Journal of Banking and Finance 88 (2018) 192–207

Contents lists available at ScienceDirect

Journal of Banking and Finance

journal homepage: www.elsevier.com/locate/jbf

How data breaches affect consumer credit☆

Vyacheslav Mikhed[a,*], Michael Vogan[b]

[a] Payment Cards Center, Federal Reserve Bank of Philadelphia, Ten Independence Mall, Philadelphia, PA 19106, USA
[b] Moody's Analytics, 121 N. Walnut St., West Chester, PA 19380, USA

ARTICLE INFO

Article history:
Received 21 December 2015
Accepted 2 December 2017
Available online 6 December 2017

JEL classification:
D12
G02
G22
C23

Keywords:
Identity theft
Fraud alert
Data breach
Consumer protection
Credit report

ABSTRACT

We use the 2012 South Carolina Department of Revenue data breach as a natural experiment to study how data breaches and news coverage about them affect consumers' interactions with the credit market and their use of credit. We find that some consumers directly exposed to the breach protected themselves against potential losses from future fraudulent use of stolen information by monitoring their files and freezing access to their credit reports. However, these consumers continued their regular use of existing credit cards and did not switch lenders. The response of consumers exposed to the news about the breach only was negligible.

1. Introduction

Data breaches have been a growing concern in the U.S. in recent years with hundreds of millions of consumer records compromised and hundreds of breaches reported each year.[1] These security events affect financial institutions directly (e.g., the JPMorgan Chase data breach) and indirectly, through the theft of payment information (e.g., breaches at Target and Home Depot). Even when no financial information is stolen in a data breach, criminals may use other consumer records such as Social Security numbers to open new fraudulent financial accounts or steal money from financial institutions. In addition, data breaches may have profound effects on consumers through identity theft, for example, which leaves about 14% of the victims with out-of-pocket losses and 36% with emotional distress (Harrell, 2015).

Despite the millions of consumers and hundreds of institutions affected by data breaches, little is known about how these actors react to such events. This study uses the 2012 South Carolina Department of Revenue data breach and a unique data set of data breach victims to provide causal estimates of the effect of cybersecurity incidents on consumers. We examine three areas identified in previous studies in which consumers may respond to breaches. First, we investigate whether affected consumers protect themselves against future losses from the breach using available fraud protection services. Second, we study whether and how consumers change their credit card payment behavior and interactions with financial institutions and the credit market. Third, we explore how data breaches and related news coverage change the behavior of breach victims and unaffected consumers and examine whether these security events could generate a panic that extends beyond those directly affected by the breach.

The first question is important because the current system of consumer privacy protection requires breached institutions to disclose data breaches to the public and to notify consumers about

☆ This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. We wish to thank Amy Crews Cutts, Bradley Dear, April Ferguson, and Henry Korytkowski of Equifax for their assistance with the data on fraud protection. We are grateful to Cris McCollum for her help with the LexisNexis data and Avi Peled for his help with maps. We thank Neil Bhutta, Julia Cheney, Robert M. Hunt, Leslie John, Kirsten E. Martin, Barry Schornick, and seminar participants at the Federal Reserve Bank of Philadelphia, GMU Digital Information Policy Scholars Conference, the Federal Reserve System Applied Microeconomics Conference, 2016 Boulder Summer Conference on Consumer Financial Decision Making, 2017 ASSA Annual Meeting, NACHA Payments 2017, and the 2015 Federal Reserve System Payments Analysts Meeting in San Francisco for their helpful suggestions. The views expressed here are those of the authors and do not necessarily reflect the views of the Federal Reserve Bank of Philadelphia or the Federal Reserve System.

* Corresponding author.
E-mail addresses: slava.mikhed@phil.frb.org (V. Mikhed), michael.vogan@moodys.com (M. Vogan).

[1] For example, see www.idtheftcenter.org/Data-Breaches/data-breaches.html.

https://doi.org/10.1016/j.jbankfin.2017.12.002
0378-4266/

the theft of their personal information.[2] While the costs of a breach disclosure may motivate institutions to invest in information security, the current system of consumer privacy protection also relies on consumers taking precautions after they receive notifications from breached institutions (Romanosky et al., 2011). However, this mechanism in the system will not work, if consumers do not protect themselves from fraudsters after they receive breach notifications. Thus, this costly mechanism may be inefficient and provide little benefit. In this case, other methods of improving consumer privacy protection, such as inspections of how firms store and transmit consumer data and ensuring a satisfactory level of protection of these data, may be more efficient (Romanosky et al., 2011).

The question of whether and how consumers change their credit card usage behavior and their interactions with the credit market is important for policymakers and financial institutions. Previous research on consumer reactions to data breaches has shown that consumers may choose to use another business after a security incident. For example, Kwon and Johnson (2015) find that hospital data breaches reduce the number of patient visits. Similarly, McGrath (2014) reports that Target's sales dropped after its 2013 data breach.[3] However, Greene and Stavins (2016) suggest that the Target data breach only somewhat worsened consumer perception of debit card security in the short term, but it did not lead to an economically significant decrease in the use of debit cards in the longer term. We contribute to this research by providing new causal evidence on changes in consumers' use of their credit cards and whether they switched lenders after a data breach.

In general, an important question remains whether data breaches and the associated news coverage can undermine consumer confidence in the U.S. payment system. This is essential because previous studies suggest that data breaches may pose risks for the U.S. payment card systems if a large number of consumers abandon electronic payments and switch to other less efficient payment options (Cheney et al., 2012). It is also possible that additional news reporting on data breaches and information security may motivate consumers to take precautions or to alter their payment choices (Kosse, 2013; Kahn and Liñares-Zegarra, 2016). The effect of news on the perceptions of risk has been shown to matter in other contexts (e.g., Kahneman, 2011 suggests that media attention may influence individuals' perceptions of the likelihood of rare events such as lottery winnings and terrorist attacks, and Gallagher, 2014 shows that news affects consumer decisions to purchase flood insurance). We provide new causal evidence on the effect of data breaches and related news coverage on unaffected consumers.

To provide evidence for these questions, we use a specific information security incident: the 2012 South Carolina Department of Revenue data breach. This data breach provides a unique natural experiment that allows us to identify precisely a group of consumers who were directly exposed to risks created by the breach. We can compare the reactions of those consumers with another group of consumers who were not directly affected by the incident. In addition, we can also identify a third group of consumers who received news about the breach, but whose accounts were not directly breached, and track their reactions as well.

To be more explicit, this incident compromised the records of most South Carolina residents (at least 81% of adults and their dependents), but very few records were stolen from residents of other states. This feature is the basis of our identification strategy. The South Carolina data breach is a "treatment" that directly affected South Carolina residents at the time of the breach (October 2012) and indirectly affected residents of certain areas in neighboring Georgia and North Carolina (consumers in shared media markets) through the news.[4] We use an event study methodology to estimate the effect of the breach itself and information about the breach on consumer responses.

To gauge the effect of the breach on consumers' fraud protection behavior and measure how breach notifications change this behavior, we examine the adoption of five fraud protection services: initial fraud alerts, extended fraud alerts, credit watches, credit (security) freezes, and credit opt outs. All these services provide consumers with one or more of the following features: additional identity verification from lenders, fraud insurance coverage, a complete credit file freeze, and removal from prescreened credit or insurance solicitations. Table 1 summarizes the main features of these fraud protection services. We hypothesize that consumers may engage one or a few of these services after receiving a breach notification and calculate how many consumers reacted to such notifications.

We find that victims of the 2012 South Carolina Department of Revenue breach acquired many more fraud protection services immediately after the breach relative to unaffected, but comparable, consumers in other states. Consumers affected by the breach were five times more likely to put an initial fraud alert in their credit files compared with unaffected individuals. In addition, the odds of data breach victims obtaining a credit watch were 48 times higher than that of the control groups. Data breach victims were 34 times more likely to freeze their credit files and three times more likely to opt out of credit offers. Consumers directly exposed by the data breach incurred nonpecuniary (and possibly pecuniary) costs to obtain additional protection from possible identity theft. Before the event, the vast majority of South Carolina residents were not using those protections, an observation suggesting that there was a significant change in their expectations in light of this specific data breach.

While data breach victims adopted fraud protection services after the incident, they did not change their credit card payment behavior or switch lenders. In particular, we find that these individuals maintained the same number of open credit cards as unaffected consumers. Breach victims also did not seem to open new credit cards at a higher rate than individuals in the control group. Taken together, these two results suggest that the data breach did not prompt consumers to switch lenders. In addition, data breach victims kept the same credit card balances as unaffected consumers and did not increase 30 days past due occurrences on their credit cards. These individuals also kept about the same proportion of cards in good standing. We did not detect any systematic pattern in the risk scores of this group; their credit card limits, which are measures of credit supply, increased, albeit slightly, after the breach compared with the unaffected group. Overall, there is little evidence that the breach had an adverse effect on credit market interactions or on the credit standing of the breached consumers.

We use the local television markets as defined by Nielsen's Designated Market Areas (DMAs) to examine the reaction of North Carolina and Georgia residents to the breach. Those who share television markets with South Carolinians received identical television news coverage about the breach as residents of South Carolina. However, these residents of North Carolina and Georgia were not members of the breached set of consumers. Thus, they were subject to the news reporting on the breach, but their personal in-

[2] According to Ablon et al. (2016), all U.S. states, except for Alabama, New Mexico, and South Dakota, had data breach notifications laws as of March 2016.

[3] These reduced sales and breach related expenses can lead to a short-term drop in the stock prices of breached entities (e.g., Campbell et al., 2003; Gatzlaff and McCullough, 2010).

[4] This example allows us to make some clear distinctions about the various ways in which a data breach can affect consumer behavior. In other data breaches, only a combination of effects can be observed.

Table 1
Fraud protection services and their features.

Fraud protection service name	Features	Fees	Duration
Initial fraud alert	Requires lenders to verify consumer's identity when they receive credit applications	No	90 days
Credit freeze	Blocks access to credit reports for everyone, makes it almost impossible to get new credit	$3 to file or lift in GA, $0 in SC and NC	Until removed by consumer
Credit watch	Notifies consumers of updates to credit reports, offers fraud insurance and access to fraud resolution	$12.95 to 29.95 per month (Equifax), free in SC after the breach	Until canceled by consumer, until Oct. 31, 2017, in SC
Credit offers opt out	Removes consumers from pre-screened solicitation lists for credit and insurance products	No	5 years
Extended fraud alert	Requires evidence of fraud with an ID theft report or police report, requires lenders to verify consumer's identity, removes consumers from pre-screened solicitation lists	No	7 years for lenders' verification and 5 years for prescreened offers removal

formation was not stolen in the incident. Therefore, in this setup, we measure the effect of the news on unaffected consumers. We find little evidence that consumers in those states took any action based on the news coverage of the breach; there was practically no increase in enrollment in various forms of protection, including free services.

Taken together, our findings suggest that some consumers benefit from breach notifications because they prompt breach victims to acquire fraud protection services. While many individuals acquired these services (e.g., 29% of South Carolina residents signed up for credit watches), many victims failed to protect themselves despite being warned and being offered free services. Policymakers may consider this finding in designing future outreach strategies for such consumers, or they may focus on improving data protection at firms to minimize the likelihood of a data breach. While fraud protection take-up increased after the breach, there is little evidence that breach victims altered their credit card behavior or interactions with the credit market after the incident. In addition, news coverage about the data breach had a very limited effect on the decision to acquire fraud protection for those consumers who were not exposed to the breach. Overall, these consumers do not seem to revise their beliefs about personal information security or change their behavior after the data breach.

2. South Carolina department of revenue data breach

On October 26, 2012, the South Carolina Department of Revenue (SCDOR) announced it had experienced a data breach (Durrette, 2012). This breach exposed 3.8 million Social Security numbers (SSNs) of South Carolina taxpayers, including 1.9 million dependents (Tripwire, 2012). The information on 3.3 million bank accounts was also stolen (Tripwire, 2012). The cyberattack was executed by an unknown hacker who acquired employee credentials via phishing techniques and proceeded to compromise a total of 44 systems to steal 74.7 GB of personally identifiable information and cardholder data. The breach, which was the largest to occur in 2012, affected about 81% of South Carolina residents.[5]

Immediately after the data breach, the SCDOR launched an engagement effort offering consumers information and services to mitigate any potential incidents of identity theft resulting from the breach. Beginning on October 26, 2012, consumers who filed tax returns after 1998 were eligible for one year of free credit monitoring through Experian's ProtectMyID Alert.[6] The ProtectMyID Alert is designed to "detect, protect, and resolve potential identity theft, and includes daily monitoring of all three credit bureaus." By registering for the ProtectMyID Alert, consumers receive a free copy of their Experian credit report, daily credit monitoring, identity theft insurance of up to $1 million, and access to a fraud resolution specialist that continues after the free one-year offer period ends.[7] The SCDOR encouraged consumers to apply for ProtectMyID Alert coverage before January 31, 2013, by visiting a website or calling a telephone number designated specifically for victims of the SCDOR data breach. By November 7, 2012, the Experian call center had received an estimated 729,000 calls and 693,000 sign-ups (McLeod, 2012). The SCDOR informed consumers about other ways to protect their identities as well. These suggestions included regularly reviewing credit reports and bank statements, replacing credit and debit cards, and filing alerts and credit freezes with one of the three major credit bureaus.[8]

In the months following its initial announcement, the SCDOR made alterations to its outreach strategy as it gradually learned more about the breach. The SCDOR notified victimized consumers in writing on the state's letterhead sent via mail between December 10, 2012, and the end of January 2013. During this time, it also extended the deadline to apply for free Experian credit monitoring to March 31, 2013. Beginning on October 24, 2013, the SCDOR announced that enrollment would begin for an additional year of free credit monitoring through a company named CSID.[9] This product was only offered to electronic tax filers because it had become known later that consumers who had submitted their tax returns by paper were not affected. Afterward, the free enrollment in the CSID credit monitoring program was extended to October 31, 2017.

3. Conceptual framework

3.1. How consumers directly affected by the breach might react

A typical data breach does not impose direct monetary losses on consumers. Hackers usually steal confidential consumer data that can be used later to steal money from consumer accounts or deceive lenders into extending credit to criminals who pose as legitimate consumers. To limit these potential monetary losses from a data breach, consumers and lenders may attempt to invalidate the stolen data by replacing it with new data. For example, if credit or bank account numbers are stolen in a data breach, lenders may preemptively cancel those accounts and send consumers new credit cards or bank account numbers. However, some bits of data

[5] See www.idtheftcenter.org/images/breach/Breach_Stats_Report_2012.pdf. The percentage is calculated using the 2012 South Carolina population as provided by the U.S. Census Bureau.

[6] See www.doi.sc.gov/DocumentCenter/Home/View/2597.

[7] See www.protectmyid.com/default.aspx?PageTypeID=HomePage111&SiteVersionID=940&SiteID=100330&sc=676980&bcd=.

[8] See www.scacpa.org/Content/Files/Consumer%20Protection%20Tips%20-%2011%201%2012.pdf.

[9] See www.wpde.com/news/local/faq-about-the-dept-of-revenue-hack-attack?id=820299.

are very difficult or impossible to replace (e.g., the date of birth cannot be replaced, and there is a complicated process for replacing SSNs even for identity theft victims). After a data breach, affected consumers are more likely to be subject to monetary losses from future criminal use of their stolen information, even if some of the stolen data is invalidated and replaced.

Exposed consumers can respond to data breaches in several ways. First, because they can anticipate future criminal use of their stolen data to perpetrate bank account takeover or new account fraud, these consumers may try to monitor their accounts and credit reports carefully or attempt to make it harder for criminals to open new accounts in their name. Various fraud protection services can assist consumers in these efforts. For example, a credit freeze does not allow lenders to access a consumer's credit file. So, it may stop a criminal from applying for credit using stolen consumer data. Thus, we hypothesize that, after a data breach, a consumer is more likely to engage in one or a few types of fraud protection services to limit the monetary losses from the potential criminal use of stolen information.

Second, information security incidents such as data breaches can affect consumers' perception of the security of certain payment instruments and may encourage them to reduce use of these instruments or switch to another. For example, after a data breach, consumers may perceive credit cards or automatic clearinghouse (ACH) payments as riskier than paying in cash or by check. In a related study, Kosse (2013) documents that debit card use declines – but for one day only – after incidents of debit card skimming (data theft) is reported by newspapers. Similarly, Kahn and Liñares-Zegarra (2016) argue that an identity theft experience can affect consumers' adoption and use of payment instruments.

Thus, we hypothesize that individuals whose information was stolen during the South Carolina breach may change their perceptions of the security of credit cards relative to other payment instruments. If breach victims consider credit cards to be riskier after a breach, they may use them less often when making payments, reducing card spending and balances. These consumers can also respond by closing credit card accounts and using cash instead. On the other hand, if these individuals see credit cards as more secure than other payment mechanisms (e.g., most credit cards offer users a zero liability policy on fraudulent charges), then they may use credit cards more often and increase credit card balances.

In addition, breach victims may switch to another financial institution, if they believe some are more secure than others. This tendency can generate an increase in new cards. Finally, consumers may become less attached to the credit market and stop paying their card bills or allow their cards to default. This behavior may result in more delinquencies on cards and fewer cards in good standing. We test if any of these effects are evident in our data.

3.2. How consumers exposed to the news about the breach might react

Individuals not exposed to a breach directly, but who are receiving extensive news coverage about the event, may respond to a breach in several ways. First, as the number of data breaches and the number of consumer records stolen increase every year, an additional data breach may signal a riskier environment for individuals not affected by the breach directly.[10] Thus, they may sign up for some fraud protective services preemptively. While credit monitoring services can be costly and rational consumers may decide against them or even wait to receive this service for free from a breached institution, other services such as credit freezes and fraud alerts are free or have a minimal charge. In this case, consumers who are exposed to extensive news coverage of a breach may react to it by acquiring fraud protection.

Some literature has examined the effects of the news on perceptions of risks in various contexts. Kosse (2013) argues that reading news about incidents of debit card skimming may keep even unaffected consumers from using their debit cards. Kahn and Liñares-Zegarra (2016) document that an identity theft experience by a close family member or friend affects an individual's payment choice. Similarly, Gallagher (2014) provides evidence that news may play a role in how people learn about an infrequent event, such as a flood, and motivate them to get protection or insure themselves against such an event. In addition, Kahneman (2011) describes a few behavioral biases, such as availability bias, which may force individuals to increase their subjective evaluations of risk when they hear related news stories about these risks, making them more salient in individuals' minds. We test whether the exposure to news about a breach affects consumers who are not subject to the breach and induces them to acquire the free or paid fraud protection services available to them.

4. Data

4.1. Credit data and fraud protection services

The primary data set used in this paper is the Federal Reserve Bank of New York/Equifax Consumer Credit Panel (CCP). The CCP contains consumer debt information for an anonymized 5% random sample of the U.S. population with credit bureau records or about 12 million consumers each quarter. The sample is chosen based on the last two digits of an individual's SSN.[11] To be included in the sample, a consumer must have at least one credit account actively reported by a lender or servicer, an item of public record within the past seven years, or a bankruptcy filing within the past 10 years (Lee and Van der Klaauw, 2010). Because the sampling criteria are the same in each quarter, the CCP is representative of the U.S. credit bureau population as new consumers gain credit and enter the data set over time, while other consumers leave the data set due to death, inactivity, or emigration.[12] Crucial to our study is that the CCP contains geographic information for the addresses of residences including the census block and zip code.

We supplement the CCP with fraud alert data that the Payment Cards Center at the Federal Reserve Bank of Philadelphia obtained from Equifax. These data provide the activation status and origination month of five different types of fraud protection services for every consumer in the primary 5% CCP sample.[13] These services include initial fraud alerts, extended fraud alerts, credit freezes, credit watches, and opt outs from prescreened offers of credit or insurance. Table 1 summarizes the main features of these fraud protection services. Table 2 shows the summary statistics for the protection services and credit variables we use in this study. While the credit bureau data set covers Q1:2010 through Q1:2016, data on fraud protection services are available for Q1:2010–Q3:2014 only.

[10] For example, according to the Identity Theft Resource Center, there were 780 breaches with 178 million records stolen in 2015, and 662 breaches with 16 million records exposed in 2010.

[11] Our data do not include SSNs. Equifax uses SSNs to assemble the data set, but these are not shared with researchers. In addition, the data set does not include any names, addresses, demographics (other than age), or other codes that could identify specific consumers or creditors.

[12] To control for *fragments* in the CCP, we only include consumers who have been in the data set for at least five quarters. See Cheney et al. (2014) for further discussion about fragments and the implications of this constraint.

[13] The month of origination is only provided for initial alerts, extended alerts, and credit freezes. We estimate the quarter of origination for opt outs and credit watches by the quarter in which one of these services first presents itself as active on a consumer's credit bureau file.

Table 2
Data breach sample statistics.

Variable	Non-missing observations	Mean	Standard deviation
Initial fraud alerts (fraction)	16,433,756	0.002	0.041
Extended fraud alerts (fraction)	16,866,527	0.0003	0.016
Credit freezes (fraction)	16,821,807	0.0005	0.022
Credit offers opt outs (fraction)	12,555,122	0.006	0.079
Credit watches (fraction)	14,166,509	0.009	0.095
Risk score	20,353,470	676	111
Total card balance ($)	13,387,673	10,219	34,240
Total credit card limit ($)	13,354,018	32,793	59,510
Number of open cards	17,717,100	3.632	3.781
Number of 30 days past due on cards	15,775,676	0.334	1.292
Percent of cards in good standing (fraction)	12,196,316	0.879	0.310
Number of new cards opened within 6 months	17,715,098	0.243	0.607

Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia
Notes: This table presents summary statistics for individuals in our sample. Extended alerts, freezes, opt outs, and credit watches are dynamic variables that become missing after a consumer has filed the first protection. Initial alerts are not dynamic because they only persist for one quarter. Other variables can be missing for a variety of reasons, including thin files, incomplete tradeline information, or exclusion categories.

Credit bureaus place initial fraud alerts on consumers' files free of charge for consumers who assert "in good faith a suspicion that the consumer has or is about to become a victim of fraud or related crime, including identity theft."[14] These alerts last for 90 days, and consumers can renew them repeatedly. Extended fraud alerts are also free of charge but require the consumer to file a police report before placing the alert in a credit bureau file. These alerts last up to seven years and include a five-year period of exclusion from prescreened credit card and insurance solicitations. Lenders must take additional steps to verify an applicant's identity when granting credit to anyone whose credit report has an active initial or extended alert.

Credit freezes are a fee-based service unless the state law requires them to be provided for free. The existence and size of a fee to initiate and disable the credit freeze temporarily or permanently also varies by state. Credit freezes differ from initial and extended alerts in that a credit freeze completely blocks access to the flagged credit bureau record until the freeze is lifted. Credit freezes are free in South Carolina and North Carolina, while in Georgia, there is a $3 fee to file, temporarily lift, or permanently lift a freeze.[15]

Credit watches, such as Experian's ProtectMyID Alerts, are commercial services offered by credit bureaus and security companies to monitor a consumer's credit bureau file for fraud activity. In our data set, we have information on credit watch services offered by Equifax and those from other companies that are recorded at the three major credit bureaus. Although the monthly fee varies among service providers, all credit watch services have similar features.[16] First, they notify consumers of any changes in the monitored credit bureau files. Second, they provide unlimited access to credit reports and identity theft insurance. In addition, credit watches allow filers to contact an identity theft specialist with fraud-related questions. Finally, credit watches from Equifax offer the option to request that Equifax files initial alerts every 90 days on the consumer's behalf.[17] As mentioned in Section 2, the SCDOR made ProtectMyID Alerts and CSID credit watches available to affected consumers for free.

Consumers who do not want to receive prescreened offers of credit or insurance can voluntarily opt out of such offers. After a period of five years, the consumer may choose to renew the opt-out provision for another five-year period.

The different types of fraud protection services considered in this paper vary in their costs and credit implications for the consumer.[18] Initial alerts and extended alerts are free options and do little to hinder future access to credit. Opt outs are also free, but they may prevent the consumer from receiving attractive credit and insurance offers through the mail. Both credit watches and credit freezes may include fees, but victims of a data breach may obtain these services for free, at least for a period of time. All else equal, credit watches are not as restrictive as credit freezes, which completely prevent credit inquiries.

4.2. Temporal and geospatial effects of the breach

Using geographic information from the CCP, we aggregated fraud protections at the state and census tract levels to examine temporal and geospatial trends surrounding the SCDOR data breach in Q4:2012. Fig. 1 reports the quarterly number of fraud protections per capita acquired in Georgia, North Carolina, and South Carolina during the Q1:2010–Q3:2014 time period. It is immediately evident that South Carolinians responded significantly to the data breach by filing initial alerts, credit freezes, credit watches, and opt outs. The number of new credit watches — the largest number of any alert type filed — increased by approximately 4000% between Q3:2012 and Q4:2012. This increase amounted to approximately 40,000 consumers.

Similarly, the number of credit freezes filed in South Carolina at the time of the breach increased by about 2381%, the number of initial alerts increased by about 562%, and the number of opt outs increased by about 104%. The increased number of protections filed by South Carolinians persisted for about two quarters before returning to pre-data breach levels, with the exception of credit watches, which continued to be filed at elevated rates through Q2:2013. This is likely to have occurred because the SCDOR extended the deadline to enroll in free credit watches until March 31, 2013.

No such obvious trend can be observed in Georgia or North Carolina, although it is notable that, prior to the data breach, Geor-

[14] See Fair and Accurate Credit Transactions Act of 2003, §112.
[15] See www.experian.com/consumer/help/states/nc.html.
[16] The monthly fee ranges from $12.95 to $29.95 for credit watch products offered by Equifax.
[17] See www.equifax.com/credit-watch-gold/.
[18] See Cheney et al. (2014) for more details on initial alerts, extended alerts, and credit freezes as well as their selection based on credit market behavior.

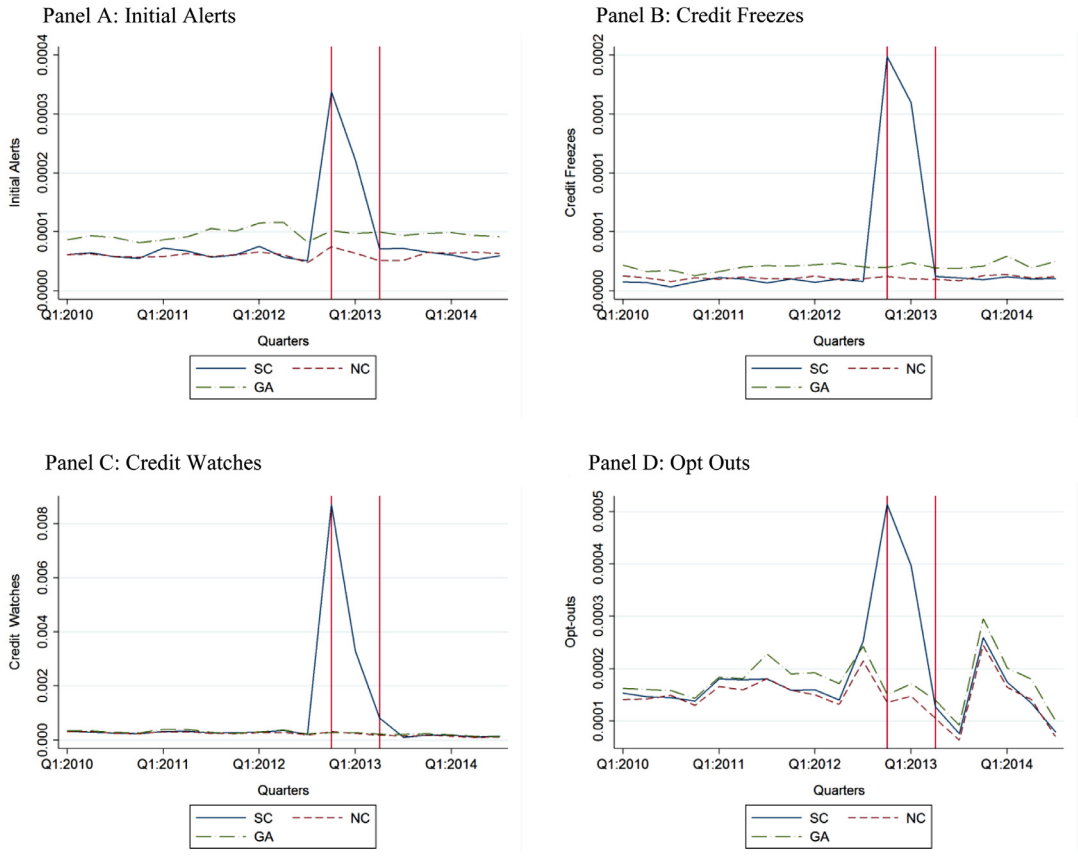

Fig. 1. Number of fraud protection services per capita adopted before and after the South Carolina data breach.
Notes: These figures show the number of fraud protection services divided by the estimated state population in each state over time. We calculate quarterly state population from the U.S. Census' annual population estimates using linear interpolation. Vertical lines denote Q4:2012 and Q2:2013. There is a significant response across all fraud protection services for consumers in South Carolina at the time of the breach (Q4:2012) and the following quarter (Q1:2013). Only the fraction of the population filing credit watches remains elevated in South Carolina in Q2:2013.
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia.

gia had more protections filed per capita per quarter compared with South Carolina. Before the breach, all three states had similar trends in fraud protection filings.

We also find evidence of consumer reaction to the SCDOR data breach in the temporal-geospatial dimension. Figs. 2–5 are heat maps of the total number of alerts filed as a percentage of census tract population (as provided by the 2010 Census) for Georgia, North Carolina, and South Carolina.[19] Initial alert filings were well below 1% of the population in census tracts across all states before surging upward in South Carolina during Q4:2012. While the adoption of fraud protection services surged in Q4:2012 in South Carolina, that was not the case in neighboring North Carolina and Georgia, where it was flat. Moreover, the effect of the breach on initial alerts, freezes, credit watches, and opt outs in South Carolina dissipated rapidly; the rate of adoption of all services, except for credit freezes, returned to pre-breach levels by Q2:2013.

The relative increase in the percentage of the population filing initial alerts, credit freezes, credit watches, and opt outs was so large in some South Carolina census tracts that we winsorized the data at the 99th percentile. If we had not done so, the intensity of alerts filed in other locations and time would not be visible in the figures. With the exception of credit watches, there were small, nonsystematic patterns of alert filings in Georgia and North Carolina. In multiple census tracts in South Carolina during Q4:2014, 2% or more of their population filed credit freezes and 3% or greater of their population filed opt outs. Opt outs do not afford direct fraud protection by monitoring credit bureau files in the way of initial alerts, credit freezes, and credit watches; however, consumers may use opt outs to prevent prescreened solicitations from ending up in the hands of criminals who may have routed the mail to a different address. Fig. 5 shows that, unlike other types of alerts, opt outs are pervasive even in periods prior to and following the SCDOR data breach (Q3:2012 and Q2:2013) across all three states where about 1% of the population of most census tracts requested an opt out per quarter.

Almost all census tracts in South Carolina had more than 10% of their population file credit watches, and a substantial proportion of census tracts had 20% or more of their populations do so. In addition, in the Q4:2012–Q2:2013 period, more than 29% of the credit bureau population of South Carolina acquired a credit watch. The credit watch maps (Fig. 4) show higher rates of filing in South Carolina compared with Georgia and North Carolina up to Q2:2013. This level of persistence is not observed in any other type of alert.

[19] A heat map of the total number of extended alerts is reported in Fig. A.1 in the Appendix. Extended alerts were not systematically filed in any state during these time periods.

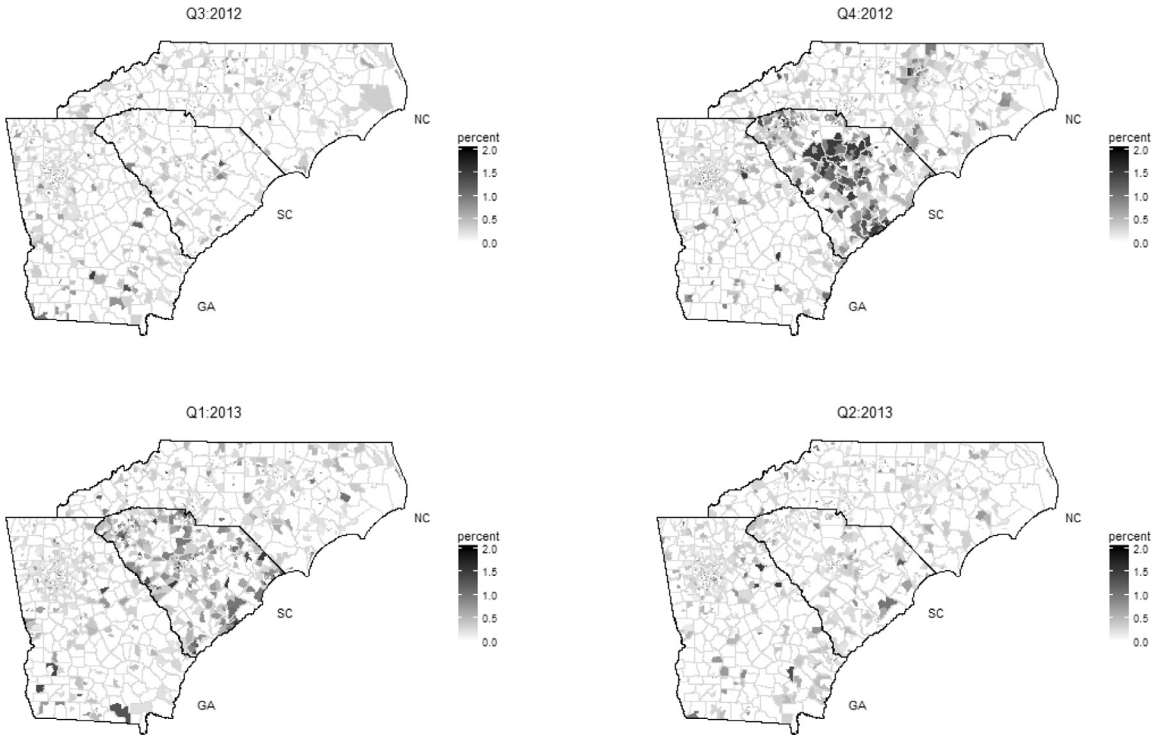

Fig. 2. Initial alerts as a percentage of census tract population.
Notes: These maps show the percentage of the 2010 Census tract populations that filed an initial alert for the first time during the quarters immediately before, during, and after the breach. The percentages of initial alerts are winsorized at the 99th percentile to eliminate outliers. Up to 2% of some South Carolina census tract populations filed initial alerts at the time of the breach.
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia.

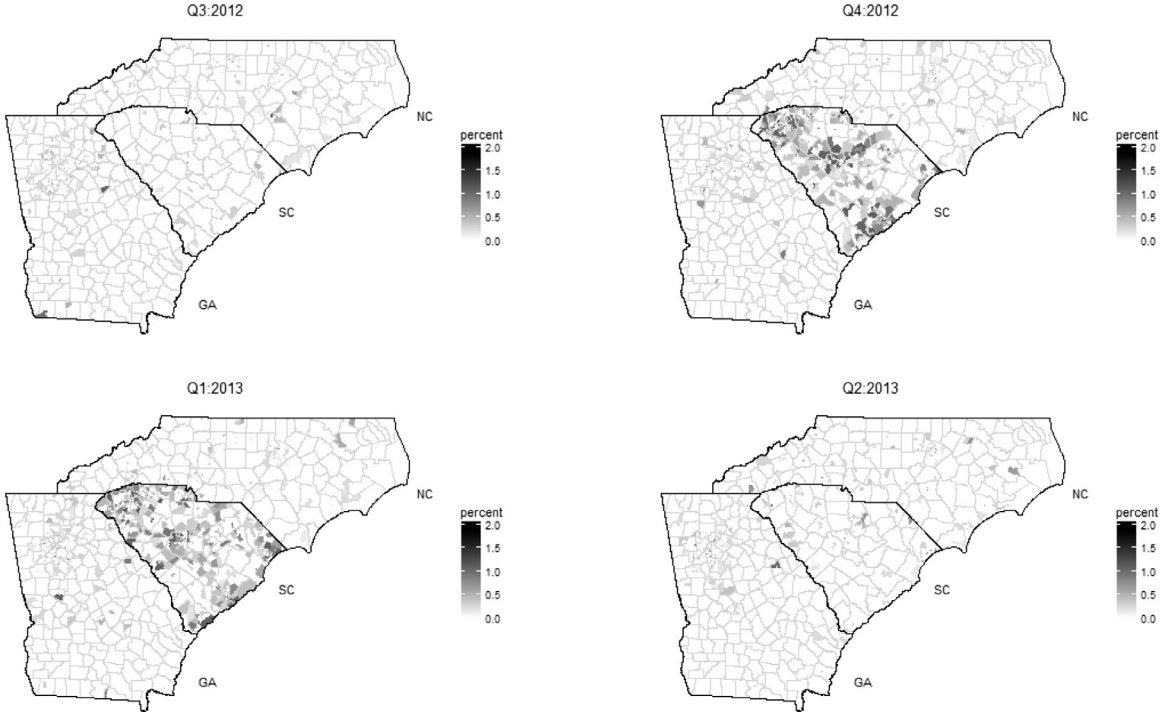

Fig. 3. Credit freezes as a percentage of census tract population.
Notes: These maps show the percentage of the 2010 Census tract populations that filed a credit freeze for the first time during the quarters immediately before, during, and after the breach. The percentages of credit freezes are winsorized at the 99th percentile to eliminate outliers. Up to 2% of some South Carolina census tract populations filed credit freezes at the time of the breach.
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia.

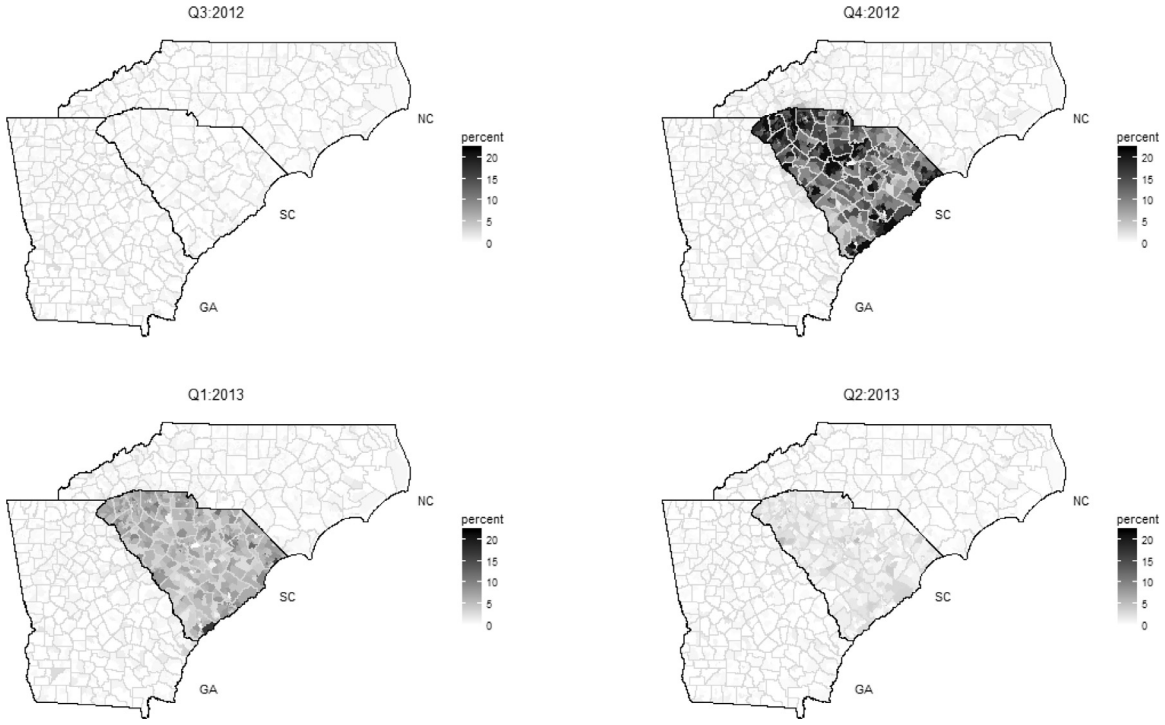

Fig. 4. Credit watches as a percentage of census tract population.
Notes: These maps show the percentage of the 2010 Census tract populations that filed a credit watch for the first time during the quarters immediately before, during, and after the breach. The percentages of credit watches are winsorized at the 99th percentile to eliminate outliers. Up to 20% of some South Carolina census tract populations filed credit watches at the time of the breach. Credit watches continued to be filed in South Carolina in the quarter after the data breach at a rate of about 10%.
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia.

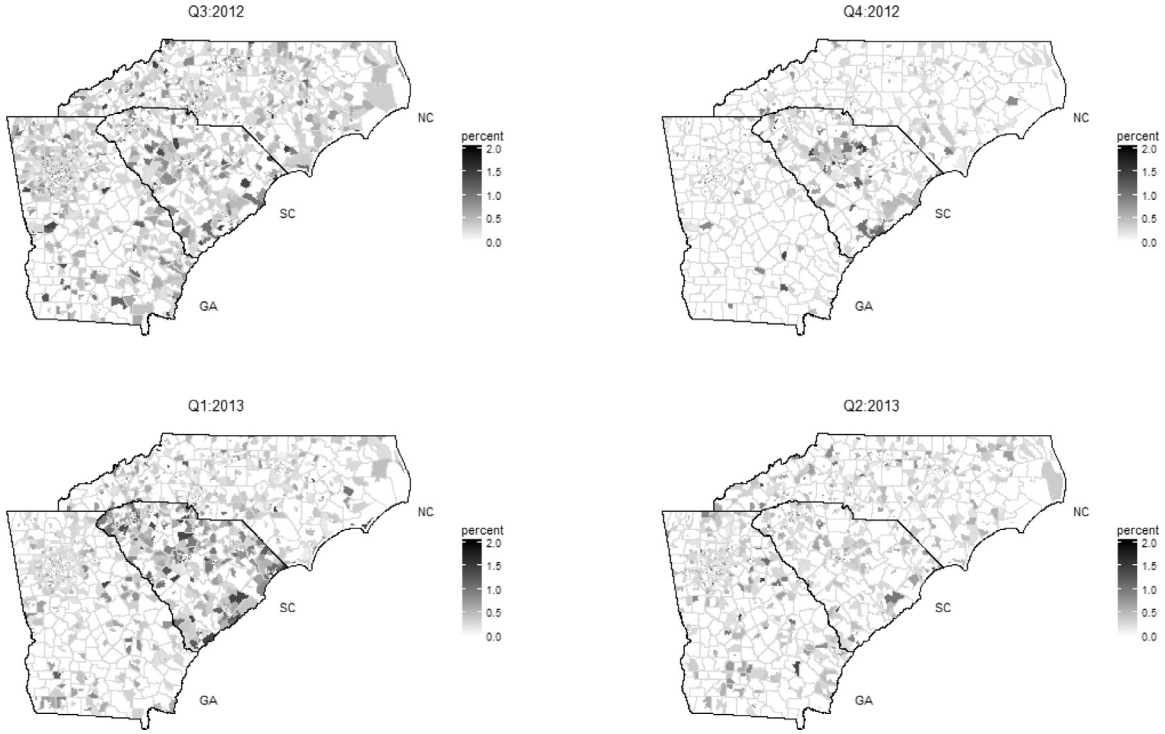

Fig. 5. Opt outs as a percentage of census tract population.
Notes: These maps show the percentage of the 2010 Census tract populations that filed an opt out for the first time during the quarters immediately before, during, and after the breach. The percentages of opt outs are winsorized at the 99th percentile to eliminate outliers. Up to 2% of some South Carolina census tract populations filed opt outs at the time of the breach. Opt outs were widespread among the three states before and after the breach occurred.
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia.

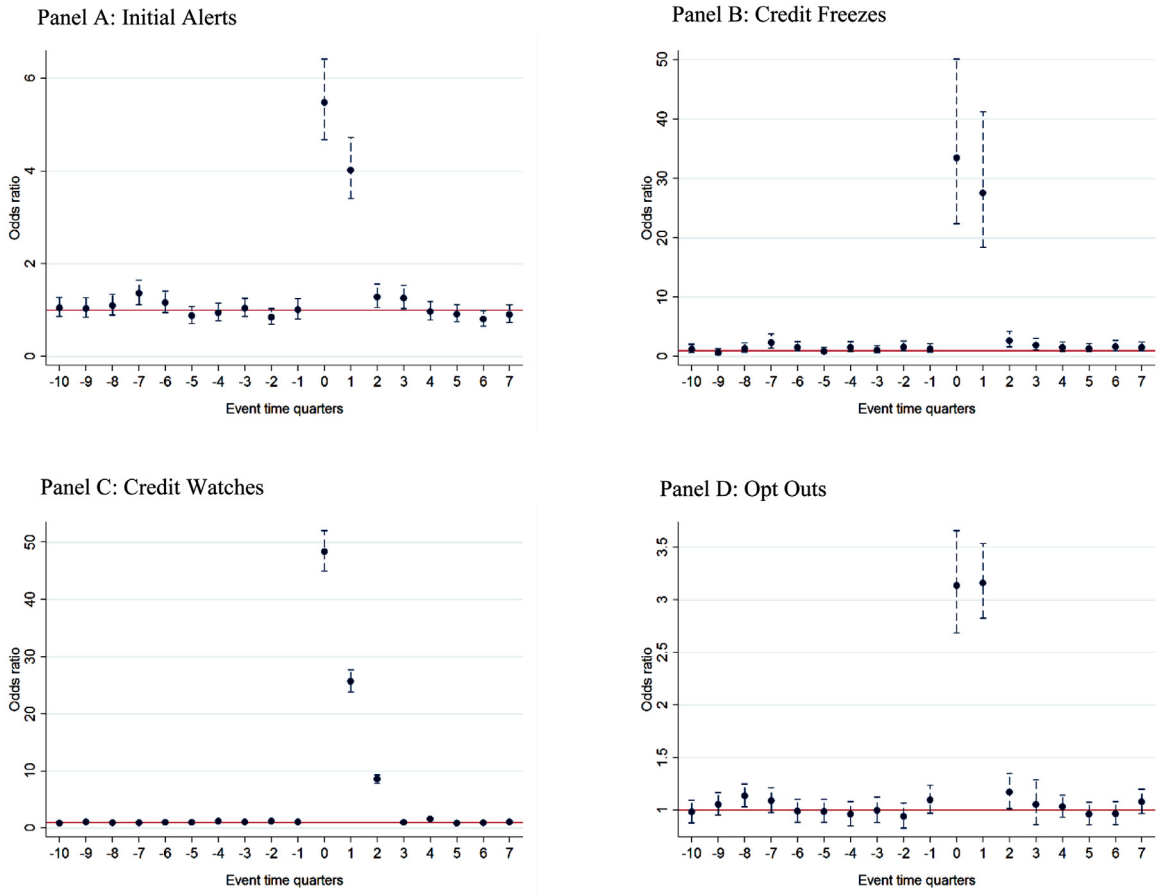

Fig. 6. Fraud protection take-up in South Carolina versus North Carolina and Georgia.
Notes: These figures show the odds ratios for the likelihood of filing a specific type of protection for individual consumers in South Carolina compared with consumers in North Carolina and Georgia. These odds ratios come from dynamic logistic regressions with control variables as described in the text. Dots represent estimated odds ratios bound by 95% confidence bands shown as vertical dashed lines. Standard errors are clustered at the individual level. South Carolina consumers were more likely to file for any type of fraud protection in the quarter of the breach and immediately afterward. The effect was largest for credit watches, with South Carolinians being 48 times more likely to file a credit watch during the breach compared with North Carolinians and Georgians. The credit watch filings showed a statistically significant increase for two quarters after the breach.
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia.

5. Data breach and fraud protection

We estimate an individual's probability of adopting a certain fraud protection service as a function of individual characteristics, the data breach, and other factors. We focus on the adoption decision because maintenance of fraud protections is mostly mechanical and automatic.[20] Our main specification is as follows:

$$Y_{i,t} = \beta_0 + \beta_1 time_t + \beta_2 state_s + \beta_3 time_t * SC_s + \beta_4 age_{i,t} + \varepsilon_{i,t}. \quad (1)$$

We use a dynamic logit model to estimate Eq. (1) separately for each type of fraud protection. The dependent variable $Y_{i,t}$ indicates whether an individual acquired one of the fraud protection services (initial alert, extended alert, credit freeze, watch, or opt out) in a particular quarter. These variables are equal to 0 in the quarters prior to the first appearance of a protection service in an individual's file. They are equal to 1 when an individual first adopts a protection. After that, this individual is dropped out of the sample. This definition of the dependent variables is similar to the one used in Gross and Souleles (2002) and Elul et al. (2010). It is designed to account for the fact that most alerts, freezes, and other protections are very persistent. Hence, once someone files an alert, oftentimes this person would have no reason to file it again.

This dynamic logit specification is equivalent to discrete duration models as pointed out by Gross and Souleles (2002) and argued in Shumway (2001). Similar to Gross and Souleles (2002) and Elul et al. (2010), we attempt to capture the baseline hazard function using a fifth-order polynomial in age. Because our unit of analysis is an individual – not a credit card account or mortgage – we use the individual's age in years. We also include quarter fixed effects (*time*) and state fixed (*state*) effects into the model (with indexes *t* and *s*, respectively). Finally, we cluster standard errors at the individual level.

The major variables of interest to us in Eq. (1) are interactions of quarter fixed effects and an indicator variable for residents of South Carolina (SC_s). These variables show the changes in the likelihood of residents of South Carolina acquiring one of the fraud protections compared with residents of North Carolina or Georgia in every quarter of the sample after controlling for other factors described previously. The implicit assumption in the event study identification strategy used later is that, in the absence of the breach, trends in the adoption of fraud protection services would

[20] For instance, a credit freeze remains active until the consumer takes some action to cancel it. Credit watches, however, which were provided for 12 months and then for another period of time with a different vendor, require decision making by the consumer for both the initial sign-up and the renewal. An initial fraud alert, which expires within 90 days, is the only mechanism that requires action on the consumer's part every quarter to maintain protection.

be the same in our control group (residents of North Carolina and Georgia) and treatment group (residents of South Carolina). We check the validity of this assumption by looking at the two groups before the breach. We can also see the effect of the breach on fraud protections directly at the time of the event.

Fig. 6 plots the estimated coefficients on the interactions of quarter dummies with the South Carolina indicator from Eq. (1). Panels A–D in this figure present the coefficients for the odds ratios for the likelihood of acquiring one of the four fraud protection services: initial fraud alert, credit freeze, credit watch, and opt out, respectively. In addition to the coefficients, we show 95% confidence intervals as bands. The omitted quarter dummy is Q1:2010, so all results are relative to this time period. The coefficients are reported as odds ratios with a coefficient of 1, implying no effect on the likelihood of fraud protection take-up. Event time quarters (the x-axis) are normalized so that the time of the breach (Q4:2012) is equal to time 0.

One noticeable result seen in all Fig. 6 panels is that the take-up of all four fraud protections jumped at the time of the breach and remained elevated in the quarter following it. The take-up returned to normal levels in the following quarters. The only service with an elevated level of adoption two quarters after the breach is the credit watch. These results are consistent with those seen in earlier figures (Figs. 1–5), showing a strong, even if short lived, response of consumers to the SCDOR data breach. Fig. 6, however, provides additional evidence as it presents the difference in consumer reaction in the affected area (South Carolina) relative to the control areas (North Carolina and Georgia) and after controlling for the time and state fixed effect and the consumer's age. The lack of any difference in fraud protection acquisition between the population of South Carolina and the consumers in North Carolina and Georgia before the data breach (time −10 to −1) suggests that residents of North Carolina and Georgia are an appropriate control group for South Carolina residents affected by the breach in Q4:2012.[21]

Fig. 6 also reveals that consumers used available protections to a varying degree. The odds of a credit watch adoption (Panel C) increased 48 times at the time of the data breach, whereas initial alerts and opt outs were five times and three times more likely to be acquired, respectively. Credit freezes were in between these two extremes, with an odds ratio of 34. This divergent take-up of fraud protections might be explained by the emphasis placed on credit watches in the SCDOR communications and remedy actions (i.e., offering and advertising a complimentary ProtectMyID Alert credit watch to all victims). The other protection services, however, were only mentioned in some communications (informational pamphlets) and not promoted widely. Hence, the relatively strong consumer response in terms of credit freezes is somewhat surprising.

6. Data breach and consumer credit use

While the previous sections presented clear evidence that consumers affected by the South Carolina data breach responded to the event by acquiring various fraud protection services, this section focuses on other ways data breach victims may react to a data breach. In particular, we examine whether and how data breach victims changed their credit card usage and payment behavior. This area is important because previous studies have shown that security may be an important feature in consumer choice of payment mechanisms (Stavins, 2013; Kahn and Liñares-Zegarra, 2016). For example, it is possible that consumers may reduce their card usage or switch lenders after a data breach, if they believe that some lenders are more secure than others.

To test these hypotheses, we run a modified version of the specification in Eq. (1). We use the number of open credit cards, new credit cards, total card balance, credit card limit, the number of 30-day delinquencies on credit cards, and other credit variables as outcome variables. We also use simple OLS models for these outcomes instead of dynamic logits used in the previous section. The rest of the specification in Eq. (1) remains the same.

Fig. 7 shows the effect of the South Carolina data breach on credit cards of affected consumers relative to the behavior of consumers in neighboring states. Overall, there is no evidence that consumers closed existing credit cards after the breach as indicated in Panel A. Panel B shows that data breach victims did not open new credit cards either. These two results suggest that the breach victims do not seem to switch lenders after the security incident. Total balances on credit cards seem to grow slowly — but mostly statistically insignificant — after the breach (Panel C), which may indicate that consumers kept using their existing cards after the security incident.[22] Finally, the results in Panel D indicate that consumers did not become more or less delinquent on their credit cards after the breach.

Fig. 8 demonstrates that the data breach had little to no effect on other credit variables. In particular, the percent of credit cards in good standing (Panel A) increased somewhat after the breach with this effect being statistically significant but economically very small. The risk score decreased by a statistically insignificant amount – 0.25 points to 0.5 points – after the breach (Panel B). Panel C shows that breach victims are more likely to have their credit card limits increased by lenders. This finding may be an indication that lenders attempted to maintain the loyalty of breached consumers by providing them with higher credit card limits. Finally, Panel D shows that, after the breach, affected consumers have about the same probability of filing an extended fraud alert as unaffected consumers. Because this type of fraud alert requires a police report or identity theft report and evidence of fraud, breach victims did not appear to be more likely to be victimized further by criminals.

Taken together, the findings presented in Figs. 7 and 8 seem to suggest that data breach victims did not alter their credit card usage or payment behavior in a negative way. They also did not seem to change lenders by acquiring new credit cards. Thus, it seems that this event had little bearing on consumer risk scores or consumers' interactions with the credit market. On the other hand, these results may also show that many of these consumers were not subject to additional losses from criminals' fraudulent use of their personal data in the three years after the data breach, which we can observe in our sample. Such fraudulent use of consumer data might have resulted in new credit cards, higher balances, and an uptick in additional delinquencies.

7. Television media markets and fraud protection adoption

7.1. The dissemination of news through media markets

In this section, we attempt to measure the effect of the news about the breach on both consumers who were exposed to the breach and unaffected individuals. Several recent studies emphasized the importance of news media coverage on the formation of public opinion, sentiments, and beliefs about risks. Soo (2015) argues that news sentiment about the housing market affects house prices, trading volume, and expectations. Azzimonti (2014) finds

[21] We also checked if economic conditions were similar in these three states using State Coincident Indexes developed by the Federal Reserve Bank of Philadelphia. The three states seem to be moving in parallel in terms of economic conditions. For additional details, see www.philadelphiafed.org/research-and-data/regional-economy/indexes/coincident.

[22] Comparable results are found for the logarithm of total credit card balances.

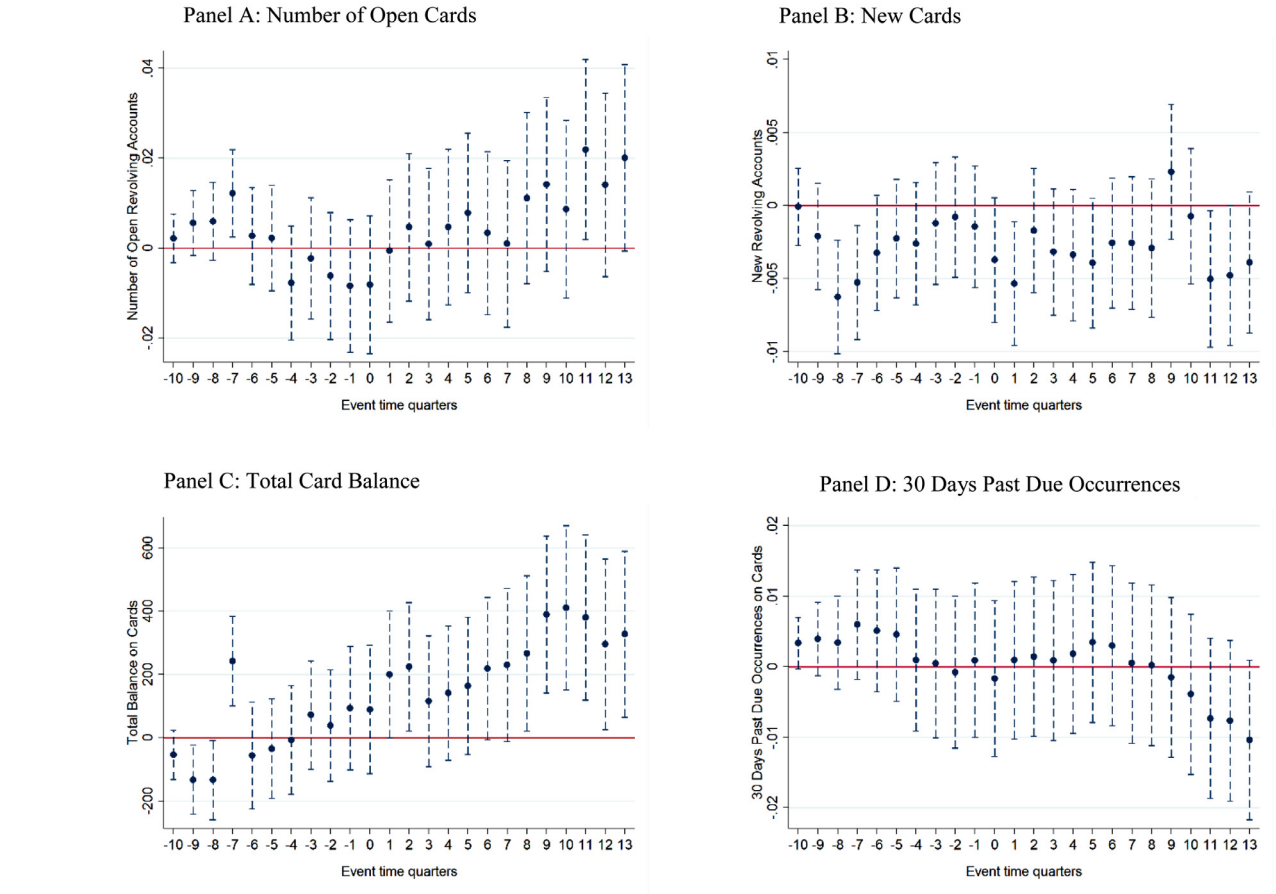

Fig. 7. Credit card use in South Carolina versus North Carolina and Georgia after the breach.
Notes: These figures show the changes in credit variables for individual consumers in South Carolina compared with consumers in North Carolina and Georgia before and after the breach. These coefficients come from OLS regressions with control variables as described in the text. Dots represent estimated coefficients bound by 95% confidence bands shown as vertical dashed lines. Standard errors are clustered at the individual level. After the South Carolina data breach, affected consumers did not change their credit card use behavior compared with the control group (North Carolinians and Georgians).
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia.

that a news index measuring partisan conflict and political polarization may be linked to uncertainty and decreases in investment, output, and employment. Kosse (2013) suggests that news on debit card fraud may discourage cardholders from using this payment option.

To test this channel of influence, we use an empirical strategy similar to the work by Gallagher (2014) and rely on data about Nielsen's DMAs. The Nielsen Company (Nielsen) conducts research on the shares of viewers of particular television stations in U.S. counties. These counties are organized into DMAs, or media markets, based on viewers' preferences for television channels and programs. Thus, residents of a particular media market are likely to view similar programs, including news on the data breach. However, viewers of a different market may see other local news on a different topic, such as identity theft. This is important for us because the boundaries of media markets and states do not coincide, with some DMAs being completely inside a state and others stretching across state borders. Therefore, we are able to separate the effect of the news about the data breach (residing in the affected television media market) from the effect of the exposure to the data breach (residing in South Carolina).

We group counties within seven DMAs created by Nielsen for South Carolina, North Carolina, and Georgia into three categories based on their location and whether their DMAs reaches across state borders: 1) NC/GA Shared – counties inside of North Carolina and Georgia that share a DMA with counties inside of South Carolina; 2) SC Shared – counties inside of South Carolina that share a DMA with counties inside of North Carolina and Georgia; 3) SC Unshared – counties in South Carolina that do not share a DMA with any bordering state. The DMAs in South Carolina that do not cross borders are Columbia and Charleston. The DMAs that cross borders are Savannah, Augusta-Aiken, Greenville-Spartanburg-Asheville-Anderson, Charlotte, and Myrtle Beach-Florence. Fig. 9 plots our defined groups of counties in South Carolina, Georgia, and North Carolina. In the subsequent analysis, we compare these three groups with the control group, which consists of residents of North Carolina and Georgia who are not sharing media markets with South Carolina.

Our identification strategy is based on the idea of differences in the exposure to the data breach or news about it among these three groups. It can be argued that residents of inner and outer South Carolina media markets are both equally likely to be exposed to the data breach. However, residents of South Carolina sharing media markets with North Carolina or Georgia, which were unaffected by the breach, may receive less news about the data breach than residents of inner South Carolina media markets. This proposition is based on the variation in local news programming and the argument that residents of the shared media regions receive news pertinent to South Carolina and North Carolina or Georgia. Hence, the news about the breach for South Carolina residents in

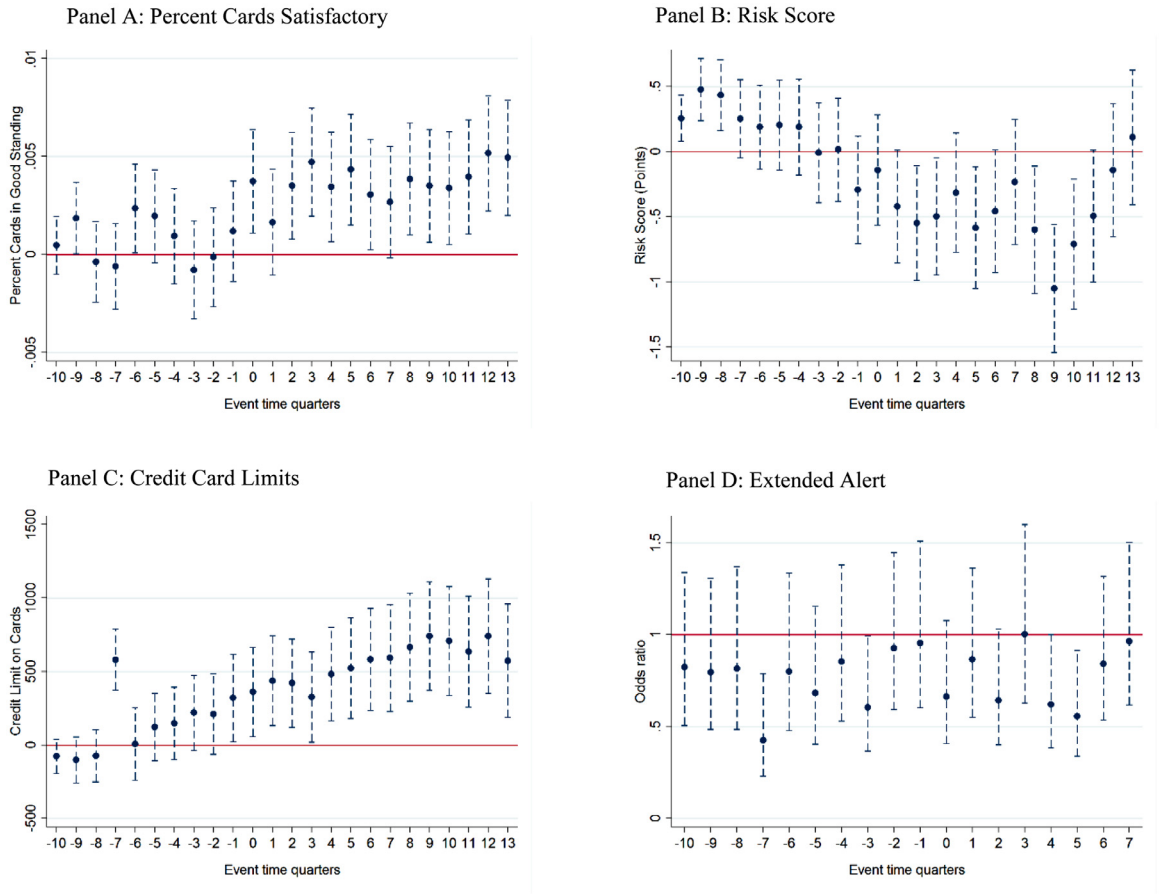

Fig. 8. Credit standing in South Carolina versus North Carolina and Georgia after the breach.
Notes: These figures show the changes in credit variables for individual consumers in South Carolina compared with consumers in North Carolina and Georgia before and after the breach. These coefficients come from OLS regressions with control variables as described in the text. Dots represent estimated coefficients bound by 95% confidence bands shown as vertical dashed lines. Standard errors are clustered at the individual level. After the South Carolina data breach, affected consumers did not change their credit card use behavior compared with the control group (North Carolinians and Georgians).
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia.

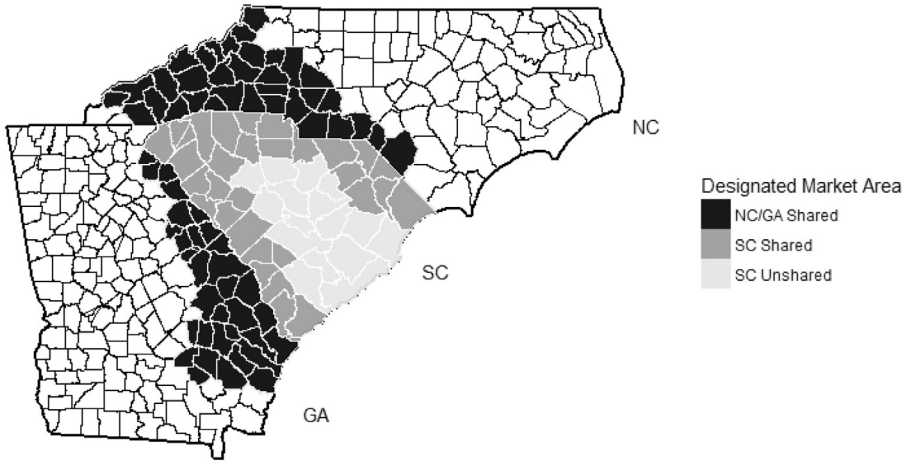

Fig. 9. Designated Market Area (DMA) regions.
Notes: This map shows counties within DMAs created by Nielsen for South Carolina, North Carolina, and Georgia. We group these counties into three categories based on their location and whether their DMA reaches across state borders: 1) NC/GA Shared – counties inside of North Carolina and Georgia that share a DMA with counties inside of South Carolina; 2) SC Shared – counties inside of South Carolina that share a DMA with counties inside of North Carolina and Georgia; 3) SC Unshared – counties in South Carolina that do not share a DMA with any bordering state.
Source: Authors' calculations using data from Nielsen.

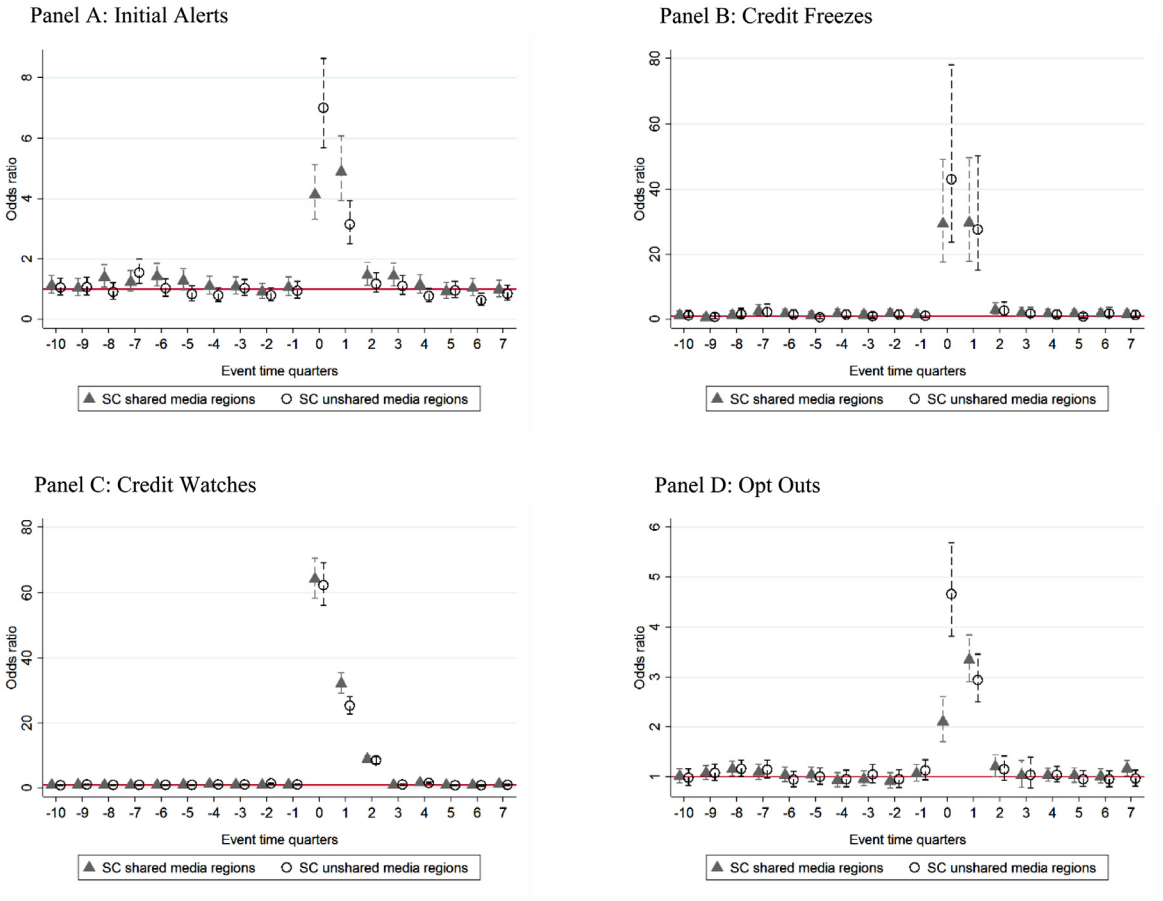

Fig. 10. Fraud protection take-up in South Carolina's shared and unshared media markets.
Notes: These figures show the odds ratios for the likelihood of filing a specific type of fraud protection for individual consumers in South Carolina counties that shared media markets with counties in other states and those that do not (as indicated by the markers explained in figures' legend). These odds ratios come from dynamic logistic regressions with control variables as described in the text. Dots represent estimated odds ratios bound by 95% confidence bands shown as vertical dashed lines. Standard errors are clustered at the individual level. For some protections, consumers in South Carolina counties that did not share media markets with counties in other states responded more strongly to the data breach than did consumers who shared media markets.
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia.

the shared media regions might be diluted by reporting on events more relevant to residents of Georgia and North Carolina. Thus, if some response to the breach was driven by news coverage, we would expect a stronger reaction among residents of inner South Carolina media markets compared with residents of South Carolina media markets shared with the other states.

7.2. The effect of news on breach victims

Fig. 10 plots coefficients from the interaction of quarter indicators with South Carolina shared (denoted by triangles) and unshared (depicted as circles) media market indicators. The rest of the specification is the same as in Eq. (1). Similar to Fig. 6, we provide odds ratios for the likelihood of acquiring one of the four fraud protection services as dots and 95% confidence intervals as bands. As seen in Fig. 10, individuals affected by the data breach acquired more fraud protection services of all types in inner and outer regions of South Carolina at the time of the breach and a quarter or two afterward. However, the take-up of initial fraud alerts and opt outs is significantly lower in the South Carolina shared media markets compared with the South Carolina inner media markets at time $t = 0$.[23] The point estimate for credit freezes is also lower for the South Carolina shared regions, but it is not statistically different from the point estimate for the South Carolina unshared markets. This discrepancy in reaction is eliminated one quarter after the breach (time 1), and shared and unshared regions return to long-term trends after that. Thus, there is an effect of news coverage on consumers exposed by the breach, but it is relatively small and transient. This finding shows that local media reporting on data breaches does not seem to amplify the effect of a data breach on the breached consumers.

7.3. The effect of news about the breach on neighbors

In addition to comparing the reactions to data breaches of consumers inside South Carolina who experienced varying degrees of news coverage, we are able to compare individuals who live inside and outside of South Carolina but share the same media markets. This group of individuals received the same amount of information about the data breach and identity theft, but only South Carolina residents had their personal information stolen during the incident. Thus, we can examine whether receiving news about the data breach is sufficient to induce consumers to adopt fraud protection or if the combination of both news and the threat of stolen information is necessary.

Fig. 11 summarizes estimated coefficients from Eq. (1) with some additional interactions. In this specification, we interact quar-

[23] We omitted the fifth order term of consumer's age variable in the opt-out model specification to ensure convergence of the model.

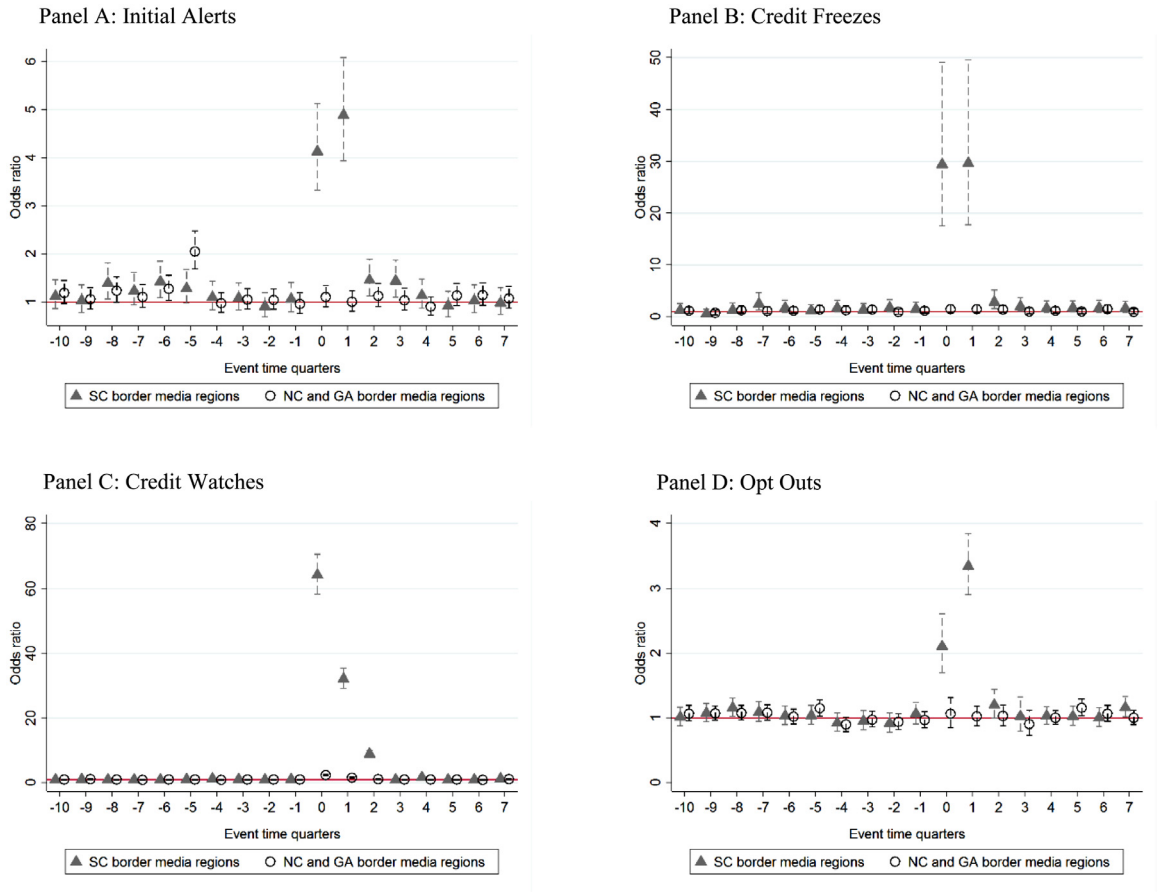

Fig. 11. Fraud protection usage in South Carolina's border media markets versus North Carolina and Georgia's border media markets.
Notes: These figures show the odds ratios for the likelihood of filing a specific type of protection for individual consumers in counties who share media markets between states (as indicated by the markers explained in figures' legend). These odds ratios come from dynamic logistic regressions with control variables as described in the text. Dots represent estimated odds ratios bound by 95% confidence bands shown as vertical dashed lines. Standard errors are clustered at the individual level. Consumers in South Carolina counties that shared media regions were up to 65 times more likely to file a credit watch at the time of the breach compared with consumers outside of South Carolina. The take-up of the other protections among South Carolina residents also increased. Consumers in Georgia and North Carolina who received the same news about the data breach as did South Carolina residents did not react to the breach.
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia.

ter dummies with an indicator for South Carolina shared markets and living in South Carolina and an indicator for South Carolina shared markets and living outside this state.[24] This figure reveals that consumers affected by the breach substantially increased adoption of all fraud protection services at the time of the event. However, consumers who received the same amount of news about the breach but lived across the border in North Carolina or Georgia and, therefore, were not directly affected by the incident, did not increase fraud protection take-up.[25] This finding suggests that receiving information about the South Carolina data breach was not sufficient in itself to lead unaffected consumers to update their beliefs about future data breaches or the likelihood of fraud and to act on these beliefs by acquiring fraud protection. Therefore, it is unlikely that a data breach can generate a widespread panic among individuals who were not affected by the incident directly, and it may be insufficient to motivate such unaffected individuals to alter their beliefs about the data security or breach-related losses.

[24] We also include, but do not report, quarter indicators interacted with inner South Carolina media markets.

[25] We omitted the fifth order term of consumer's age variable in the opt-out model specification to ensure convergence of the model.

8. Conclusion

This paper uses a natural experiment generated by the 2012 SCDOR data breach to study the response of individual consumers to information security events that expose them to potential future monetary losses. We are able to identify likely victims of the breach and link them to a unique database of fraud protection services as well as credit bureau data. The five fraud protection services we use in this study are initial fraud alert, extended fraud alert, credit (security) freeze, credit watch, and credit and insurance solicitation opt out. Using these data, we examine how the take-up of fraud protection services responds to direct exposure from the data breach and television coverage of the incident. We also study how data breach victims react to the incident in terms of their credit card use and payment behavior.

We find that, within two quarters of the data breach event, consumers who were directly exposed responded by acquiring the fraud protections available to them, excluding the extended fraud alert. This tendency is consistent with these individuals being relatively unprotected against fraud and identity theft before the incident and protecting against further fallout from the breach. The very high relative rate of take-up of protections among this population may be because highly salient notifications were sent by the

South Carolina government on the state's letterhead. Data breaches with less formal notifications or with less clarity about the affected population may elicit a different response from consumers. Nevertheless, even with this notification from a credible source, only 29% of consumers with credit bureau files signed up for free credit watches. This finding may imply that breach notifications are not the most effective mechanism to protect consumers from identity theft after a data breach. While breach notifications, and accompanying litigation costs, and stock price declines may induce firms to invest in consumer data protection regardless of consumers' actions. If consumers do not react to breach notifications and do not acquire fraud protection services, it may be more efficient to strengthen firms' data security standards to make data breaches and accompanying identity theft less likely.

While some data breach victims acquired the various fraud protection services after the breach, they did not seem to change their use of credit cards or interactions with the credit market. In particular, we find that there was no change in the number of cards these affected consumers carried; they also did not obtain new cards from other lenders. The breach did not affect card balances, 30-day card delinquencies, percent of cards in good standing, or consumers' risk scores. The security event also did not seem to increase the probability of an extended fraud alert filing, which requires evidence of fraud and a police report. These findings may imply that data breaches do not affect victimized consumer interactions with credit and payments markets.

We also find that individuals who were not directly affected by the breach but who share the same television markets and were thus subject to the same amount of media coverage of the breach, generally did not respond to this breach by acquiring fraud protection. We conclude that, in this instance, consumers primarily responded to clear and direct evidence of their own exposure to a breach. In the absence of a clear indication of their own direct exposure, consumers did not appear to revise their beliefs about future expected losses associated with data breaches and act on these beliefs to acquire fraud protection services. This finding suggests against the possibility of a panic after a data breach that extends beyond those directly affected by the incident.

Appendix

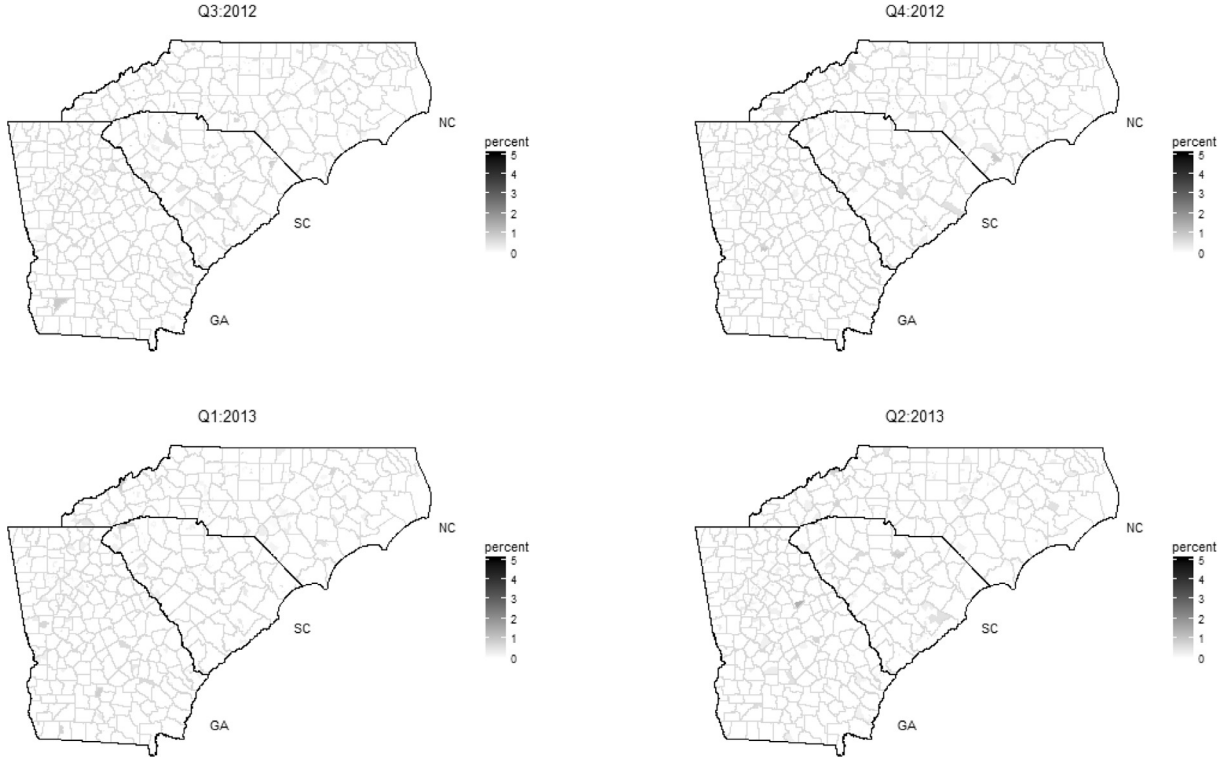

Fig. A.1. Extended alerts as a percentage of census tract population.
Notes: These maps show the percentage of the 2010 Census tract populations that filed an extended alert for the first time during the quarters immediately before, during, and after the breach. Extended alerts were not systematically filed in any state during these time periods.
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia.

References

Ablon, L., Heaton, P., Lavery, D., Romanosky, S., 2016. Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information. RAND Corporation, Santa Monica, CA.

Azzimonti, M., 2014. Partisan Conflict. Federal Reserve Bank of Philadelphia Working Paper 14–19.

Campbell, K., Gordon, L., Loeb, M., Zhou, L., 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. J. Comput. Secur. 11 (3), 431–448.

Cheney, J.S., Hunt, R.M., Jacob, K.R., Porter, R.D., Summers, B.J., 2012. The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risks Posed by Data Breaches. Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper 12-04.

Cheney, J., Hunt, R., Mikhed, V., Ritter, D., Vogan, M., 2014. Consumer Use of Fraud Alerts and Credit Freezes: An Empirical Analysis. Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper 14-04.

Durrette, K., 2012. SC Department of Revenue Hacked; Millions of SC Residents Affected. Wach TV Station, Columbia, SC Available at (last accessed 09/21/2017): wach.com/news/local/sc-department-of-revenue-hacked-millions-of-sc-residents-affected?id=817902.

Elul, R., Souleles, N., Chomsisengphet, S., Glennon, D., Hunt, R., 2010. What 'triggers' mortgage default? Am. Econ. Rev. 100 (2), 490–494.

Gallagher, J., 2014. Learning about an infrequent event: evidence from flood insurance take-up in the United States. Am. Econ. J.: Appl. Econ. 6 (3), 206–233.

Gatzlaff, K., McCullough, K., 2010. The effect of data breaches on shareholder wealth. Risk Manag. Insurance Rev. 13 (1), 61–83.

Greene, C., Stavins, J., 2016. Did the Target Data Breach Change Consumer Assessments of Payment Card Security?. Federal Reserve Bank of Boston Research Data Reports 16-1.

Gross, D.B., Souleles, N.S., 2002. An empirical analysis of personal bankruptcy and delinquency. Rev. Financ. Stud. 15 (1), 319–347.

Harrell, E., 2015. Victims of Identity Theft, 2014. U.S.. Department of Justice, Bureau of Justice Statistics Bulletin NCJ 248991.

Kahn, C., Liñares-Zegarra, J., 2016. Identity theft and consumer payment choice: does security really matter? J. Financ. Serv. Res. 50 (1), 121–159.

Kahneman, D., 2011. Thinking, Fast and Slow. Straus and Giroux, New York Farrar.

Kosse, A., 2013. Do newspaper articles on card fraud affect debit card usage? J. Bank. Financ. 37 (12), 5382–5391.

Kwon, J., Johnson, M.E., 2015. The market effect of healthcare security: do patients care about data breaches? In: Proceedings of the Workshop on the Economics of Information Security (WEIS 2015).

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

McGrath, M., 2014. Target Profit Falls 46% on Credit Card Breach and the Hits Could Keep on Coming. Forbes February 26, 2014.

McLeod, H., 2012. South Carolina Raises Number of Hacked Tax Records to 3.8 Million. Reuters Available at (last accessed 09/21/2017): www.reuters.com/article/2012/11/07/usa-southcarolina-taxes-idUSL1E8M7NVO20121107.

Romanosky, S., Telang, R., Acquisti, A., 2011. Do data breach disclosure laws reduce identity theft. J. Policy Anal. Manag. 30 (2), 256–286.

Shumway, T., 2001. Forecasting bankruptcy more accurately: a simple hazard model. J. Bus. 74 (1), 101–124.

Soo, C.K., 2015. Quantifying Animal Spirits: News Media and Sentiment in the Housing Market. Ross School of Business Paper 1200. Available at SSRN https://ssrn.com/abstract=2330392 or http://dx.doi.org/10.2139/ssrn.2330392.

Stavins, J., 2013. Security of Retail Payments: The New Strategic Objective. Federal Reserve Bank of Boston Discussion Paper 13-9.

Tripwire, 2012. South Carolina Department Of Revenue Data Breach: What Went Wrong?. Tripwire Available at (last accessed 09/21/2017): www.tripwire.com/state-of-security/security-data-protection/south-carolina-department-of-revenue-data-breach-what-went-wrong/.