need.

Although prior fraud and data breach victims were more likely to freeze their credit reports than previously unexposed individuals, the vast majority of these individuals did not do so. Thus, while past fraud exposure likely increased awareness and knowledge and decreased the cost of credit freezes, our results suggest that the cost of placing a freeze continued to outweigh the perceived benefit for most prior victims. One possible explanation for this finding is that the perceived fraud risk resulting from a data compromise, and hence the perceived benefit of adopting precautionary measures, is relatively low. A low perceived fraud loss could arise because of cognitive errors and biases or a low (objective) probability of fraud arising from data compromises or both. It may be the case that even if individuals were perfectly informed about the true fraud risk of data compromises, a majority would still not adopt precautionary measures because their incentive to do so is relatively weak. Consumer protection agencies may thus have a role to play in improving individuals' understanding of fraud risks and losses they could face from a breach of their personal data, and the potential benefits of taking precuationary actions.

References

Agarwal, S., P. Ghosh, T. Ruan, and Y. Zhang (2024). Transient customer response to data breaches of their information. *Management Science 70*(6), 4105–4114.

Andersson, P., R. L. Sjöberg, J. Öhrvik, and J. Leppert (2009). Effects of family history and personal experience of illness on inclination to change health related behavior. *Central European Journal of Public Health 17*(1), 3–7.

Averdijk, M. (2011). Reciprocal effects of victimization and routine activities. *Journal of Quantitative Criminology 27*, 125–149.

Baer, H. J., P. Brawarsky, M. F. Murray, and J. S. Haas (2010). Familial risk of cancer and knowledge and use of genetic testing. *Journal of General Internal Medicine 25*(7), 717–724.

Becker, J. S., D. Paton, D. M. Johnston, K. R. Ronan, and J. McClure (2017). The role of prior experience in informing and motivating earthquake preparedness. *International Journal of Disaster Risk Reduction 22*, 179–193.

Benner, K. (2020). U.S. charges Chinese military officers in 2017 Equifax hacking. *The New York Times*.

Blascak, N., J. Cheney, R. Hunt, V. Mikhed, D. Ritter, and M. Vogan (2025). Financial fraud through the lens of extended fraud alerts. Working Paper 25-29, Federal Reserve Bank of Philadelphia.

Bogani, A., G. Faccenda, P. Riva, J. Richetin, L. Pancani, and S. Sacchi (2023). The near-miss effect in flood risk estimation: A survey-based approach to model private mitigation intentions into agent-based models. *International Journal of Disaster Risk Reduction 89*, 103629.

Brodkin, J. (2007, April). Victims of Choicepoint data breach didn't take advantage of free offers. Available at https://www.networkworld.com/article/2297654/victims-of-choicepoint-data-breach-didn-t-take-advantage-of-free-offers.html.

Cody, R. and C. Lee (1990). Behaviors, beliefs, and intentions in skin cancer prevention. *Journal of Behavioral Medicine 13*, 373–389.

Dillon, R. L., C. H. Tinsley, and M. Cronin (2011). Why near-miss events can decrease an individual's protective response to hurricanes. *Risk Analysis: An International Journal 31*(3), 440–449.

Dooley, D., R. Catalano, S. Mishra, and S. Serxner (1992). Earthquake preparedness: predictors in a community survey 1. *Journal of applied social psychology 22*(6), 451–470.

Dugan, L. (1999). The effect of criminal victimization on a household's moving decision. *Criminology 37*(4), 903–930.

Fein, S. B., C.-T. J. Lin, and A. S. Levy (1995). Foodborne illness: perceptions, experience, and preventive behaviors in the United States. *Journal of food protection 58*(12), 1405–1411.

Finucane, M. L., A. Alhakami, P. Slovic, and S. M. Johnson (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making 13*(1), 1–17.

Finucane, M. L. and J. L. Holup (2006). Risk as value: Combining affect and analysis in risk judgments. *Journal of Risk Research 9*(2), 141–164.

Giannetti, M. and T. Yue Yang (2016). Corporate scandals and household stock market participation. *Journal of Finance 71*(6), 2591–2636.

Gurun, U. G., N. Stoffman, and S. E. Yonker (2018). Trust busting: The effect of fraud on investor behavior. *Review of Financial Studies 31*(4), 1341–1376.

Hamdi, N., A. Kalda, and D. Sovich (2024). The costs of financial fraud victimization. Working Paper.

Harell, E. and A. Thompson (2023, October). Victims of identity theft, 2021. Available at https://bjs.ojp.gov/document/vit21.pdf.

Hertwig, R., G. Barron, E. U. Weber, and I. Erev (2004). Decisions from experience and the effect of rare events in risky choice. *Psychological Science 15*(8), 534–539.

Holtgrave, D. R. and E. U. Weber (1993). Dimensions of risk perception for financial and health risks. *Risk Analysis 13*(5), 553–558.

Institute, P. (2014). The aftermath of a data breach: Consumer sentiment. Available at https://www.ponemon.org/research/ponemon-library/security/the-aftermath-of-a-data-breach-consumer-sentiment.html.

Jackson, E. L. (1981). Response to earthquake hazard: The West Coast of North America. *Environment and Behavior 13*(4), 387–416.

Knüpfer, S., V. Rantala, E. Vihriälä, and P. Vokata (2024). Household responses to phantom riches. Fisher College of Business Working Paper No. 2021-03-008.

Lee, D. and W. van der Klaauw (2010). An Introduction to the FRBNY Consumer Credit Panel. Staff Report 479, Federal Reserve Bank of New York.

Lillian, A., P. Heaton, D. C. Lavery, and S. Romanosky (2016). *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information.* RAND Corporation.

Lindell, M. K. and S. N. Hwang (2008). Households' perceived personal risk and responses in a multihazard environment. *Risk Analysis: An International Journal 28*(2), 539–556.

Lindell, M. K. and R. W. Perry (2012). The protective action decision model: Theoretical modifications and additional evidence. *Risk Analysis: An International Journal 32*(4), 616–632.

Loewenstein, G. F., E. U. Weber, C. K. Hsee, and N. Welch (2001). Risk as feelings. *Psychological Bulletin 127*(2), 267.

Mayer, P., Y. Zou, B. M. Lowens, H. A. Dyer, K. Le, F. Schaub, and A. J. Aviv (2023). Awareness, intention,(in) action: individuals' reactions to data breaches. *ACM Transactions on Computer-Human Interaction 30*(5), 1–53.

McKenna, D., Y. Faustini, J. Nowakowski, and C. P. Wormser (2004). Factors influencing the utilization of Lyme disease-prevention behaviors in a high-risk population. *Journal of the American Association of Nurse Practitioners 16*(1), 25–31.

Mikhed, V. and M. Vogan (2018). How data breaches affect consumer credit. *Journal of Banking & Finance 88*, 192–207.

Mouchawar, J., T. Byers, G. Cutter, M. Dignan, and S. Michael (1999). A study of the relationship between family history of breast cancer and knowledge of breast cancer genetic testing prerequisites. *Cancer Detection and Prevention 23*(1), 22–30.

Nowak, G. J., K. Sheedy, K. Bursey, T. M. Smith, and M. Basket (2015). Promoting influenza vaccination: insights from a qualitative meta-analysis of 14 years of influenza-related communications research by US Centers for Disease Control and Prevention (CDC). *Vaccine 33*(24), 2741–2756.

Peacock, W. G. (2003). Hurricane mitigation status and factors influencing mitigation status among Florida's single-family homeowners. *Natural Hazards Review 4*(3), 149–158.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology 91*(1), 93–114.

Romanosky, S., R. Telang, and A. Acquisti (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management 30*(2), 256–286.

Rountree, P. W. and K. C. Land (1996). Burglary victimization, perceptions of crime risk, and routine activities: A multilevel analysis across Seattle neighborhoods and census tracts. *Journal of Research in Crime and Delinquency 33*(2), 147–180.

Siegrist, M. and H. Gutscher (2006). Flooding risks: A comparison of lay people's perceptions and expert's assessments in Switzerland. *Risk Analysis 26*(4), 971–979.

Siegrist, M. and H. Gutscher (2008). Natural hazards and motivation for mitigation behavior: People cannot predict the affect evoked by a severe flood. *Risk Analysis: An International Journal 28*(3), 771–778.

Slovic, P., M. L. Finucane, E. Peters, and D. G. MacGregor (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis 24*(2), 311–322.

Tinsley, C. H., R. L. Dillon, and M. A. Cronin (2012). How near-miss events amplify or attenuate risky decision making. *Management Science 58*(9), 1596–1613.

Turjeman, D. and F. M. Feinberg (2019). When the data are out: Measuring behavioral changes following a data breach. Working Paper, SSRN 3427254.

Tversky, A. and D. Kahneman (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology 5*(2), 207–232.

Van der Linden, S. (2014). On the relationship between personal experience, affect and risk perception: The case of climate change. *European Journal of Social Psychology 44*(5), 430–440.

Weinstein, N. D. (1989). Effects of personal experience on self-protective behavior. *Psychological bulletin 105*(1), 31.

Zaleskiewicz, T., Z. Piskorz, and A. Borkowska (2002). Fear or money? Decisions on insuring oneself against flood. *Risk, Decision and Policy 7*(3), 221–233.

Zou, Y., S. Danino, K. Sun, and F. Schaub (2019). You might be affected: An empirical analysis of readability and usability issues in data breach notifications. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–14.

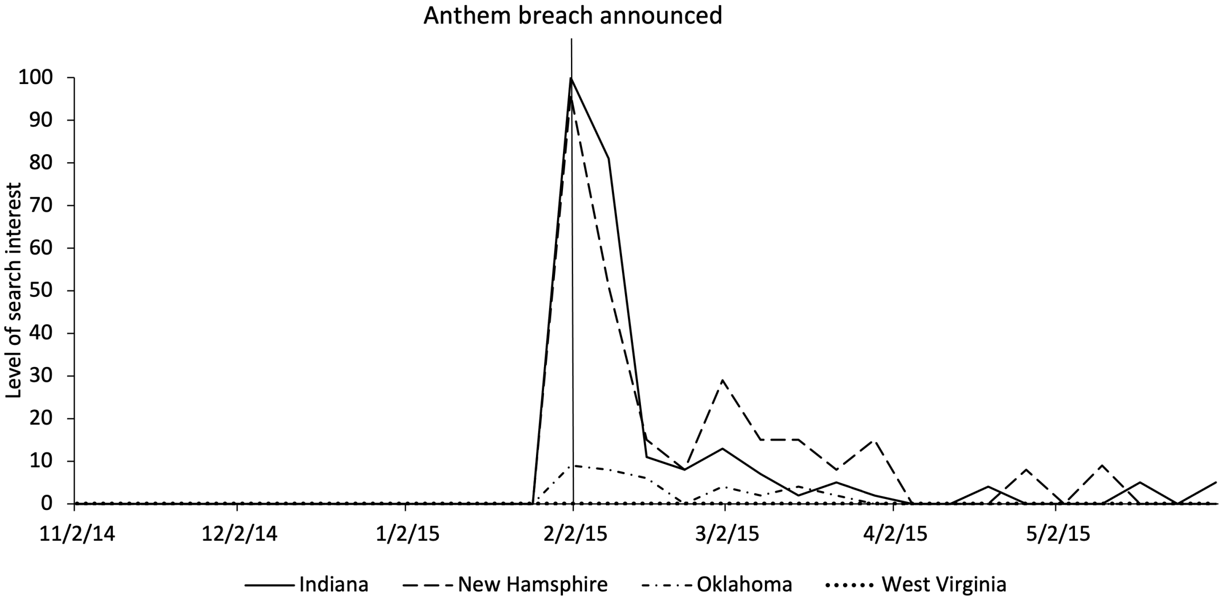
Zou, Y., A. H. Mhaidli, A. McCall, and F. Schaub (2018). I've got nothing to lose: Consumers' risk perceptions and protective actions after the Equifax Data Breach. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pp. 197–216.

APPENDIX

A Anthem Data Breach

As a basic soundness check for our identification strategy, we compared the Google search interest in the term *Anthem breach* in two high-exposure states (Indiana and New Hampshire) relative to two low-exposure states (Oklahoma and West Virginia). Figure A1 shows that prior to the Anthem breach announcement, the level of search interest in the term was zero in any of the four states. In the week of the breach announcement (the week of Feb. 1, 2015), the search interest in *Anthem breach* increased substantially in the high-exposure states relative to the low-exposure states. The level of Google search interest for *Anthem breach* rose slightly in Oklahoma and not at all in West Virginia. These search trends suggest that residents in high- and low-exposure states are likely to have responded differently to the breach, lending support to our identification strategy.

Figure A1: Google Search Trends for "Anthem Breach"; Nov. 1, 2014 - May 31, 2015



Notes: Authors' calculations using data from Google trends from November 2014 to May 2015 for the states of Indiana, New Hampshire, Oklahoma, and West Virginia. Indiana and New Hampshire are "high" exposure states in that they had the highest percentages of their population affected by the Anthem data breach. Oklahoma and West Virginia are "low" exposure states as they had the lowest percentages of their population affected by the breach.

B Credit Card Tradeline Data

We also use additional anonymized data on individual credit card accounts (i.e., tradelines) for individuals in the CCP. This data set contains detailed disaggregated information on up to 10 credit card accounts for every individual in the CCP, although the periodicity of the data has changed over time. Tradeline data are available from 2017 to 2018 at a quarterly frequency and are available at a semiannual frequency from 2014 to 2016. For each account, we can observe the date it was opened, its payment status, current balance and limit, and the date of the last activity on the account. We also observe contextual information for each account in the form of "narrative codes." For example, narrative codes can indicate if an account is part of a bankruptcy proceeding or if the account has been closed. Since both the main CCP and fraud alert data (both anonymized) are at the individual-quarter level, we aggregate the tradeline data up to the individual level.

To create a variable for the number of closed bankcards at the individual level, we first identify each credit card tradeline's opening date and, if available, its last activity date. For accounts that have a closure narrative code, we use the tradeline's last activity date as the closure date. For accounts that drop out of the data and we do not observe a last activity date and/or a closure narrative code, we use information on the last observed date of last activity to assign a closure date. We then assign closure dates to its respective calendar time quarter and sum the number of closings we observe for each closure.

C Other Precautionary Measures

Credit monitoring services are commercial services that help individuals watch their credit reports for changes and activities, such as new account openings and credit inquiries, notifying individuals whenever any change or activity occurs.[17] Credit monitoring services do not restrict creditors' access to individuals' credit reports and hence do not prevent fraudsters from opening fraudulent new accounts under an individual's name. However, these services can alert individuals to signs of potential fraudulent activities, such as changes or activities that they did not initiate, thereby enabling individuals to act to prevent further fraud or limit their losses.

An initial fraud alert is a free, consumer-initiated credit report flag that indicates to creditors that an individual is a possible victim of fraud.[18] These flags last for one year and the credit bureau that was contacted by the individual will notify the other bureaus of the alert.[19] Under FACTA, when creditors observe an initial fraud alert in an individual's credit file, they are required to take extra steps to verify the individual's identity before opening a new credit account, increasing an existing credit line, or issuing additional cards for existing credit accounts under the individual's name. Because of these requirements, initial fraud alerts may help to lower the chances that an individual experiences new account fraud. However, unlike credit freezes, fraud alerts do not limit creditors' access to the individual's credit files; a criminal may thus still be able to open fraudulent new accounts under the individual's name.

[17] These services can be purchased from any of the three major credit bureaus, as well as third-party ID theft protection companies. Breached entities often offer affected individuals one to two years of free credit monitoring services. In Equifax's case, the company offered all affected individuals one year of its credit monitoring services for free.

[18] Individuals who have been actual victims of fraud, such as severe ID theft, can file for an extended fraud alert. Extended fraud alerts are similar to initial fraud alerts, but they impose stricter filing requirements and last for a longer period time.

[19] Prior to the passage of a new federal law on September 21, 2018, each initial fraud alert lasts 90 days.

D DID Results for Consumer Credit Outcomes

We compare each prior fraud exposure group to prior non-victims and prior fraud victims to prior breach victims to examine if there were any differences in our credit variables across fraud exposure groups. Results are shown in Appendix Figures A7-A9. Results for prior fraud victims relative to non-victims are presented in Figure A7. Unlike the freeze results presented in Figure 12, none of the credit variables exhibit parallel trends in the pre-period, so we do not view any of these estimates as causal. In panel A, we see that prior fraud victims have relatively fewer inquiries than prior non-victims in the quarters after the breach announcement. In the remaining panels, we can see that prior fraud victims had relatively fewer accounts and lower balances and limits than prior non-victims in the pre-announcement quarters, but had relatively similar numbers of accounts, balance and limits in the post-announcement quarters.

In panel A of Figure A8, we see that prior breach victims had relatively more inquiries than prior non-victims (though, as shown in panel A of Appendix Figures A4 and A5, both groups had an overall downward trend in the number of inquiries). Panel B indicates that prior breach victims had relatively fewer accounts than non-victims in the post-announcement quarters, while panels C and D show that prior breach victims had lower balances and limits in the pre-announcement quarters, but had higher balances and limits in the post quarters than prior non-victims.[20]

Finally, in Figure A9, we compare prior fraud victims to prior breach victims. Prior fraud victims had relatively fewer inquiries than prior breach victims in the post-announcement quarters, while the number of accounts, balances, and limits on all accounts were roughly similar across the two groups. Overall, there is clear evidence of secular trends in all four variables, with differences across exposure group, and no clear evidence of any major changes in credit in response to the breach announcement. These results, however, do not take into account that a share of each exposure group freezes their credit report in response to the breach announcement. We explore if credit changes by freeze status in Section 7.1.

[20] One hypothesis for the results we see for prior breach victims is that for these measures of precaution in the credit market, it may be the case that the cost of closing accounts and reducing demand is different than placing a credit report freeze for this group. As we discuss in our conceptual framework, prior breach victims experience a 'near-miss' and may have a lower level of perceived fraud risk than non-victims, which in turn may lead prior breach victims to have lower take-up of precautionary actions that have higher costs.

Table A1: Anthem Breach: Most and Least Affected States

	Most Affected States		
State	Number of Victims	State Population	% Affected
California	13,500,000	38,918,045	34.69%
Connecticut	1,700,000	3,587,122	47.39%
Georgia	3,700,000	10,178,447	36.35%
Indiana	4,500,000	6,608,422	68.09%
Maine	531,000	1,328,262	39.98%
Missouri	2,000,000	6,071,732	32.94%
New Hampshire	668,000	1,336,350	49.99%
New York	5,023,000	19,654,666	25.56%
Virginia	3,770,000	8,361,808	45.09%
	Least Affected States		
State	Number of Victims	State Population	% Affected
Alaska	34,000	737,498	4.61%
Colorado	19,700	5,450,623	0.36%
Hawaii	18,000	1,422,052	1.27%
Illinois	215,000	12,858,913	1.67%
Montana	48,000	1,030,475	4.66%
New Jersey	209,000	8,867,949	2.36%
New Mexico	11,600	2,089,291	0.56%
North Dakota	27,000	754,066	3.58%
Oklahoma	100	3,909,500	0%
Utah	10,956	2,981,835	0.37%
West Virginia	220	1,842,050	0.02%

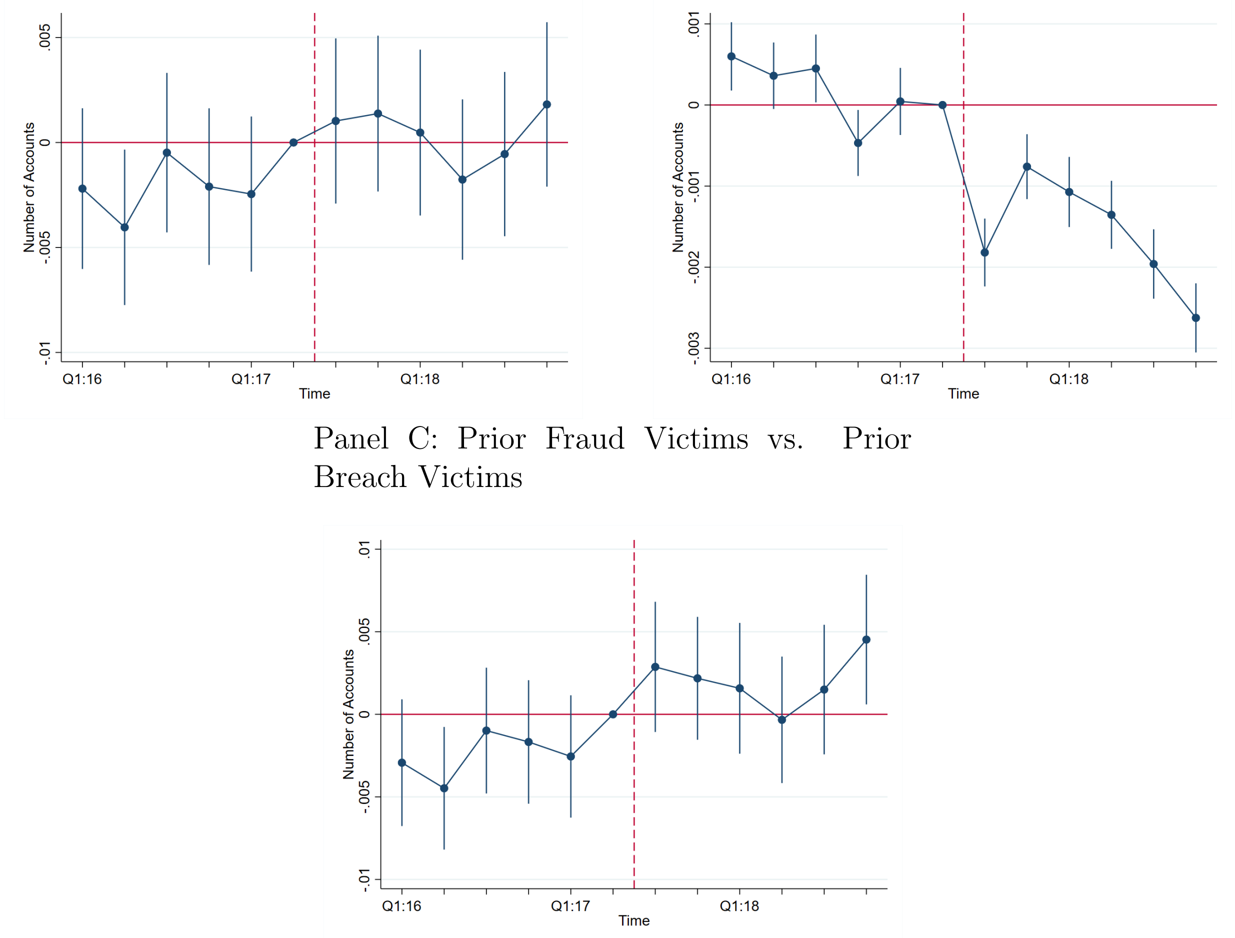
Note: Authors' calculations based on statistics from state websites, press articles, and correspondence from states' attorney's generals offices as of March 2020. Population as of 2015 using data from the US Census Bureau.

Table A2: Additional CCP Summary Statistics

	Pre-Equifax Breach Average (S.D.)	Post-Equifax Breach Average (S.D.)
Panel A: Full Sample		
% with a closed credit card account	11.0%	11.8%
Total number of accounts	4.99 (4.36)	5.17 (4.51)
Total balance on all accounts	$90,123 ($170,207)	$92,891 ($175,139)
Total credit limit on all accounts	$125,700 ($205,007)	$130,327 ($211,995)
Number of inquiries	0.554 (1.06)	0.500 (0.97)
Credit Score	696 (105)	699 (106)
Panel B: Prior Fraud Victims		
% with a closed credit card account	14.7%	15.1%
Total number of accounts	5.79 (5.00)	6.06 (5.20)
Total balance on all accounts	$96,605 ($170,567)	$103,794 ($176,786)
Total credit limit on all accounts	$127,824 ($204,844)	$137,613 ($211,542)
Number of inquiries	0.988 (1.68)	0.849 (1.47)
Credit Score	650 (119)	656 (121)
Panel C: Prior Breach Victims		
% with a closed credit card account	11.7%	13.8%
Total number of accounts	5.18 (4.41)	5.46 (4.58)
Total balance on all accounts	$110,293 ($218,032)	$116,815 ($227,778)
Total credit limit on all accounts	$150,786 ($257,619)	$160,729 ($270,065)
Number of inquiries	0.500 (0.97)	0.456 (0.89)
Credit Score	704 (103)	709 (103)

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Sample is from Q1:2016 to Q4:2018. Prior fraud victims are individuals who had filed an extended fraud alert any time between Q1:2010 to Q2:2017. Prior data breach victims are individuals living in states where at least 25% of the total population was affected by the 2015 Anthem data breach. We exclude individuals who fall into both victimization categories. Credit score is the Equifax Risk Score. Details on the construction of the closed credit card account variable are in Appendix B.

Figure A2: Number of Closed Card Accounts



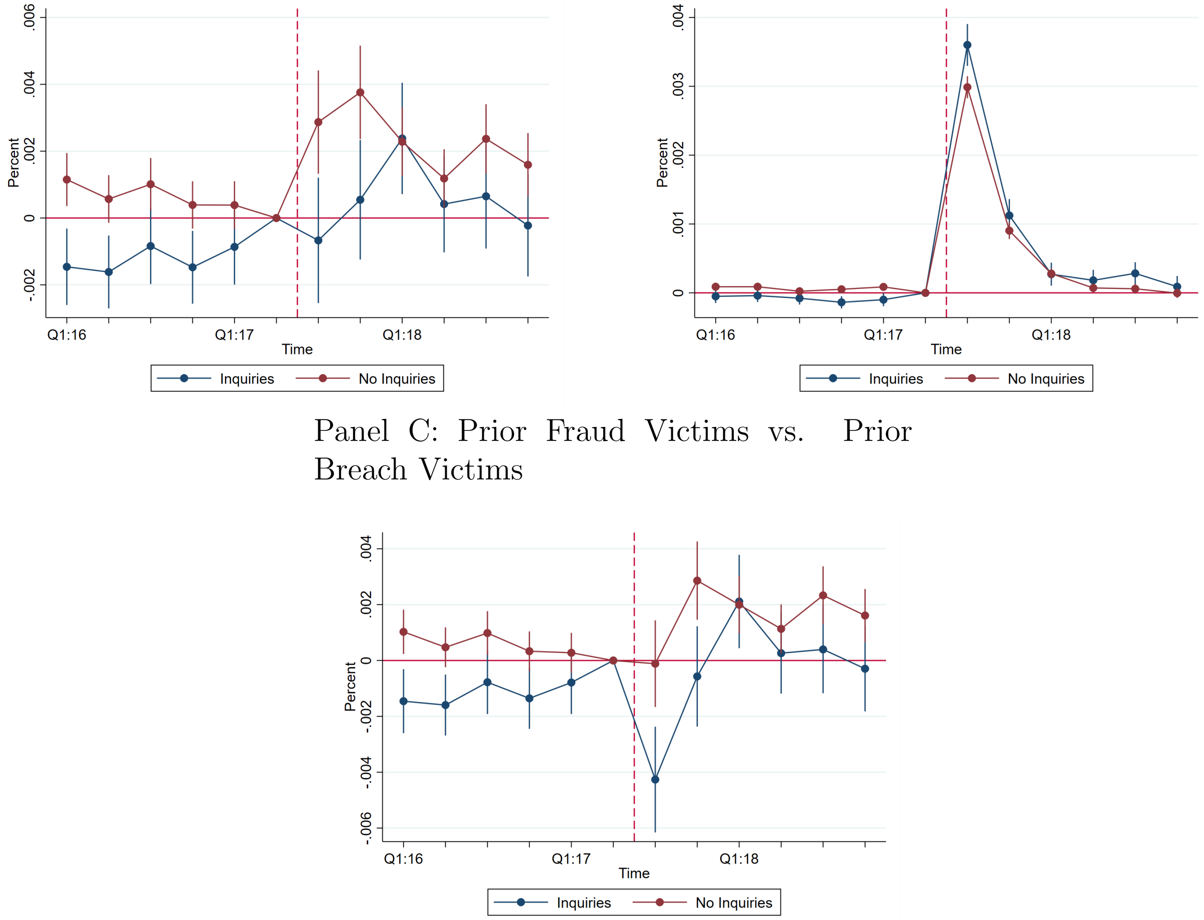
Panel A: Prior Fraud Victims vs. Non-Victims

Panel B: Prior Breach Victims vs. Non-Victims

Panel C: Prior Fraud Victims vs. Prior Breach Victims

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. The dependent variable is the number of credit card accounts an individual closed that quarter; details on the construction of the closed credit card account variable are in Appendix B. Results in panel C are for prior fraud victims relative to prior data breach victims (the control group). Dots represent point estimates and bands show 95% confidence intervals.

Figure A3: Equifax Breach: Inquiry vs No Inquiry; Probability of Having a New Credit Freeze



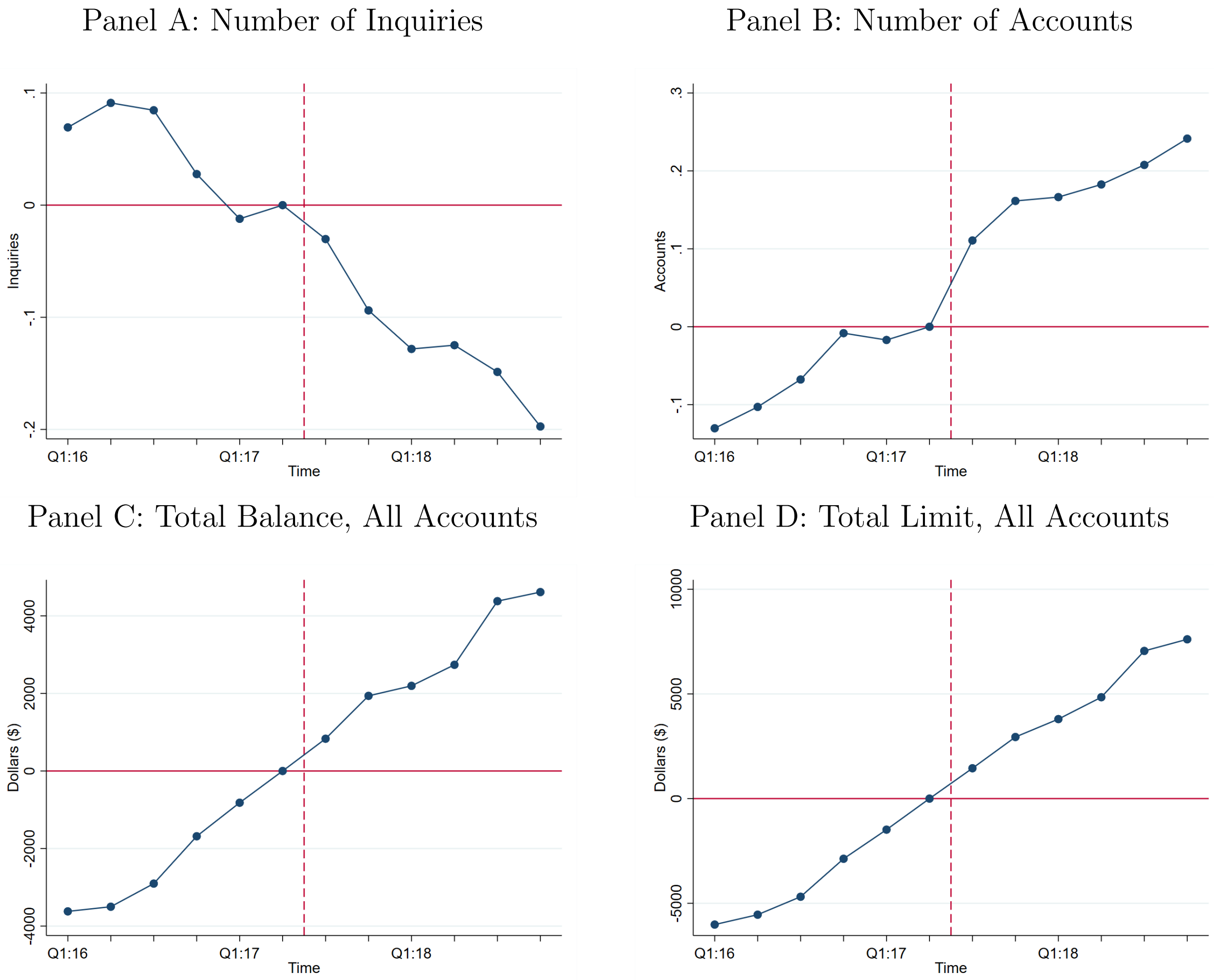
Panel A: Prior Fraud Victims vs. Non-Victims

Panel B: Prior Breach Victims vs. Non-Victims

Panel C: Prior Fraud Victims vs. Prior Breach Victims

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Dots represent point estimates and bands show 95% confidence intervals. The dependent variable in all three panels is the dummy variable for having a new credit report freeze.

Figure A4: Equifax Breach Event Study Results: Non-Victims


Panel A: Number of Inquiries

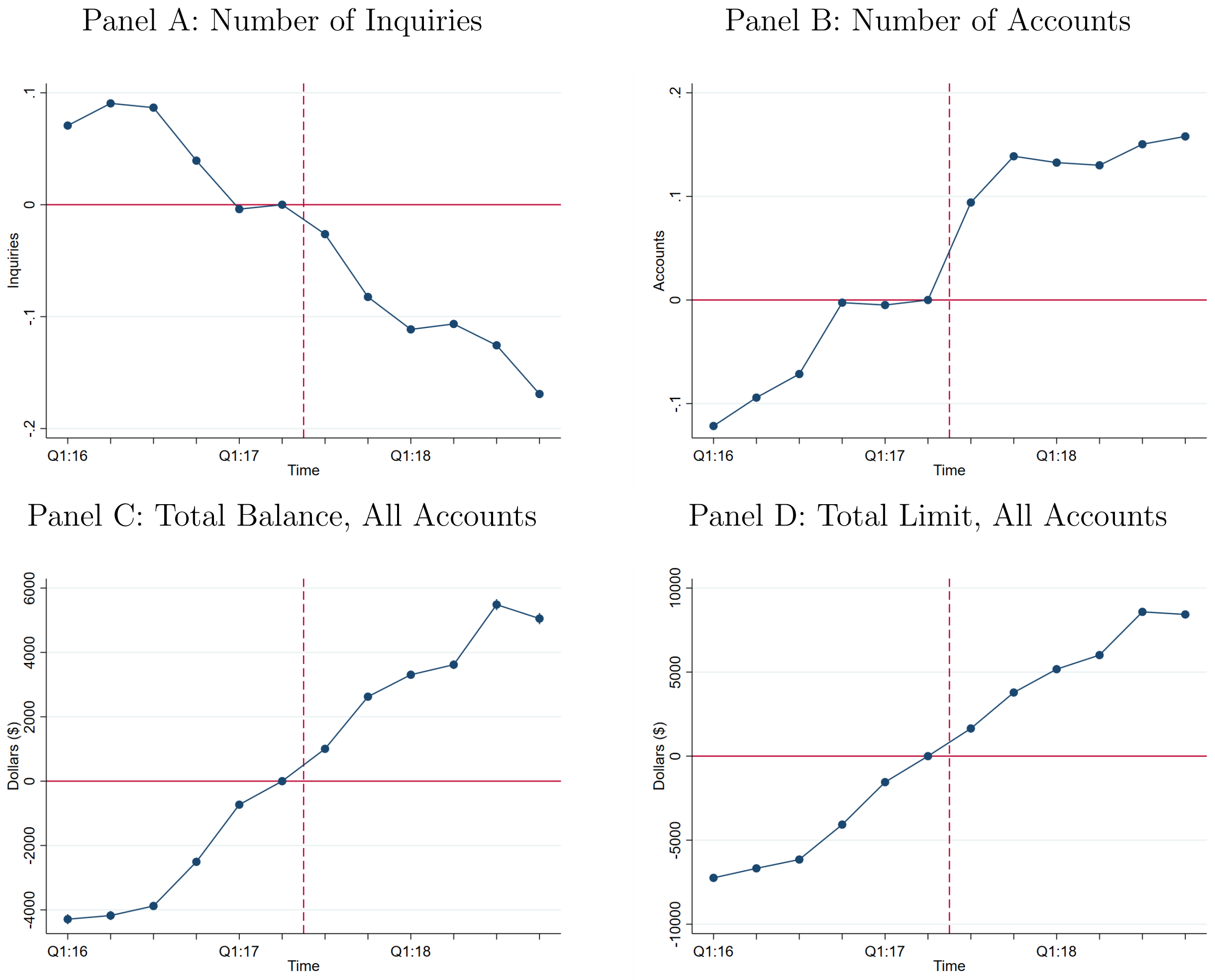
Panel B: Number of Accounts

Panel C: Total Balance, All Accounts

Panel D: Total Limit, All Accounts

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. These figures present estimates from the event study regression model described in Section 5.3. Estimates in panels C and D are measured in dollars. Dots represent point estimates and bands show 95% confidence intervals.

Figure A5: Equifax Breach Event Study Results: Prior Breach Victims


Panel A: Number of Inquiries

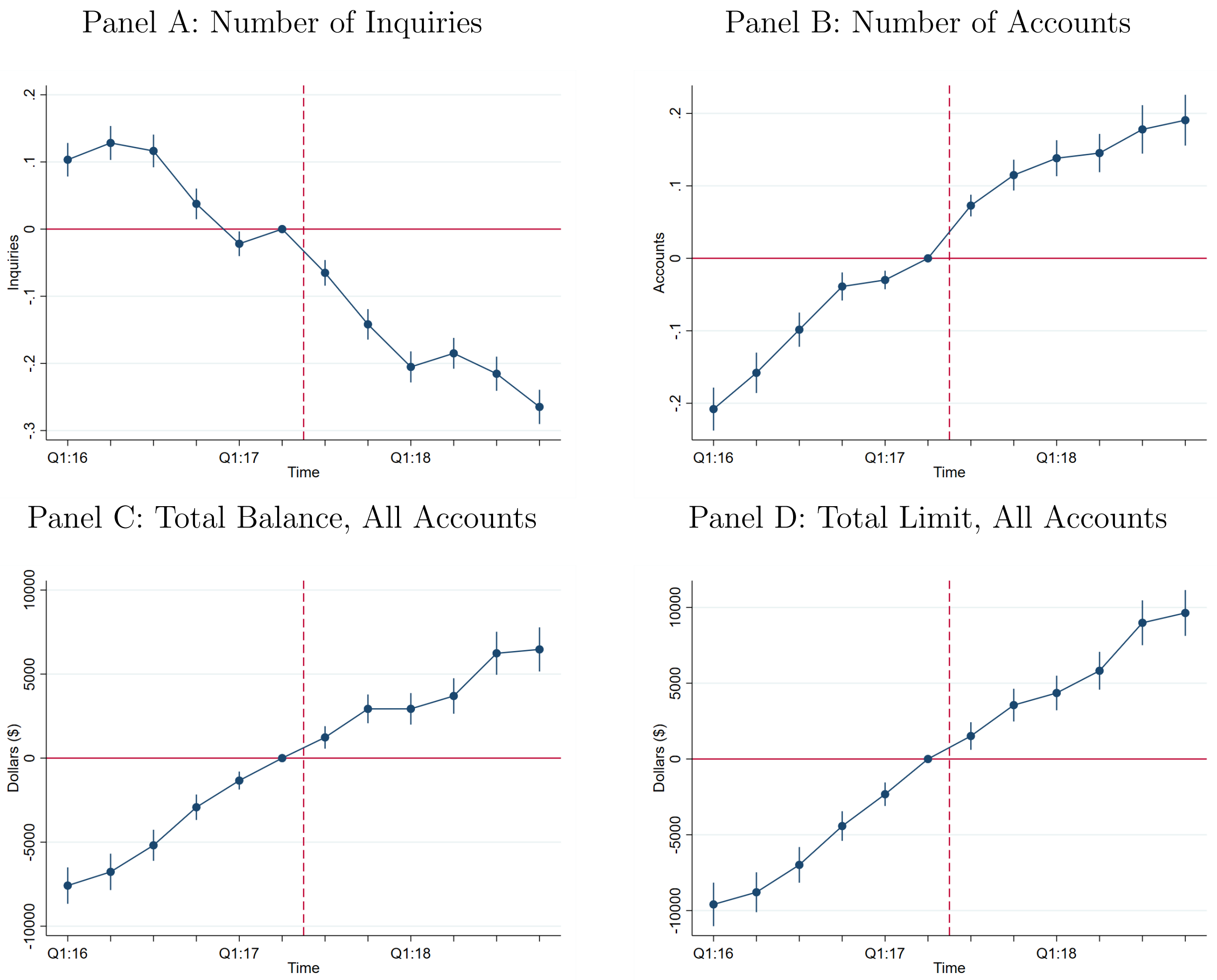
Panel B: Number of Accounts

Panel C: Total Balance, All Accounts

Panel D: Total Limit, All Accounts

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. These figures present estimates from the event study regression model described in Section 5.3. Estimates in panels C and D are measured in dollars. Dots represent point estimates and bands show 95% confidence intervals.

Figure A6: Equifax Breach Event Study Results: Prior Fraud Victims



Panel A: Number of Inquiries

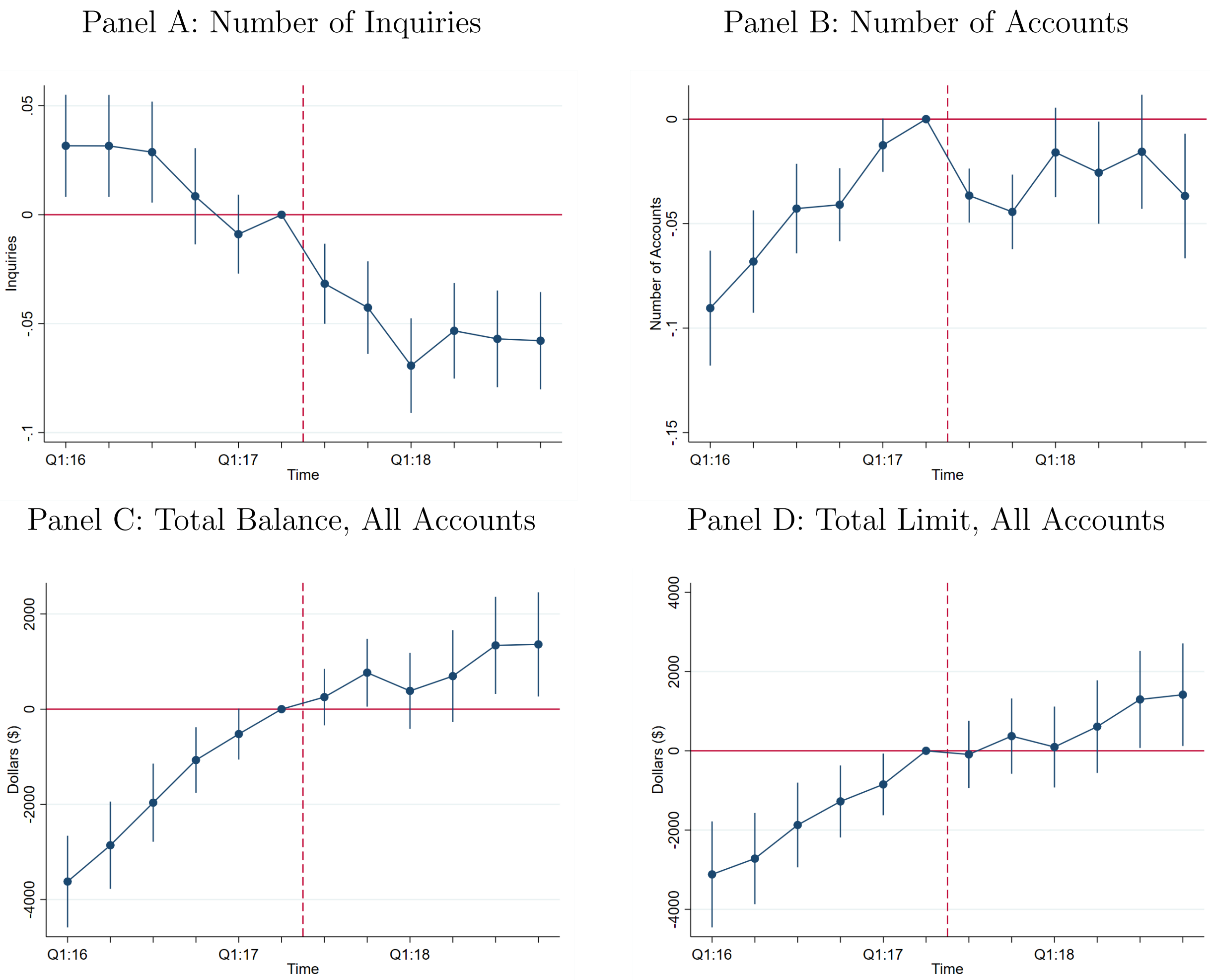
Panel B: Number of Accounts

Panel C: Total Balance, All Accounts

Panel D: Total Limit, All Accounts

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. These figures present estimates from the event study regression model described in Section 5.3. Estimates in panels C and D are measured in dollars. Dots represent point estimates and bands show 95% confidence intervals.

Figure A7: Equifax Breach Difference-in-Difference Results: Prior Fraud Victims vs. Non-Victims



Panel A: Number of Inquiries

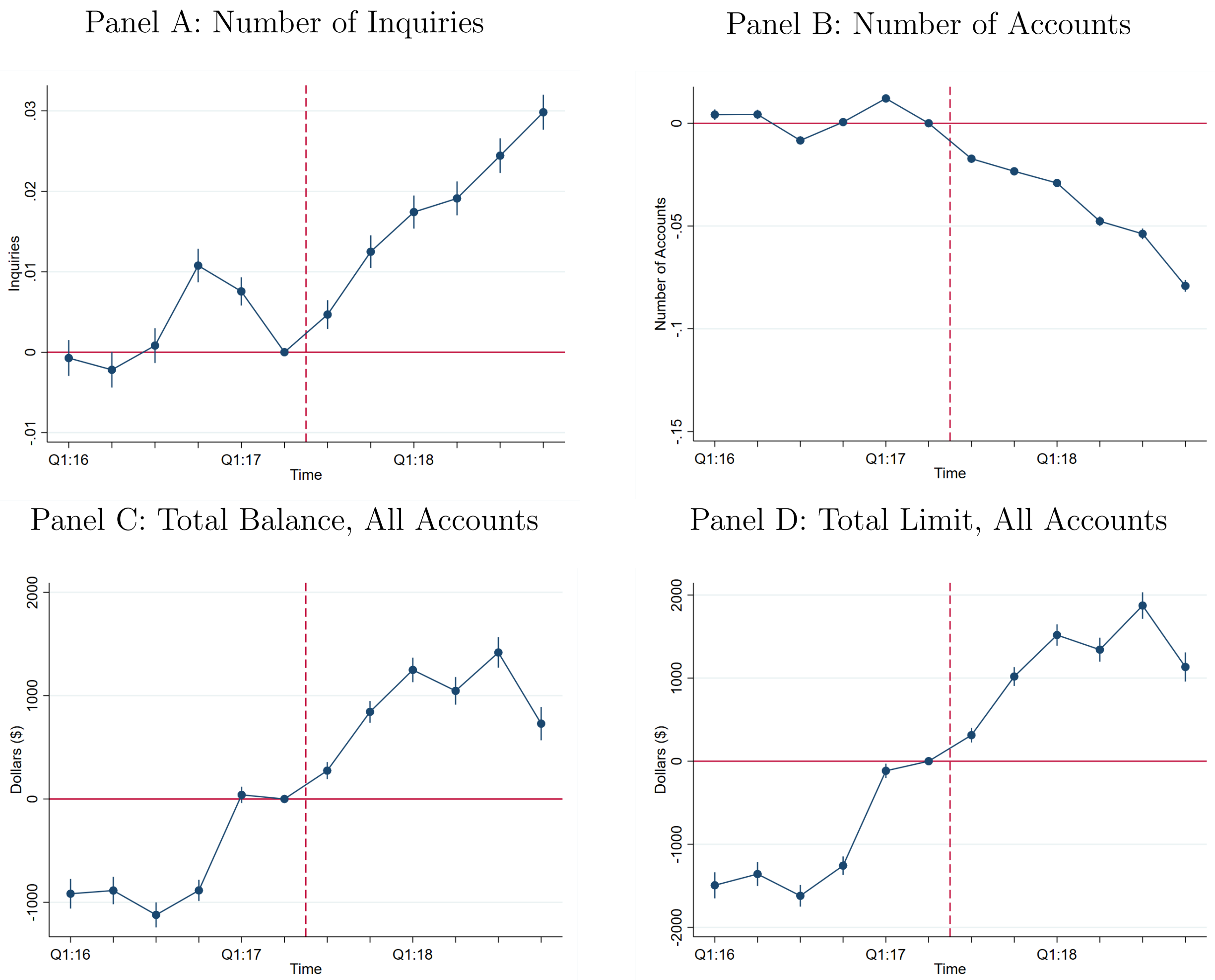
Panel B: Number of Accounts

Panel C: Total Balance, All Accounts

Panel D: Total Limit, All Accounts

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Estimates in panels C and D are measured in dollars. Dots represent point estimates and bands show 95% confidence intervals.

Figure A8: Equifax Breach Difference-in-Difference Results: Prior Breach Victims vs. Non-Victims


Panel A: Number of Inquiries

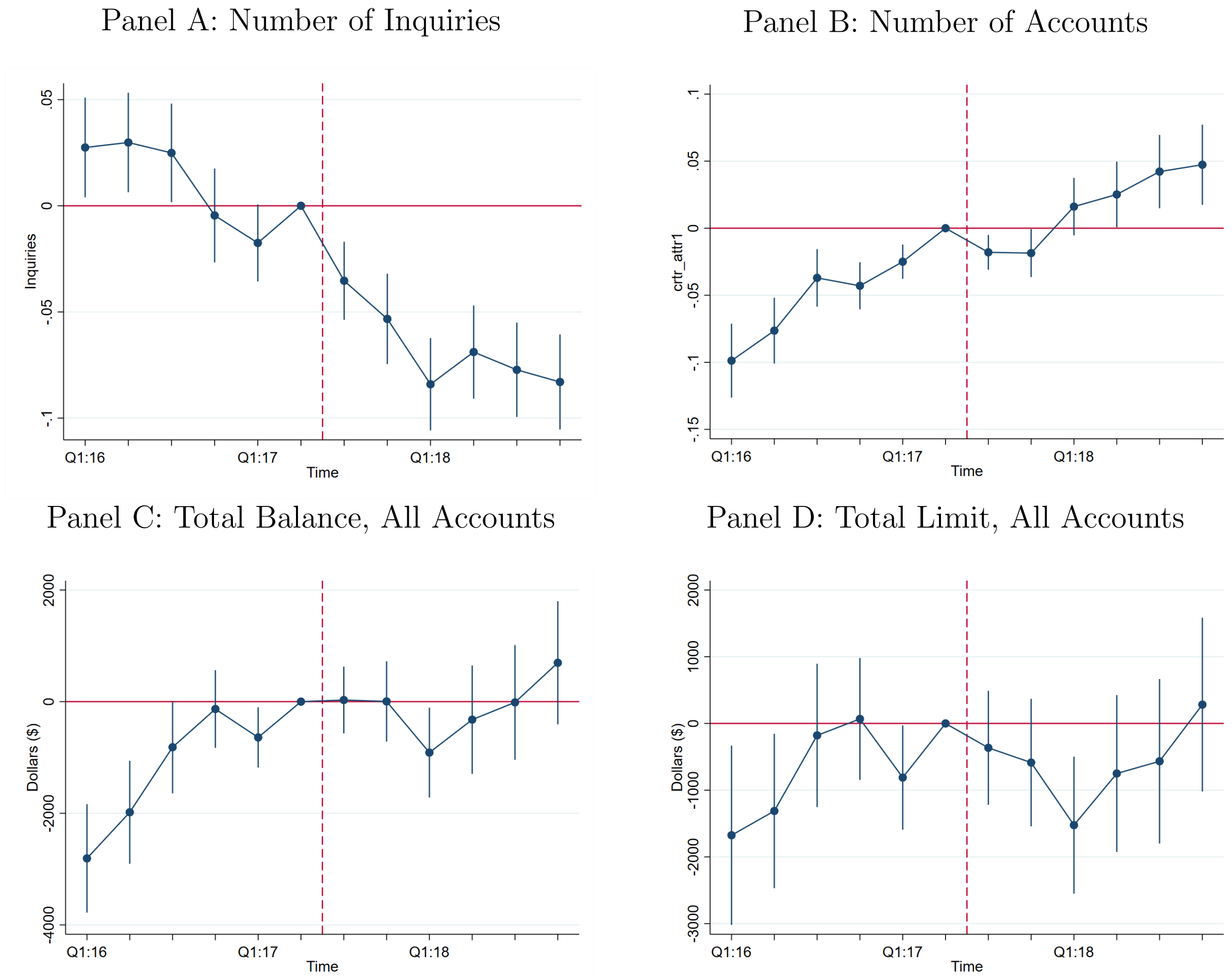
Panel B: Number of Accounts

Panel C: Total Balance, All Accounts

Panel D: Total Limit, All Accounts

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Estimates in panels C and D are measured in dollars. Dots represent point estimates and bands show 95% confidence intervals.

Figure A9: Equifax Breach DID Results: Prior Fraud Victims vs. Prior Breach Victims



Panel A: Number of Inquiries

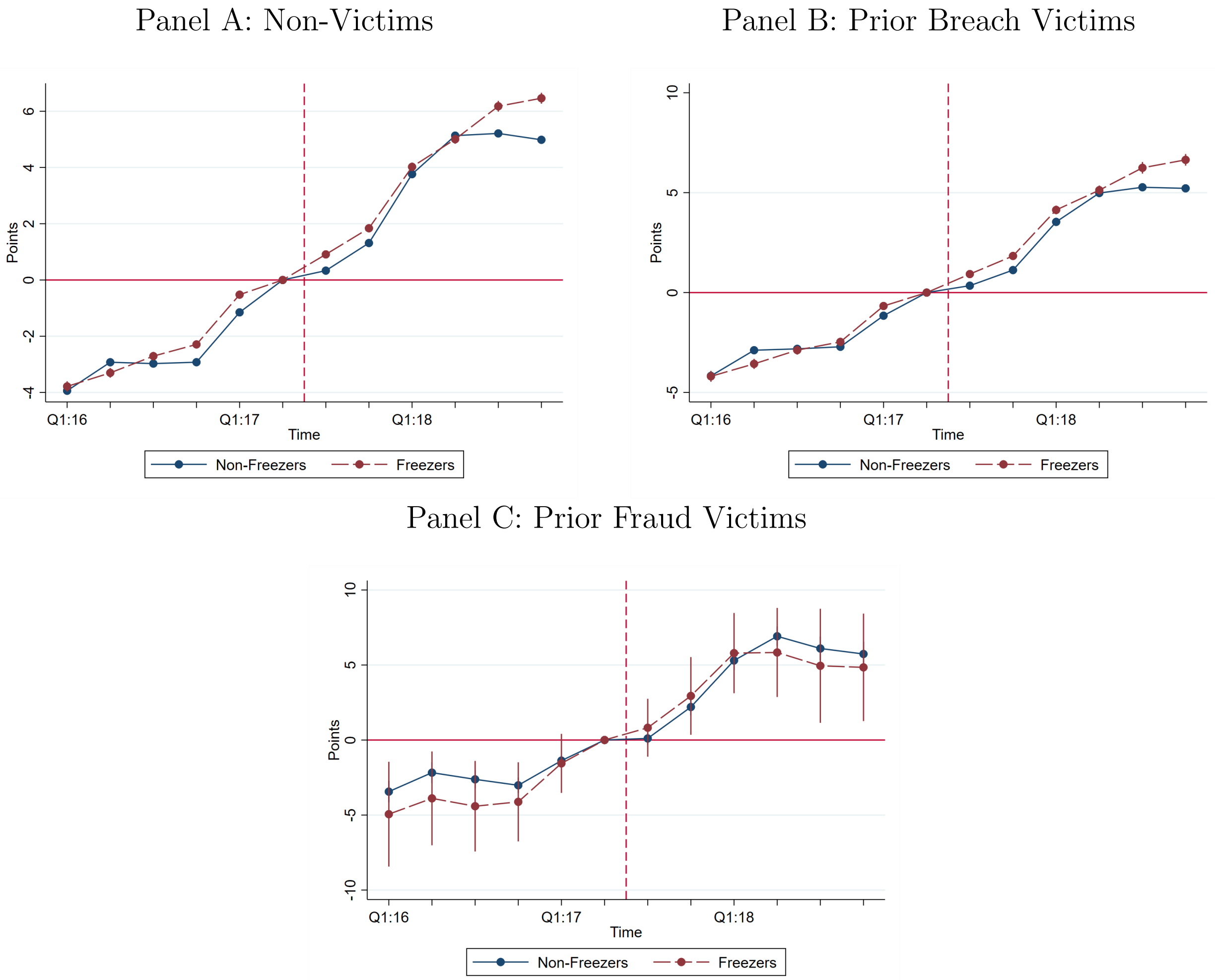
Panel B: Number of Accounts

Panel C: Total Balance, All Accounts

Panel D: Total Limit, All Accounts

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Results are for prior fraud victims relative to prior data breach victims (the control group). Estimates in panels C and D are measured in dollars. Dots represent point estimates and bands show 95% confidence intervals.

Figure A10: Equifax Breach: Freeze vs. Non-Freeze; Credit Scores



Panel A: Non-Victims

Panel B: Prior Breach Victims

Panel C: Prior Fraud Victims

Notes: Authors' calculations using data from FRBNY Consumer Credit Panel/Equifax Data, augmented with variables obtained by the Consumer Finance Institute from Equifax. Credit score is the Equifax Risk Score. Freezers are individuals who froze their credit report in either Q3 or Q4 of 2017 and kept their freeze on for the remainder of the sample. Non-freezers never placed a credit report freeze during the same period. The dependent variable in all three panels is credit score.