WORKING PAPER NO. 15-42
OUT OF SIGHT, OUT OF MIND:
CONSUMER REACTION TO NEWS
ON DATA BREACHES AND IDENTITY THEFT

Vyacheslav Mikhed
Federal Reserve Bank of Philadelphia

Michael Vogan
Federal Reserve Bank of Philadelphia

November 2015

RESEARCH DEPARTMENT, FEDERAL RESERVE BANK OF PHILADELPHIA
Ten Independence Mall, Philadelphia, PA 19106-1574 • www.philadelphiafed.org/research-and-data/

Out of Sight, Out of Mind:

Consumer Reaction to News on Data Breaches and Identity Theft*

Vyacheslav Mikhed

Michael Vogan

Payment Cards Center, Federal Reserve Bank of Philadelphia

November 2015

ABSTRACT

We use the 2012 South Carolina Department of Revenue data breach to study how data breaches and news coverage about them affect consumers' take-up of fraud protections. In this instance, we find that a remarkably large share of consumers who were directly affected by the breach acquired fraud protection services immediately after the breach. In contrast, the response of consumers who were not directly exposed to the breach, but who were exposed to news about it, was negligible. Even among consumers directly exposed to the data breach, the incremental effect of additional news about the breach was small. 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 direct exposure, consumers did not appear to revise their beliefs about future expected losses associated with data breaches.

Keywords: identity theft, fraud alert, data breach, consumer protection, credit report

JEL Codes: D14, D18, G02

---

* Michael Vogan was with the Payment Cards Center of the Federal Reserve Bank of Philadelphia during the time he worked on this paper. We wish to thank Dennis Carlson, Amy Crews Cutts, Bradley Dear, April Ferguson, and Henry Korytkowski of Equifax for their assistance with the data on fraud protections. We are grateful to Cris McCollum for her help with the LexisNexis data. We thank Robert M. Hunt, Julia Cheney, and seminar participants at the Federal Reserve Bank of Philadelphia and the 2015 Federal Reserve System Payments Analysts Meeting in San Francisco for their helpful suggestions.

1. Introduction

In 2013–2014, a number of high-profile data breaches hit U.S. companies, including big-box retailers Target and Home Depot and a major U.S. bank, JPMorgan Chase. In these three incidents, 312 million consumer records were compromised. The stolen information included names, addresses, and e-mail addresses at JPMorgan Chase and individual credit and debit card numbers at Target and Home Depot.[1] As one expert said, "It'd be hard to find anybody in the US who hasn't had a credit card affected."[2] Despite the millions of consumers affected by data breaches, little is known about how these actors react to such events. We attempt to answer this question by analyzing how consumers reacted to a particular 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 others who were not directly affected but who were exposed to essentially the same news about the breach. For the latter group, there might have been an indirect effect of the breach: Those consumers might have updated their beliefs about expected losses from future data breaches.

To be more explicit, this incident compromised the records of most South Carolina residents (at least 81 percent), 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 neighboring Georgia and North Carolina (consumers in shared media markets) through the news.[3] We use a difference-in-differences methodology to estimate the effect of the breach itself and information about the breach on consumer responses.

Previous research on the effect of identity theft on consumers mostly focuses on the adoption and use of various payment options, such as debit or credit cards and online bill pay (Kahn and Liñares-Zegarra, 2013). Stavins (2013) argues that the adoption of less-established payment methods may be affected by their perceived security, and security may influence the use

[1] www.cnet.com/news/in-shift-hackers-want-your-identity-not-just-your-credit-card/

[2] www.cnet.com/news/security-in-2015-will-you-care-about-the-next-big-breach/

[3] 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.

of more established payments. Cheney et al. (2012) suggest that data breaches may pose risks for the U.S. payment card systems. In addition, Kosse (2013) argues that news on debit card fraud decreases consumer usage of debit cards for only about one day.

Our paper is related to these previous studies, but we look beyond the consumer's payment choice and into other ways the consumer may react to data breaches and identity theft, such as protecting her credit file by purchasing insurance and credit monitoring services. This study shares similarities with previous research on consumer reaction to crime and natural disasters. For example, Gallagher (2014) shows there is a transitory spike in flood insurance coverage among residents of recently flooded communities. In addition, flood insurance coverage among residents in nonflooded communities in the same television media market increases at one-third the rate of coverage in flooded communities. This appears to be an irrational response because the occurrence of a recent flood is not usually an informative indicator of the likelihood of future flooding. On the other hand, Gallagher argues that such behavior would be consistent with Bayesian learning in which events that are more recent are weighted more heavily than events in the distant past. It would also be consistent with availability bias (Kahneman, 2011).[4]

We hypothesize that the South Carolina data breach can affect consumers' perception about the safety of their personal information via three separate channels. First, this event can have a direct effect on victims. The data breach notification letter sent by the South Carolina government emphasized that breach victims were at risk of further identity theft and damage from criminal use of the stolen data.[5] Second, consumers who became aware of the South Carolina data breach via news coverage in shared media markets may update their beliefs about their exposure to losses from future, unrelated data breaches. This reaction would be consistent with Bayesian learning (Gallagher, 2014) or availability bias (Kahneman, 2011). Third, local news coverage of the South Carolina data breach and generic identity theft may trigger additional consumer responses if it generates a panic. Kahneman (2011) suggests that extensive media coverage may generate an "availability cascade," in which an event may trigger a self-

[4] Availability bias is a mental heuristic that assigns more weight to recent, easily recalled memories when making decisions (Kahneman, 2011).

[5] Data breaches with more informal notifications or notifications coming from less trustworthy sources may be less effective in warning consumers about the danger of additional criminal activity.

reinforcing media cycle. In our example, an availability cascade would ensue if local news about a data breach propagates widespread public fear about identity theft. We refer to these latter two channels as indirect effects. We compare the reactions of consumers in several "treatment" and "control" groups to measure the relative importance of these three channels.

Only South Carolina residents were directly affected by the breach, and their exposure was clearly communicated to them by the South Carolina government. The response of residents in Georgia and North Carolina must come through the second and third channels described previously. In contrast, South Carolina residents may be reacting to all three channels. This permits us to distinguish between the direct and indirect effects defined previously. In other words, by comparing the reaction of South Carolina residents to this specific breach with the reaction of Georgia and North Carolina residents, we can separate the effect of consumers taking precautions in response to their actual exposure to this event from the response of consumers updating their beliefs about future risks. In addition, we can measure the exposure to news about the South Carolina data breach among residents of South Carolina and the other two states. By doing so, we can determine if greater exposure to news increases the response among data breach victims and their geographic neighbors.

To gauge the effect of the breach on consumers' 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. We find that victims of the 2012 South Carolina Department of Revenue Breach acquired much more fraud protection services immediately after the breach relative to consumers in other states. Consumers affected by the breach were six 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 55 times higher than that of the control groups. Data breach victims were 29 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 that suggests there was a significant change in their expectations in light of this specific data breach.

We use the local television markets as defined by Nielsen's Designated Market Areas (DMAs) to examine the reaction to the breach of North Carolina and Georgia residents who received television news coverage about the breach identical to that received by residents of South Carolina but who were not members of the breached set of consumers. Consumers in neighboring states might have used information about the breach in South Carolina to update their beliefs about the likelihood of future, unrelated data breaches. We find little evidence that consumers in those states revised their beliefs; there was practically no increase in enrollment in various forms of protection.[6]

Finally, we measure the effects of the amount of news coverage about the data breach on consumers' take-up of fraud protection services.[7] We construct a local news index on data security, fraud, and identity theft using the LexisNexis news database. We find that the breach generated a large increase in the amount of news about fraud and identity theft, disproportionately so for newspapers headquartered in South Carolina. Local newspaper coverage of this topic seemed to increase slightly the take-up of fraud protection in South Carolina as well as in North Carolina and Georgia. However, the effect of increased news coverage is much smaller than the effect of being a South Carolina resident at the time of the breach. In addition, it does not appear that newspaper reporting significantly amplified the effect of the breach on the take-up of fraud protection within South Carolina at the time of the breach.

From our results, we conclude that news coverage informed the decision to insure against future breach events for some consumers. The majority of consumers, however, only seriously considered fraud protection services after they formed a strong belief that their personal information was compromised. That belief was almost certainly created by the written and other communications of the South Carolina government.[8]

---

[6] It is possible that the certainty of which consumers were directly affected by the breach contributed to this result. In other breaches in which the extent of the exposed population is less clear, the reaction to news about the breach might be different.

[7] This is our attempt to identify and measure a potential availability cascade.

[8] We cannot rule out the possibility that, in the absence of the government's highly salient communications, media coverage might have had a stronger effect.

2. South Carolina Department of Revenue Data Breach

On October 26, 2012, the South Carolina Department of Revenue (henceforth referred to as the SCDOR) announced it had experienced a data breach that exposed 3.6 million Social Security numbers (SSNs) and 387,000 credit and debit card numbers of South Carolina taxpayers.[9] The information on 3.3 million bank accounts was also stolen.[10] 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 percent of South Carolina residents.[11]

Immediately after the data breach, the SCDOR launched an engagement effort to offer 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.[12] The ProtectMyID Alert product is designed to "detect, protect, and resolve potential identity theft, and includes daily monitoring of all three credit bureaus." By registering for 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.[13] 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.[14] The SCDOR informed consumers about other ways to protect their identities as well. These

[9] www.governor.sc.gov/Documents/Media_Release_10262012.pdf

[10] www.tripwire.com/state-of-security/security-data-protection/south-carolina-department-of-revenue-data-breach-what-went-wrong/

[11] 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.

[12] www.governor.sc.gov/Documents/Media_Release_10262012.pdf.

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

[14] www.reuters.com/article/2012/11/07/usa-southcarolina-taxes-idUSL1E8M7NVO20121107

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.[15]

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.[16] 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. The deadline for enrollment into the CSID credit monitoring program was initially set for October 1, 2014, but was changed to October 1, 2015.

3. Data

3.1 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 percent 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 the SSN.[17] 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

[15] www.governor.sc.gov/Documents/Media_Release_10262012.pdf

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

[17] Our data do not include SSNs. Equifax uses SSNs to assemble the data set, but the SSNs 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.

due to death, inactivity, or emigration.[18] Crucial to our study is that the CCP contains geographic information for the address of residence down to the census block and zip code levels in addition to credit-related variables.

We supplement the CCP with fraud alert data obtained from Equifax by the Payment Cards Center at the Federal Reserve Bank of Philadelphia. These data provide the activation status and origination date of five different types of fraud protection services for consumers in the primary 5 percent CCP sample.[19] 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 quarterly number of consumers in South Carolina, Georgia, and North Carolina represented in our data along with the number who filed any type of fraud protection. This data set covers Q1:2010 through Q3:2013.

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."[20] These alerts last 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 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

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

[19] The date of origination is only provided for initial alerts, extended alerts, and credit freezes. We estimate the date 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.

[20] Fair and Accurate Credit Transactions Act of 2003, §112.

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 the freeze.[21]

Credit watches, such as Experian's ProtectMyID Alert, 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.[22] 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 offered by Equifax offer the option to request that Equifax files initial alerts every 90 days on the consumer's behalf.[23] As mentioned in Section 2, the SCDOR made ProtectMyID Alert 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 activate opt-outs for such offers. After a period of five years, the consumer may choose to renew the opt-out 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.[24] Initial alerts and extended alerts are the cheapest 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 have fees, but victims of a data breach may obtain these services at no cost, at least for a period of time. All else equal, credit watches are not as restrictive as credit freezes, which completely prevent credit inquiries. In the subsequent analysis, we will use such stratification in the direct and indirect costs of the five fraud protection services as a proxy for the "seriousness" of consumer expected loss from the SCDOR data breach.

[21] www.experian.com/consumer/help/states/nc.html

[22] This monthly fee ranges from $12.95 to $29.95 for credit watch products offered by Equifax.

[23] www.equifax.com/credit-watch-gold/

[24] 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.

3.2 News Index

We created an index that measures the intensity of news coverage about data breach and fraud events using the Nexis news database provided by LexisNexis. The Nexis news database is a collection of newspaper articles, trade press, magazines, newswires, and television transcripts from 26,000 sources around the world.[25]

To create the news index, we constructed a Boolean search focused on finding news articles about identity theft and data breaches between 01/01/2010 and 09/30/2013 from local newspapers in South Carolina, North Carolina, and Georgia. Our search criteria identified articles with variations of the terms "identity theft" and "data breaches" as well as articles more broadly about financial or data crimes. Additional search terms included variations of the following terms: *data security*, *system security*, *network security*, *hack*, *data compromise*, *tokenization*, *data intrusion*, *system intrusion*, *network intrusion*, and *stolen data*. These search terms were further filtered to apply only to articles tagged with *cybercrime*, *fraud and financial crime*, and *identity theft* index terms in the Nexis system. More general articles about information crime were included with the expectation that the content of such articles raises similar concern about the safety of consumers' financial information as does the content in articles about identity theft and data breaches. We restrict the search to local newspapers only because information from national newspapers is distributed across all regions, and geographic variation in news coverage is needed to measure the effect of news exposure on the propagation of fraud alert filings.

The search is designed explicitly to manage the tradeoff between identifying the most articles possible while filtering out articles that are irrelevant to the subject matter of interest. Although it is possible that a few extraneous articles slipped through our criteria, a visual examination of the search results shows that the search is as accurate and comprehensive as we intended.[26]

Our search returned 7,166 unique articles about identity theft and data breaches from 155 local sources in 124 cities, towns, and other locations across the three states during 01/01/2010 to 09/30/2013. Table A1 in the Appendix lists the names of the searched newspapers and their

[25] www.lexisnexis.com/en-us/products/nexis/feature-get-the-story.page

[26] An example of a typical article returned can be found at www.thestate.com/news/business/article13825211.html.

associated cities and towns of coverage. We identify the city or town associated with a particular newspaper by the newspaper description presented by LexisNexis. In the cases in which the city or town is not present in the newspaper description, we use the city or town where the newspaper is headquartered.

Figure 1 shows the number of articles about identity theft and data breaches that our news index captures aggregated to the state level in each quarter.[27] During the quarter of the breach, news outlets in South Carolina dramatically increased their coverage on the subject of identity theft by approximately 750 percent compared with the coverage leading up to the incident. A smaller increase can be observed in North Carolina and Georgia during the same quarter. Figure 1 also shows that local press in all three states covered the topic of fraud at approximately the same level in the years leading up to the breach.

3.3 Geographic and Temporal 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. Figure 2 reports the quarterly number of fraud protections acquired in Georgia, North Carolina, and South Carolina during the Q1:2010 to Q3:2013 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 approximately 1,500 percent between Q3:2012 and Q4:2012 to include about 40,000 consumers. The explosion of credit watches filed is a direct result of enrollment into the free Experian ProtectMyID Alert offered immediately after the breach.

Similarly, the number of credit freezes filed in South Carolina at the time of the breach increased by about 1,700 percent, the number of initial alerts increased about 540 percent, and the number of opt-outs increased about 233 percent. 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

[27] We use the original city-level news index in our regression analysis.

Q2:2013. This is likely to have occurred because the SCDOR pushed back the deadline to enroll in free credit watches to 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, both states had more protections filed per quarter compared with South Carolina (which can be explained by the larger populations in North Carolina and Georgia). Before the breach, all three states had similar trends in fraud protection filings. There was a small increase present in the number of initial alerts filed in both Georgia and North Carolina coinciding with the timing of the SCDOR data breach that could have been a response to news coverage of the event. However, this increase seems to be in line with long-term trends in these states. There was also a curious increase in the number of credit offer opt-outs filed in all three states in the quarter preceding the data breach.

Omitted from Figure 2 is the trend of extended alerts over time. This trend is presented in Panel A of Figure 3. Extended alerts require sufficient evidence of fraud that would enable a consumer to submit a police report. Thus, this protection service is associated with instances of severe identity theft in which financial damage is visible on the credit bureau record leading up to the time that the alert is filed (Cheney et al., 2014). In the case study examined here, there is no change in the time trend of extended alerts for any state at the time of the SCDOR data breach.

In Panels B–D of Figure 3, the average time trends for three variables known to be associated with fraudulent credit activity are presented for our states of interest. Average risk scores, average number of credit inquiries, and the percentage of address changes do not significantly change in South Carolina after the data breach.[28] The nonresponse of extended alerts, risk score, credit inquiries, and address changes suggests that data stolen in the SCDOR data breach were not used to perpetrate much serious fraud in the quarters immediately following the breach.

Nevertheless, we find much evidence of consumer reaction to the SCDOR data breach in the temporal-geospatial dimension. Figures 4–7 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

[28] *Risk score* is a proprietary credit score derived by Equifax that is a measure of consumer credit risk based on information contained in Equifax's credit bureau files. It is similar to other credit scores available in the marketplace.

Carolina, and South Carolina. Initial alert filings were well below 1 percent of the population in census tracts across all states before surging upward in South Carolina during Q4:2012, especially in the urban areas of Columbia and Charleston. The number of alert filings in urban areas, including credit freezes, opt-outs, and credit watches, is relatively higher than that of filings in less urban areas. While the adoption of fraud protection services surged in Q4:2012 in South Carolina, it was flat in neighboring North Carolina and Georgia. Moreover, the effect of the breach on initial alerts, freezes, credit watches, and opt-outs in South Carolina dissipated rapidly; it was completely gone for all services except for credit freezes by Q2:2013.

The relative increase in the percentage of the population who filed credit freezes, opt-outs, and credit watches was so large in some South Carolina census tracts that we winsorized the data at the 99th percentile.[29] With the exception of credit watches, there were small, nonsystematic patterns of alert filings in Georgia and North Carolina, but nothing compared with the filings in South Carolina following the SCDOR data breach. Multiple census tracts in South Carolina during Q4:2014 had 2 percent or greater of their population file credit freezes and 3 percent or greater of their population file 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 mail to a different address. Figure 7 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 percent of the population of most census tracts requested an opt-out per quarter.

Almost all census tracts in South Carolina had more than 10 percent of their population file credit watches, and a substantial proportion of census tracts had 20 percent or more of their populations do so. In addition, in the Q4:2012 to Q2:2013 period, more than 29 percent of the credit bureau population of South Carolina acquired a credit watch. The credit watch maps (Figure 6) 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.

These astounding rates of credit watch filings directly follow from the free availability of and encouragement to file credit watches provided by the SCDOR to individuals affected by the

[29] If we had not done so, the intensity of alerts filed in other locations and time would not be visible in the figures.

data breach. A similar argument could be made for initial alerts, credit freezes, and opt-outs as well, since the SCDOR actively reached out to consumers to inform them of the available options to protect their identities from potential harm. However, the explicit encouragement to use credit watches and other types of alerts after the data breach does not mitigate our ability to assess the impact of news on consumer behavior. Consumers still must choose to begin the fraud protection filing process after they receive information on the available options.

4. 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 risk factors. We focus on the adoption decision because maintenance of fraud protections is mostly mechanical and automatic.[30] Our main specification is as follows:

$$Y_{i,t} = \beta_0 + \beta_1 time_t + \beta_2 state_s + \beta_3 time_t * SC_s + \beta_4 age_{i,t} + \beta_5 risk_{i,t} + \varepsilon_{i,t}. \qquad (1)$$

We use a dynamic logit model to estimate equation (1) separately for each type of fraud protection. The dependent variable $Y_{i,t}$ indicates whether an individual acquired one of the five 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, it is not possible 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-

[30] For instance, credit freezes and opt-outs remain active until the consumer takes some action to cancel them. Credit watches, however, which were provided for 12 months and then for another year 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.

order polynomial in age. As 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). Moreover, we control for a set of risk factors recorded in credit bureau files. These factors include risk score, an indicator for the presence of a mortgage, number of credit inquiries within three months and 12 months, age of the newest account, difference in the number of accounts, overall credit card utilization rate (total revolving balance divided by total credit limit), number of 120 days past due occurrences, and change of address. We specify risk score and card utilization rate nonparametrically by including two sets of dummy variables for them. Risk score is divided into nine bins spaced apart by 20 to 60 points, with the risk score below 580 serving as an omitted category. We include four dummy variables for credit card utilization: (0.25, 0.5], (0.5, 0.75], (0.75, 1], and over 1. The dummy variable for utilization of 0.25 or less is omitted. Table 2 summarizes these control variables.

Because some credit file characteristics, such as credit inquiries and age of the newest account, may be affected by contemporaneous identity theft and fraud (e.g., criminals opening new fraudulent accounts in a victim's name), we use lags of certain control variables. We select four quarter lags to ensure our control variables are not affected by fraudulent activity.[31] Lagged control variables include credit card utilization, number of inquiries, an indicator for the presence of a mortgage, mobility, age of newest account, and number of 120 days past due occurrences. Finally, we cluster standard errors at the individual level.

The major variables of interest to us in equation (1) are interactions of quarter fixed effects and an indicator variable for residents of South Carolina (SC_s). These variables show by how much residents of South Carolina are more likely to acquire 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 difference-in-differences identification strategy used later is that, in the absence of the breach, trends in the adoption of fraud protection devices would be the same in our control group (residents of North Carolina and Georgia) and treatment group (residents of South Carolina). We check the validity

[31] See Cheney et al. (2014) for an additional discussion of lagged control variables.

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.

Figure 8 plots the estimated coefficients on the interactions of quarter dummies with the South Carolina indicator from equation (1). Panels A–D of this figure present the coefficients for the probability of acquiring one of the four fraud protection devices: initial fraud alert, credit freeze, credit watch, and opt-out, respectively. In addition to coefficients, we show the 95 percent 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 the panels of Figure 8 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 device with an elevated level of adoption two quarters after the breach is credit watch. These results are consistent with those seen in earlier figures (Figures 2, 4–7), showing a strong, even if short-lived, response of consumers to the SCDOR data breach. Figure 8, 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 credit file characteristics of consumers. 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 should be an appropriate control group for South Carolina residents affected by the breach in Q4:2012.

Figure 8 also reveals that consumers used available protections to a varying degree. The odds of a credit watch adoption (Panel C) increased 55 times at the time of the data breach, whereas initial alerts and opt-outs were six and three times more likely to be acquired, respectively. Credit freezes were in between these two extremes, with an odds ratio of 29. 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 complimentary ProtectMyID credit watch to all victims). The other protection devices, however, were only mentioned in some communications (information pamphlets) and not promoted

widely. Hence, the relatively strong consumer response in terms of credit freezes is somewhat surprising.

5. Television Media Markets and Fraud Protection Adoption

5.1. The Dissemination of News Through Media Markets

In this section, we attempt to disentangle the different channels through which consumers receive information about data breaches and identity theft and how consumers perceive and react to this information. Several recent studies emphasized the importance of news media coverage on the formation of public opinion, sentiments, and beliefs about risks. Soo (2013) argues that news sentiment about the housing market affects house prices, trading volume, and expectations. Azzimonti (2014) finds 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 card holders from using this payment option. Finally, Kahneman (2011) explains how media coverage may create very powerful images of trivial events, reinforce these images, and generate a very high level of public concern (an availability cascade).

To test this channel of influence, we use data on Nielsen's DMAs. The Nielsen Company (hereafter, Nielsen) conducts research on the shares of viewers of particular television stations in U.S. counties. These counties are organized into DMAs or, simply, 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. Importantly for us, 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 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.[32] Figure 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 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 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.

5.2. The Effect of News on Breach Victims

Figure 10 plots coefficients from the interaction of quarter indicators with South Carolina shared (orange lines) and unshared (blue lines) media market indicators. The rest of the specification is the same as in equation (1). Similar to Figure 8, we provide point estimates and 95 percent confidence intervals as bands. As seen in Figure 10, individuals affected by the data breach acquire 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 smaller in the South Carolina shared media markets compared with the South Carolina inner media markets at time 0. The point estimate for credit

[32] 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.

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.

5.3. 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.

Figure 11 summarizes estimated coefficients from equations (1) with some additional interactions. In this specification, we interact quarter 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.[33] 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. 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 and to act on these beliefs by acquiring fraud protections.[34]

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

[34] It is possible that in other breaches, with less clarity about who was exposed or less clear and publicized notifications, news accounts may have different effects on consumers.

6. Consumer Reaction to Newspaper Articles on Data Breaches and Identity Theft

In this section, we examine whether newspaper articles about data breaches, identity theft, and fraud influenced consumers who were or were not directly affected by the South Carolina data breach. To explore this question, we use data on the number of newspaper articles from LexisNexis as described in Section 3.2. We modify our main specification in the following way:

$$Y_{i,t} = \beta_0 + \beta_1 articles_{c,t} + \beta_2 time_t + \beta_3 state_s + \beta_4 articles_{c,t} * time_t * SC_s + \beta_5 articles_{c,t} * time_t + \beta_6 articles_{c,t} * state_s + \beta_6 time_t * state_s + \beta_7 age_{i,t} + \beta_8 risk_{i,t} + \varepsilon_{i,t} \quad (2)$$

where *articles* is the count of newspaper articles at the city or town (index *c*) and quarterly level (index *t*), *time* and *state* are sets of quarterly and state fixed effects (indexes *t* and *s*, respectively), and (SC_s) is an indicator variable for living in South Carolina.[35] The variables of major interest to us are the interaction of the time of the breach dummies (Q4:2012–Q2:2013) with the article count and the living in South Carolina indicator. This specification also includes all the other interactions of these variables (South Carolina and other states, time, and article count).

Table 3 reports results from dynamic logit regressions for the take-up of the five fraud protection services. As can be seen in this table, newspaper articles on fraud and identity theft increase the odds of a consumer acquiring one of the protections. The coefficients in Table 3 imply that an extra article increases the odds of a consumer filing an initial alert by about 1.9 percent. The implied coefficients for the other protection devices are similar in magnitude. The effects of being in South Carolina at the time of the breach are much larger in magnitude and imply that data breach victims are about 170 percent more likely to file an initial alert immediately after the breach was announced and 320 percent more likely one quarter after that. These consumers are also more likely to file credit freezes (1,700 percent), credit watches (7,100

[35] The median number of articles per city in our sample is five. We included only the first-order term of the *article* variable in equation (2) because the higher-order terms of this variable were statistically insignificant and did not affect any other results.

percent), and opt-outs (370 percent, but one quarter after the incident). There is no statistically significant effect of the data breach on extended alerts. The interaction of the number of newspaper articles and the data breach is typically economically and statistically insignificant.

All these findings are consistent with our previous results showing that South Carolina consumers reacted strongly to the data breach. However, most of this effect cannot be explained by the number of newspaper articles, as additional news items on fraud and data breach have relatively little effect at the time of the breach. The absence of the extra effect of the news at the time of the breach in South Carolina suggests there was no availability cascade in this particular data breach episode. An availability cascade would imply that extra newspaper articles would generate an increased reaction among South Carolina residents at the time of the breach.

On the other hand, local newspaper articles seem to have a small, but statistically significant effect on fraud protection take-up independent of the data breach. This is consistent with prior work showing that consumers alter their behavior after receiving news on debit card fraud but only for brief periods of time (Kosse, 2013).

7. 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 fraud. We are able to identify likely victims of the breach and link them to a unique database of fraud protection services. 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, television coverage of the incident, and local newspaper articles about the issue. We use differences in the take-up of fraud protections among the populations affected through these channels to test several hypotheses about consumers' data security perceptions and interactions with the media.

We find that, within two quarters of the data breach event, consumers directly exposed responded by acquiring fraud protections available to them, excluding the extended fraud alert. This tendency is consistent with these individuals being unprotected against fraud and identity theft before the incident and protecting against further fallout from the breach. The very high 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.

We also find that individuals not directly affected by the breach, but who share the same television markets and thus are subject to the same amount of media coverage of the breach, did not respond to this breach by acquiring fraud protections. This suggests that consumers in shared television media markets did not substantially update their beliefs about future and unrelated data breaches as a result of the televised news.

We also construct an identity theft news index to examine how local media attention to the issue of data breaches and identity theft may affect individuals and whether it may increase the effect of cybersecurity accidents. Our results suggest that news on identity theft and personal information security prompted some consumers to increase their protections independent of the breach, though the independent effect of the news was small. This is consistent with consumers updating their beliefs about the likelihood of fraud and identity theft based on information contained in the news but also based on their beliefs as to whether they were exposed to a particular breach. On the other hand, we do not find any significant additional effects of media coverage on fraud protections at the time of the South Carolina breach. This finding may imply that media coverage did not amplify the effect of the breach in this particular episode.

References

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

Cheney, Julia S., Robert Hunt, Katy Jacob, Richard D. Porter, and Bruce J. Summers. 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, Julia S., Robert Hunt, Vyacheslav Mikhed, Dubravka Ritter, and Michael Vogan. 2014. "Identity Theft as a Teachable Moment," Federal Reserve Bank of Philadelphia, Working Paper 14-28.

Elul, Ronel, Nicholas Souleles, Souphala Chomsisengphet, Dennis Glennon, and Robert Hunt. 2010. "What 'Triggers' Mortgage Default?" *American Economic Review*, Vol. 100, No. 2, pp. 490–494.

Gallagher, Justin. 2014. "Learning About an Infrequent Event: Evidence from Flood Insurance Take-Up in the United States," *American Economic Journal: Applied Economics*, Vol. 6, No. 3, pp. 206–233.

Gross, David, and Nicholas Souleles. 2002. "An Empirical Analysis of Personal Bankruptcy and Delinquency," *Review of Financial Studies,* Vol. 15, No. 1, pp. 319–347.

Kahn, Charles, and José Liñares-Zegarra. 2013. "Identity Theft and Consumer Payment Choice: Does Security Really Matter?" mimeo, University of Illinois.

Kahneman, Daniel. 2011. *Thinking, Fast and Slow.* New York: Farrar, Straus and Giroux.

Kosse, Anneke. 2013. "Do Newspaper Articles on Card Fraud Affect Debit Card Usage?" *Journal of Banking & Finance*, Vol. 37, No. 12, pp. 5382–5391.

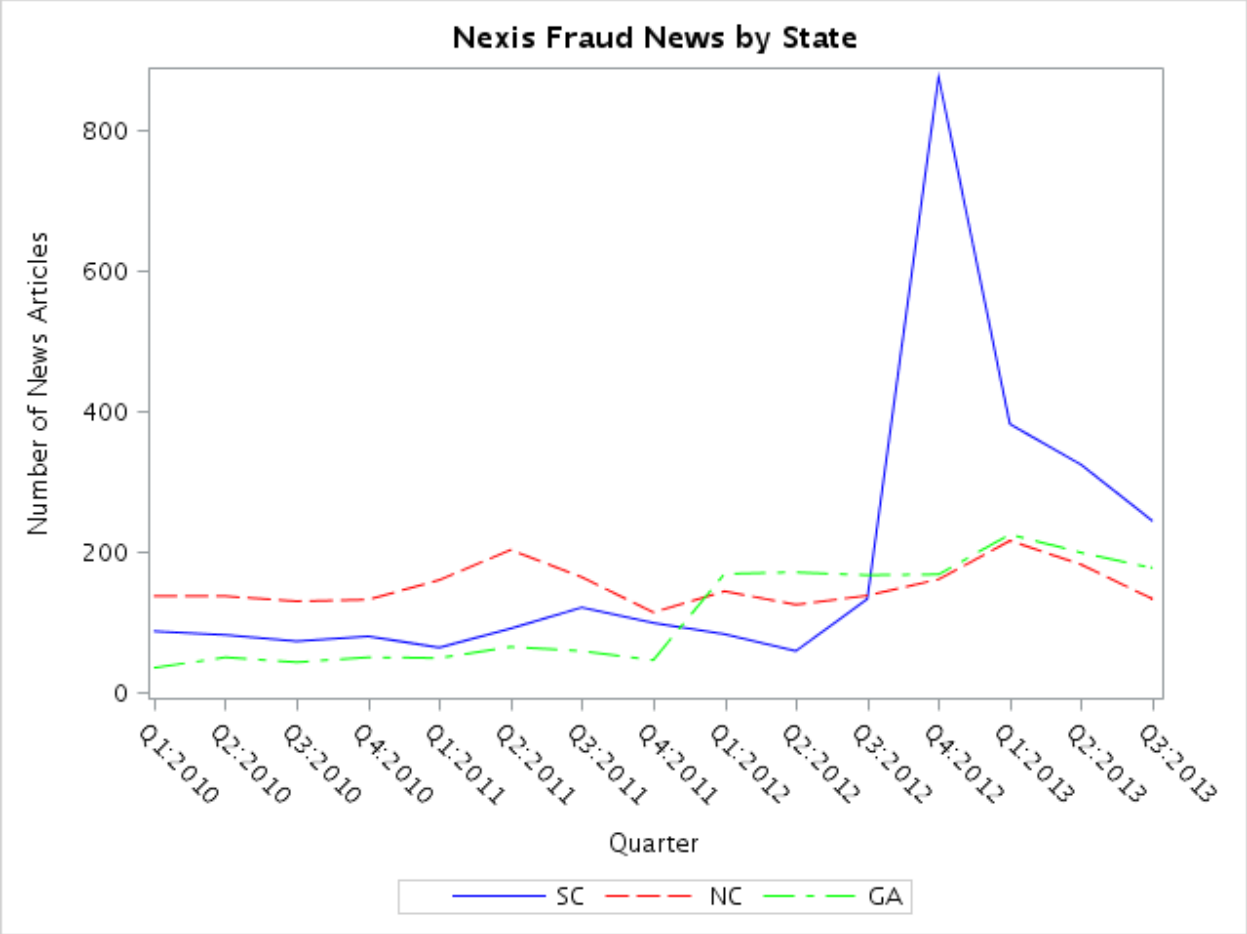
Lee, Donghoon, and Wilbert van der Klaauw. 2010. "An Introduction to the FRBNY Consumer Credit Panel," Federal Reserve Bank of New York, Staff Report 479.

Shumway, Tyler. 2001. "Forecasting Bankruptcy More Accurately: A Simple Hazard Model," *Journal of Business*, Vol. 74, No. 1, pp. 101–124.

Soo, Cindy K. 2013. "Quantifying Animal Spirits: News Media and Sentiment in the Housing Market," mimeo, University of Michigan, Stephen M. Ross School of Business.

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

Figure 1. Number of Newspaper Articles on Fraud in South Carolina, North Carolina, and Georgia

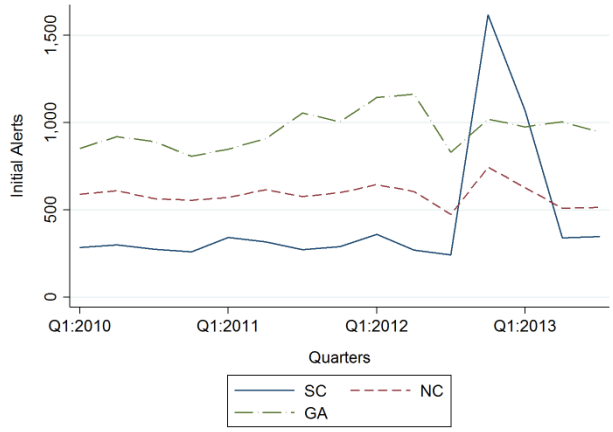


Note: This figure shows aggregated local data breach news coverage in the states of interest over time.

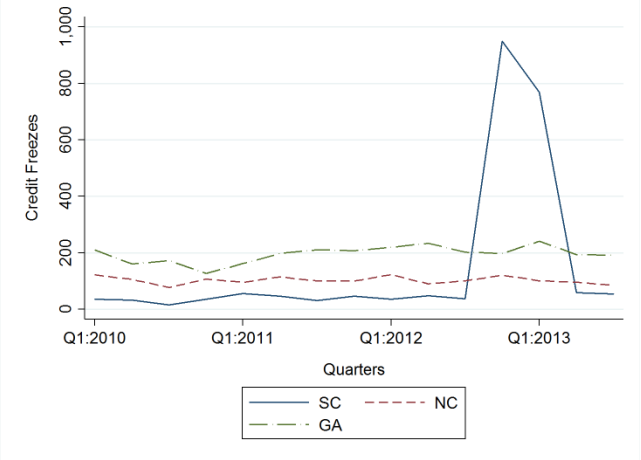
Source: Authors' calculations using a news index derived from the Nexis news database

Figure 2. Number of Fraud Protection Services Adopted Before and After the South Carolina Data Breach

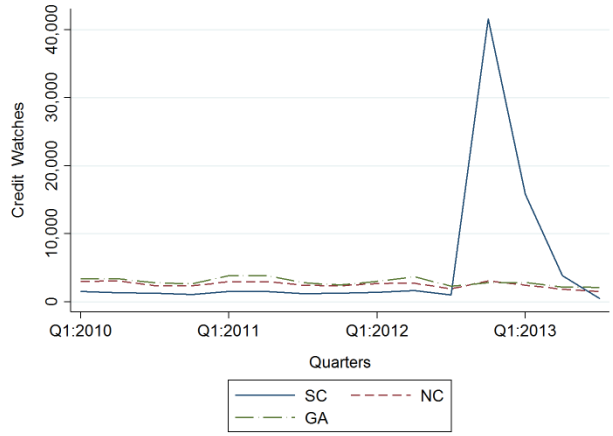
Panel A: Initial Alerts



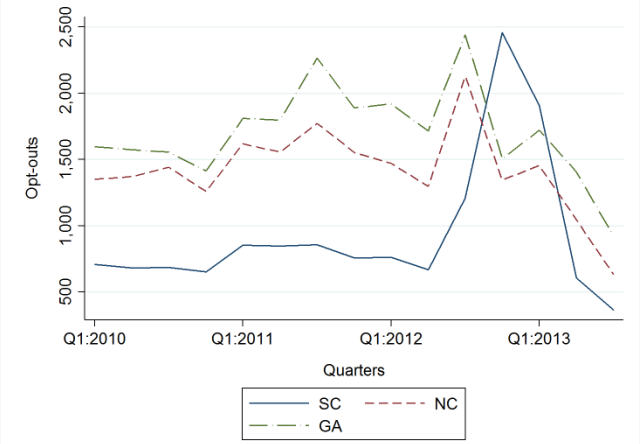
Panel B: Credit Freezes



Panel C: Credit Watches



Panel D: Opt-outs

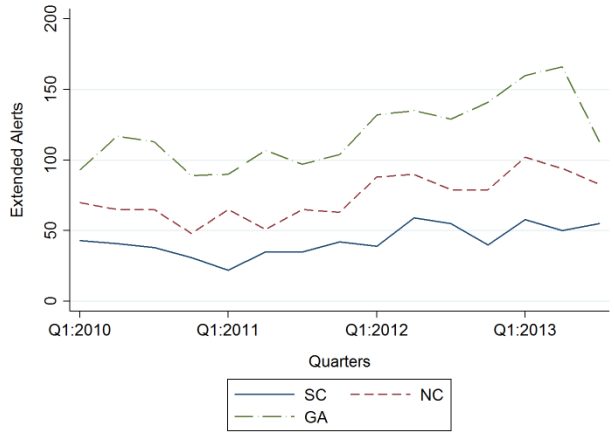


Notes: These figures show the number of fraud protection services acquired in each state over time. There is a significant response across all fraud protection services for consumers in South Carolina at the time of the breach.

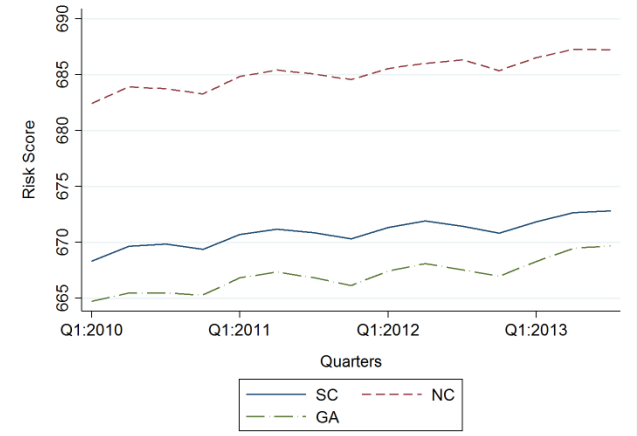
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia

Figure 3. No Evidence of Actual Fraud in Extended Alerts, Risk Score, Credit Inquiries, or Address Changes

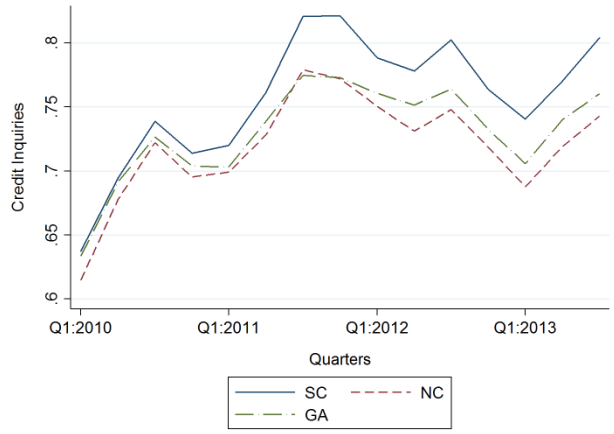
Panel A: Extended Alert Count



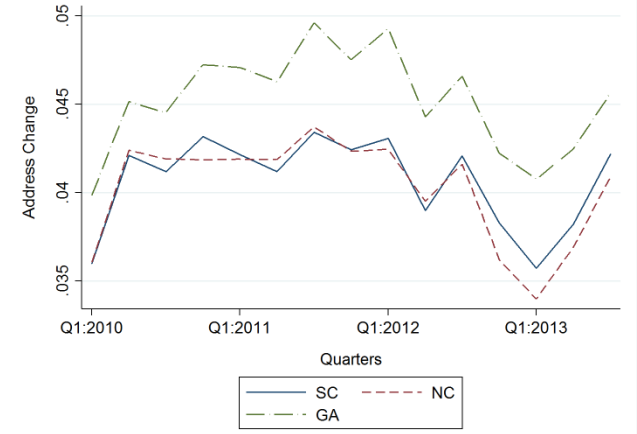
Panel B: Average Risk Score



Panel C: Average Credit Inquiries



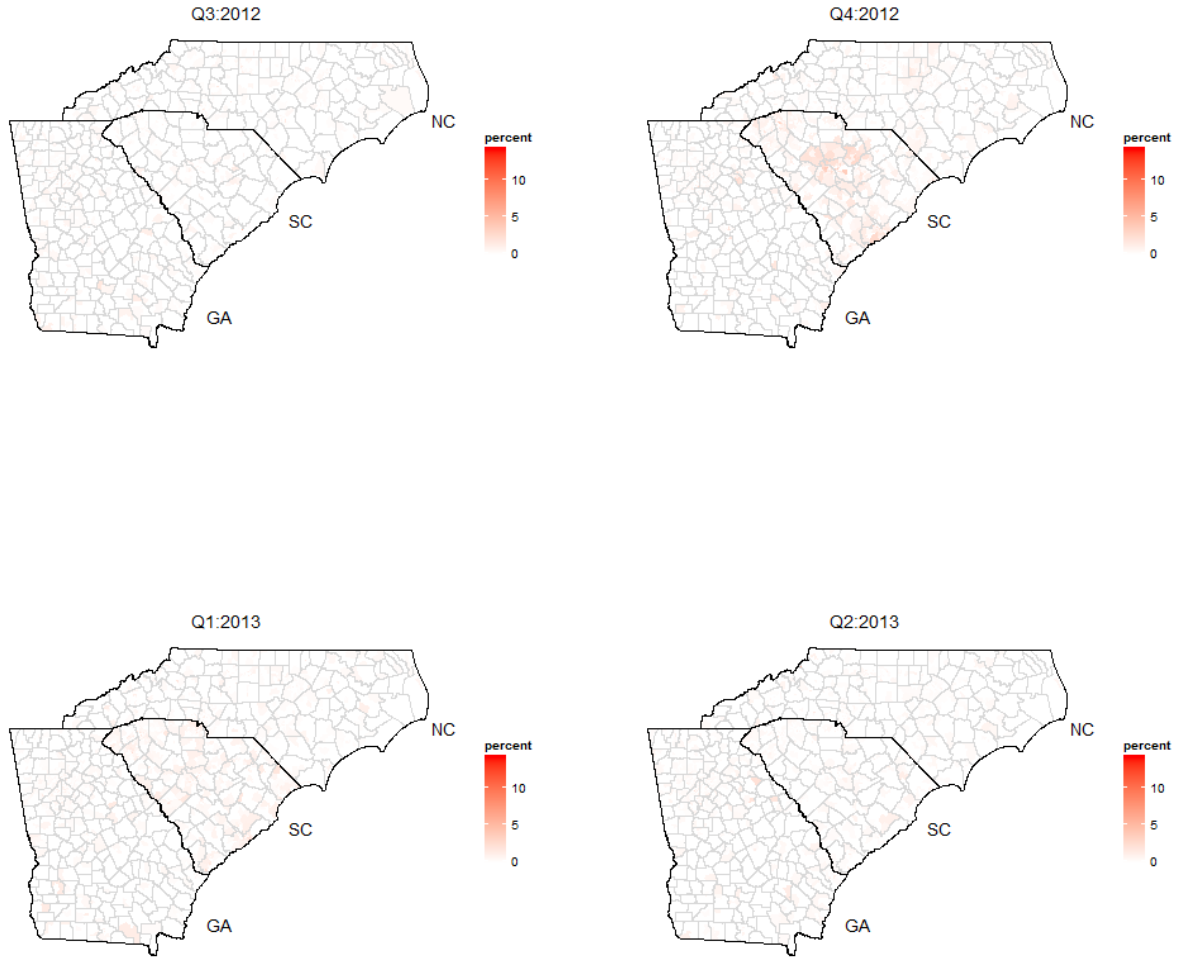
Panel D: Proportion of Address Changes



Notes: These figures show changes in variables that are indicative of perpetrated fraud in the states of interest over time. The lack of extended alerts filed in South Carolina coupled with the nonsystematic movement of fraud-related variables at the time of the breach strongly suggest that information stolen in the breach was not used immediately afterward to commit more serious fraud.

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

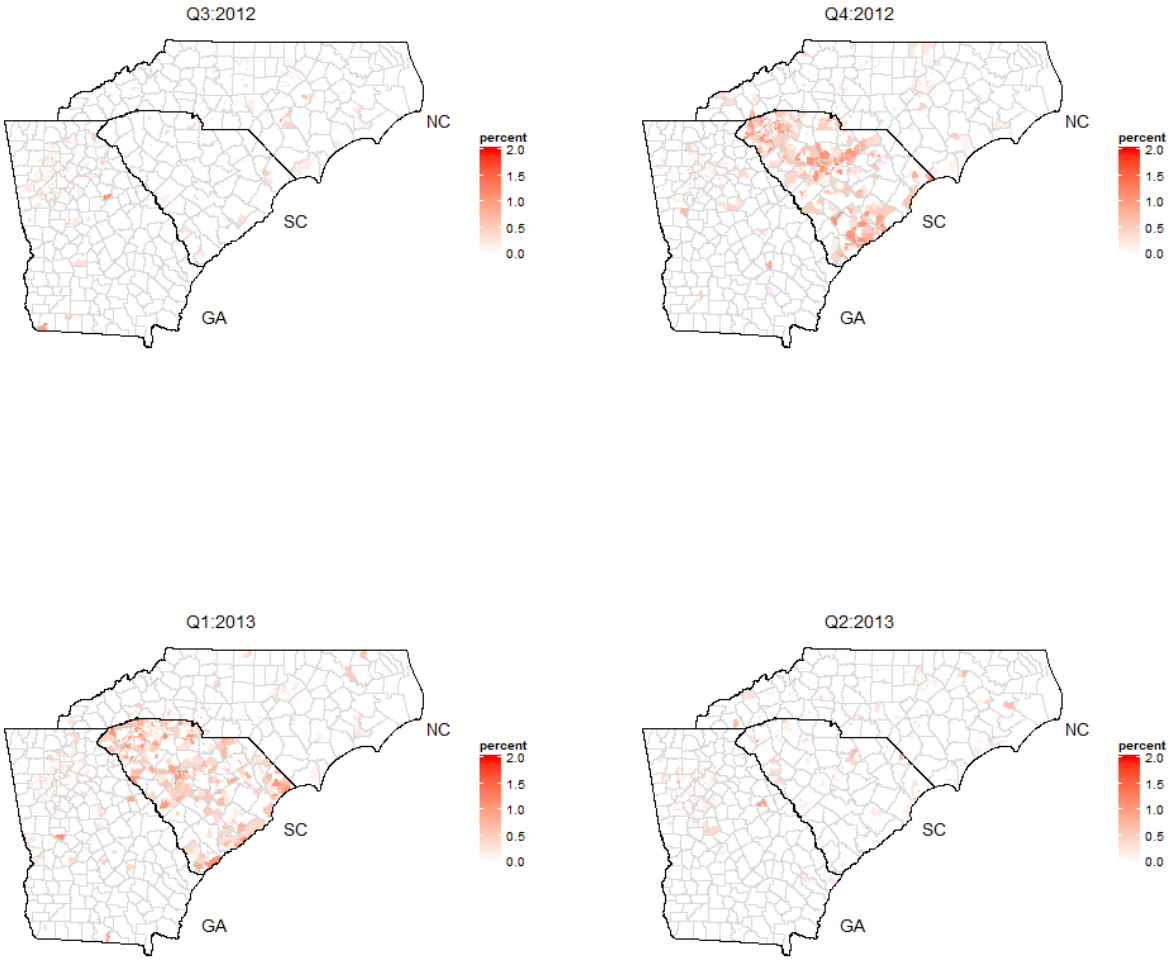
Figure 4. Initial Alerts as a Percentage of Census Tract Population



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. Up to 10 percent 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

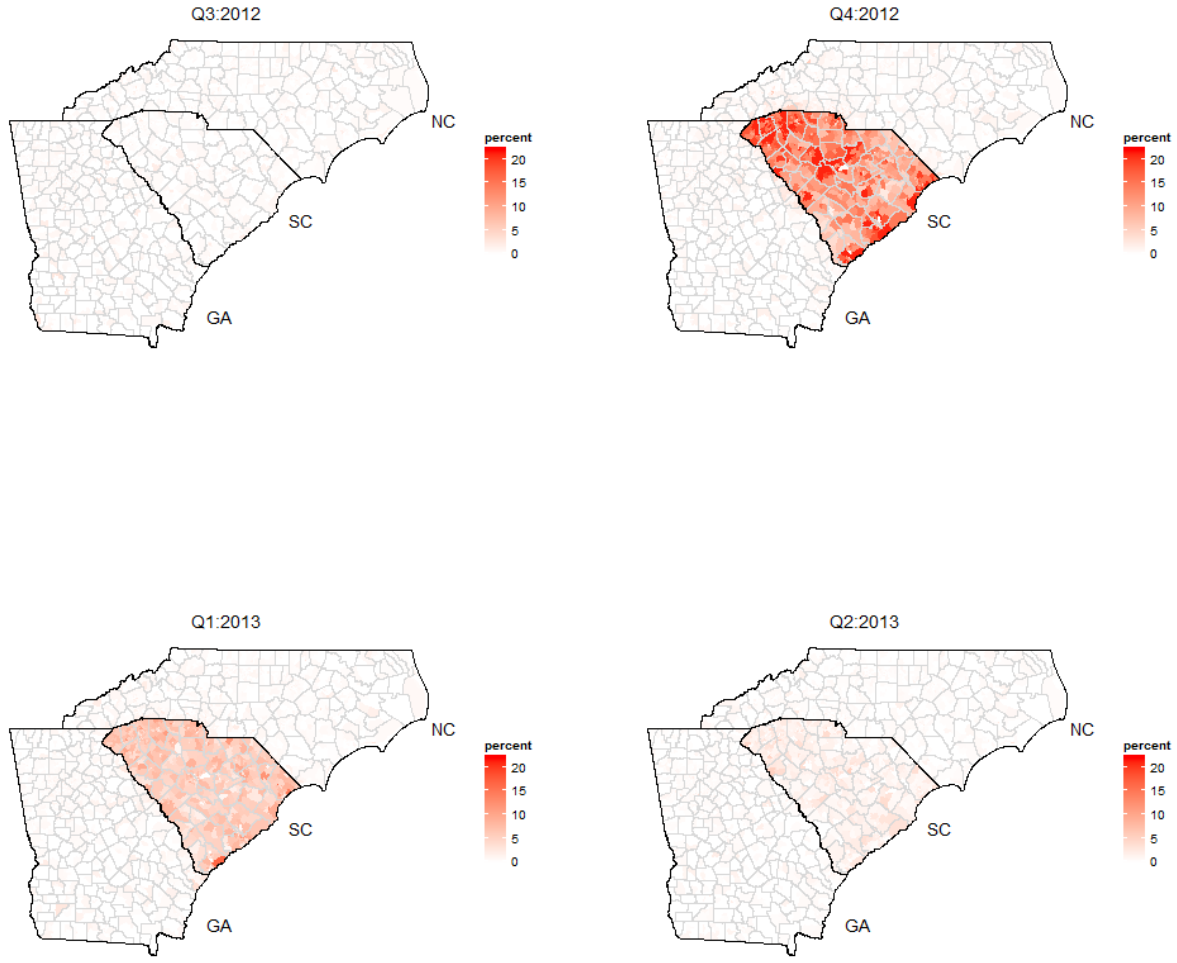
Figure 5. Credit Freezes as a Percentage of Census Tract Population



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 percent 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

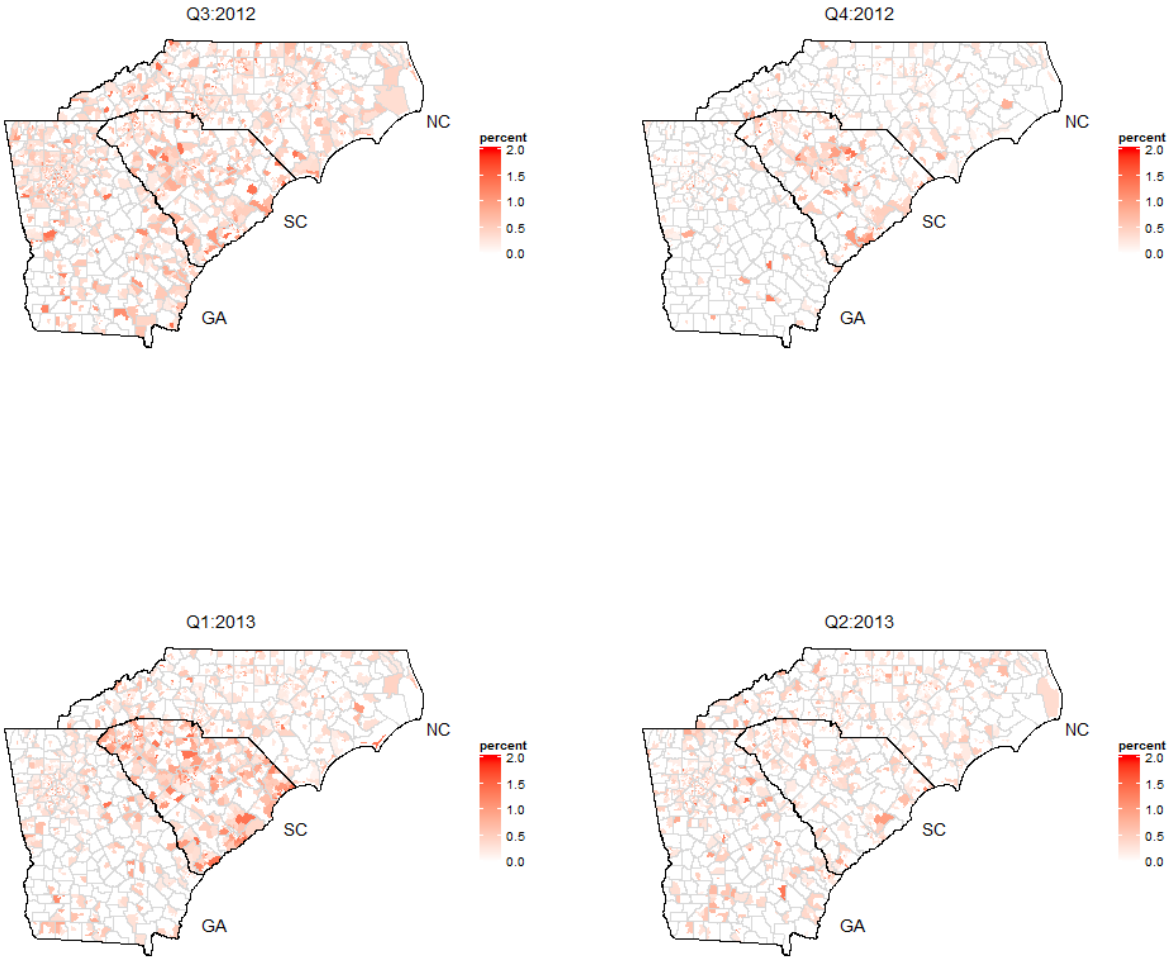
Figure 6. Credit Watches as a Percentage of Census Tract Population



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 percent 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 percent.

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

Figure 7: Opt-outs as a Percentage of Census Tract Population

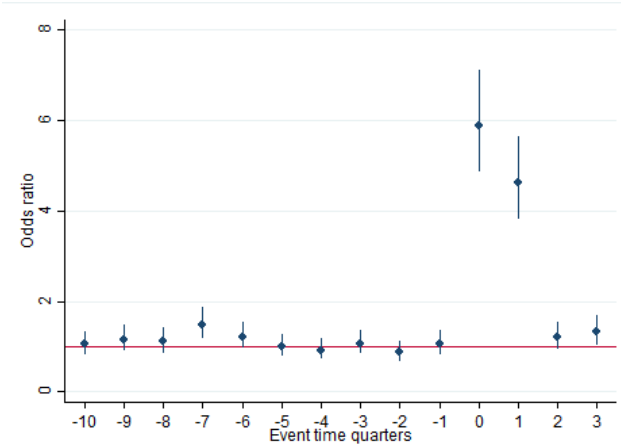


Notes: These maps show the percentage of the 2010 Census tract populations that filed an opt-out for the first time during the quarters immediately before, during, and after the breach. The percentages of opt-outs are winsorized at the 99th percentile to eliminate outliers. Up to 2 percent of some South Carolina census tract populations filed opt-outs at the time of the breach. Opt-outs were widespread among the three states before the breach occurred.

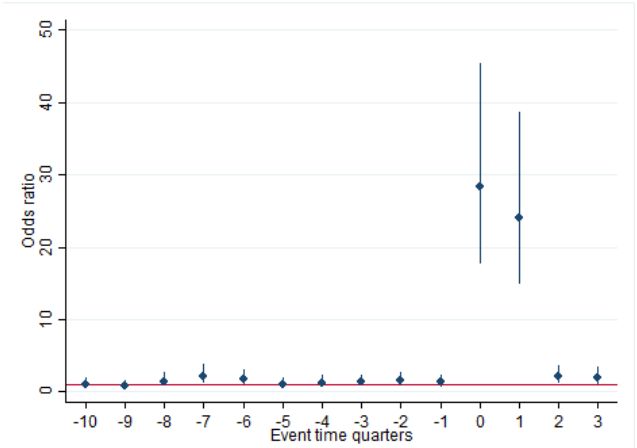
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia

Figure 8. Fraud Protection Take-up in South Carolina versus North Carolina and Georgia

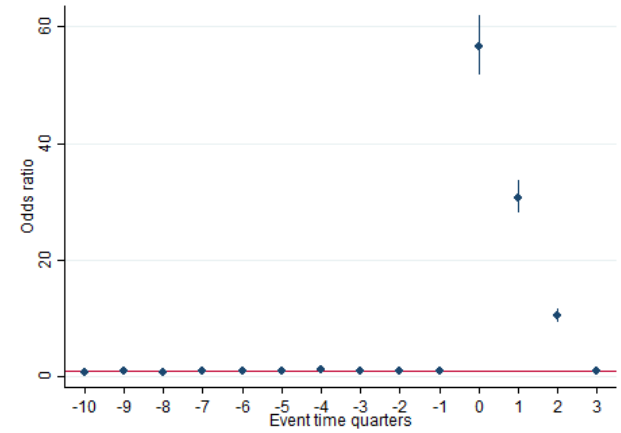
Panel A: Initial Alerts



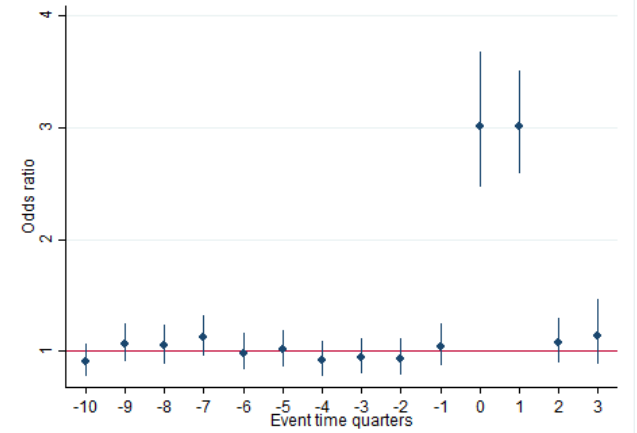
Panel B: Credit Freezes



Panel C: Credit Watches



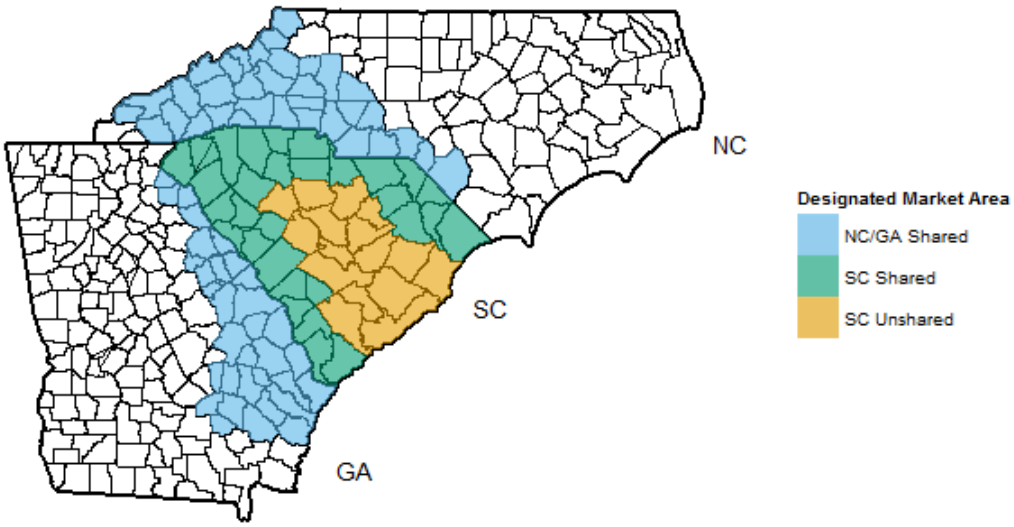
Panel D: Opt-outs



Notes: These figures show the odds ratios for the likelihood of filing a specific type of protection for 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 and Table 2. Dots represent estimated odds ratios bound by 95 percent confidence bands. 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 almost 60 times more likely to file 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

Figure 9. Designated Market Area (DMA) Regions

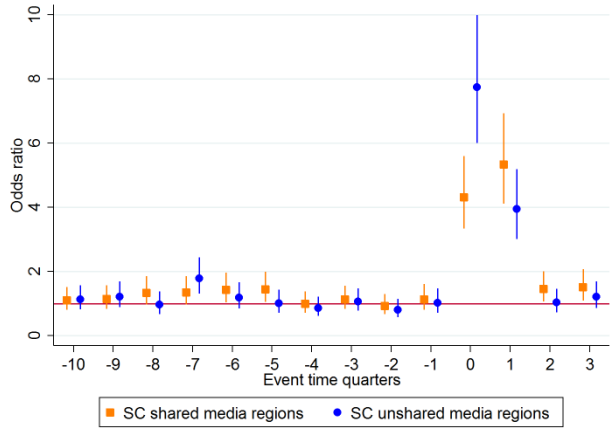


Notes: This map shows counties within seven DMAs created by Nielsen for South Carolina, North Carolina, and Georgia. We group these counties into three categories based on their location and whether their DMA reaches across state borders: 1) NC/GA Shared — counties inside of North Carolina and Georgia 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.

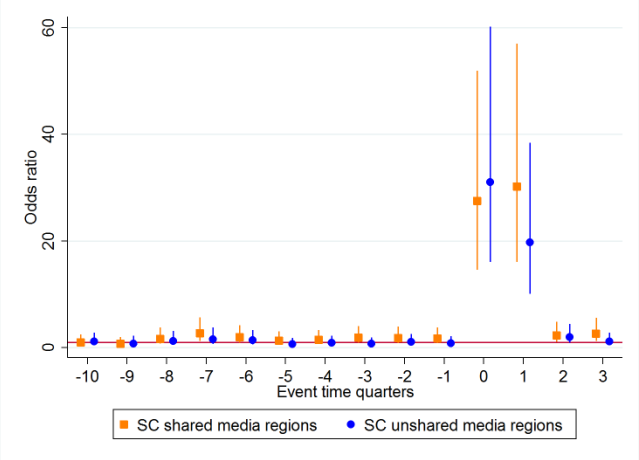
Source: Authors' calculations using data from Nielsen

Figure 10. Fraud Protection Take-up in South Carolina's Shared and Unshared Media Markets

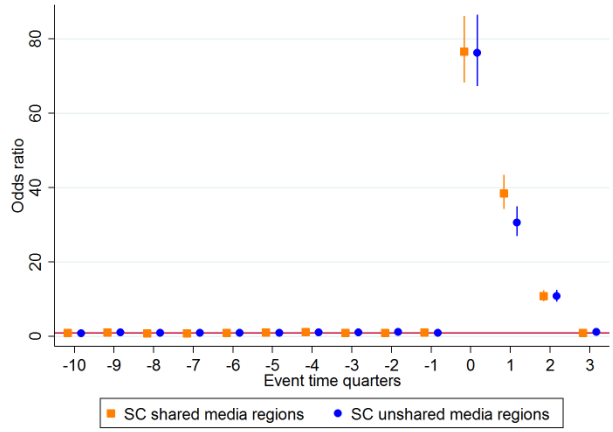
Panel A: Initial Alerts



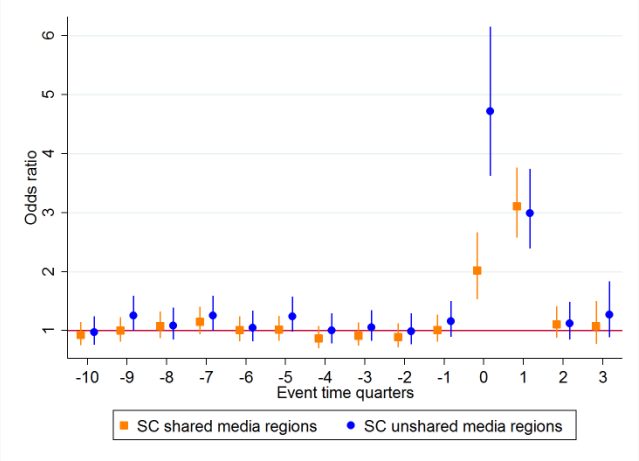
Panel B: Credit Freezes



Panel C: Credit Watches



Panel D: Opt-outs

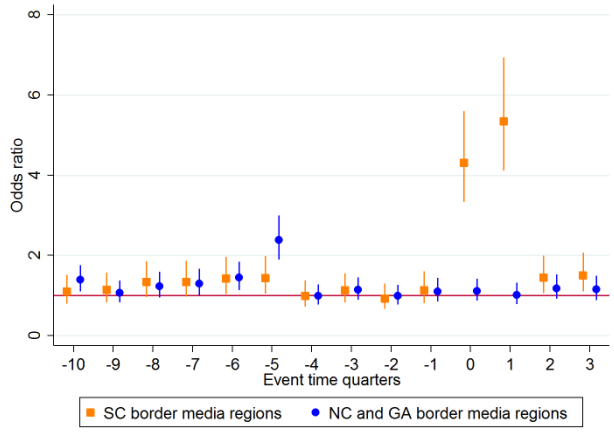


Notes: These figures show the odds ratios for the likelihood of filing a specific type of fraud protection for consumers in South Carolina counties that shared media markets with counties in other states and those that do not. These odds ratios come from dynamic logistic regressions with control variables as described in the text and Table 2. Dots represent estimated odds ratios bound by 95 percent confidence bands. Standard errors are clustered at the individual level. 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.

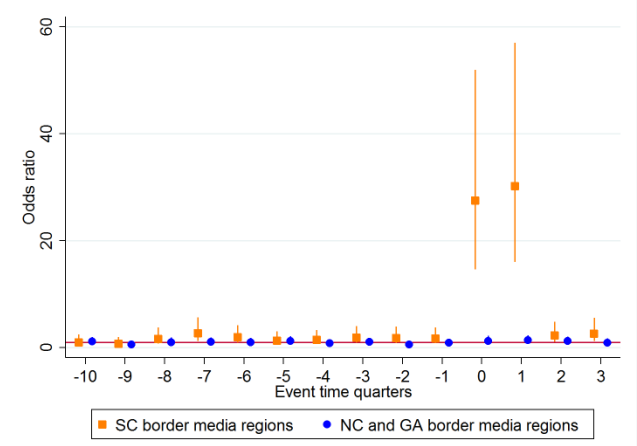
Source: Authors' calculations using data from the Federal Reserve Bank of New York Consumer Credit Panel/Equifax, augmented with variables obtained by the Payment Cards Center of the Federal Reserve Bank of Philadelphia

Figure 11. Fraud Protection Usage in South Carolina's Border Media Markets versus North Carolina and Georgia's Border Media Markets

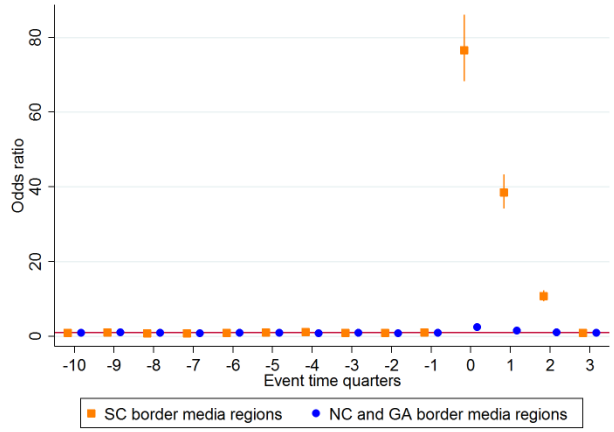
Panel A: Initial Alerts



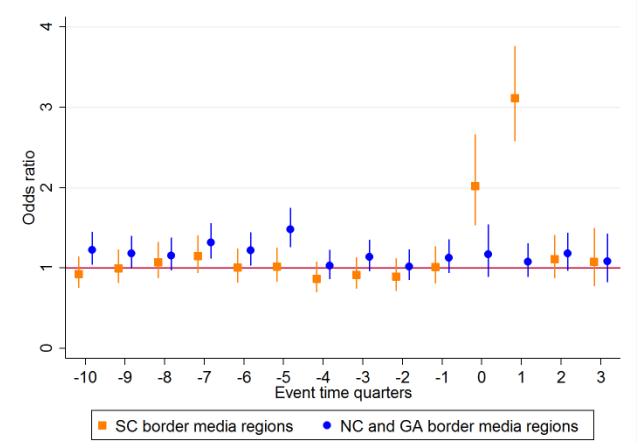
Panel B: Credit Freezes



Panel C: Credit Watches



Panel D: Opt-outs



Notes: These figures show the odds ratios for the likelihood of filing a specific type of protection for consumers in counties who share media markets between states. These odds ratios come from dynamic logistic regressions with control variables as described in the text and Table 2. Dots represent estimated odds ratios bound by 95 percent confidence bands. Standard errors are clustered at the individual level. Consumers in South Carolina counties that shared media regions were up to 80 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

Table 1. Number of Fraud Protection Filers in South Carolina, Georgia, and North Carolina

State	South Carolina		Georgia		North Carolina	
Quarter	CCP Population	# of Protection Filers	CCP Population	# of Protection Filers	CCP Population	# of Protection Filers
Q1:2010	176,292	2,170	354,806	5,073	350,326	4,317
Q2:2010	176,394	1,993	355,344	4,940	350,624	4,377
Q3:2010	176,946	2,180	356,012	4,760	351,347	4,352
Q4:2010	177,865	2,241	357,656	4,884	352,367	4,257
Q1:2011	178,195	2,122	357,930	4,979	352,673	4,073
Q2:2011	178,217	2,090	358,273	5,052	352,924	4,027
Q3:2011	178,652	1,838	359,094	4,514	353,588	3,562
Q4:2011	178,460	1,695	358,782	3,764	352,859	3,151
Q1:2012	178,410	1,710	358,551	3,952	352,282	3,305
Q2:2012	178,346	1,841	358,296	4,286	352,258	3,171
Q3:2012	178,588	1,373	358,580	3,134	351,818	2,512
Q4:2012	177,971	36,646	357,356	2,857	350,973	2,960
Q1:2013	177,662	15,180	356,640	2,939	350,251	2,533
Q2:2013	177,450	3,754	355,801	2,520	349,633	1,912
Q3:2013	177,158	725	354,548	2,152	348,978	1,477

Notes: This table presents the number of consumers in the CCP population who acquired any type of fraud protection service in each state for the first time in our sample in each quarter. The fraud protection take-up peaked in South Carolina at the time of the data breach (Q4:2012).

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

Table 2: Data Breach Sample Statistics

Variable	Nonmissing Observations	Mean	Standard Deviation
Initial alerts (proportion)	13,297,176	0.0017	0.0410
Extended alerts (proportion)	13,238,153	0.0002	0.0156
Freezes (proportion)	13,212,361	0.0005	0.0223
Opt-outs (proportion)	9,613,532	0.0057	0.0753
Credit watches (proportion)	11,135,948	0.0108	0.1034
Risk score	12,030,641	674.97	111.1906
Number of inquiries (3 months)	9,380,961	0.73	1.2934
Number of inquiries (12 months)	9,380,961	2.45	2.8934
Mortgage indicator (proportion)	11,992,041	0.3161	0.4649
Individual's age (years)	13,126,244	50.18	18.0090
Age of newest account (months)	11,989,875	32.30	46.9666
Number 120+ days past due occurrences — bankcards	9,486,479	0.56	3.0724
Number of accounts	12,245,631	13.70	10.8620
Percentage of revolving credit limit used	7,824,653	39.68	47.9386
Mobility indicator (proportion)	13,259,743	0.04	0.2014
Number of newspaper articles on identity theft	5,264,718	10.52	18.3538
Total Observations	13,297,176		

Notes: This table presents summary statistics for 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. Risk score and utilization rate are bucketed in the regressions to include missing value categories.

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

Table 3. The Effect of the South Carolina Data Breach and News on Fraud on Consumers

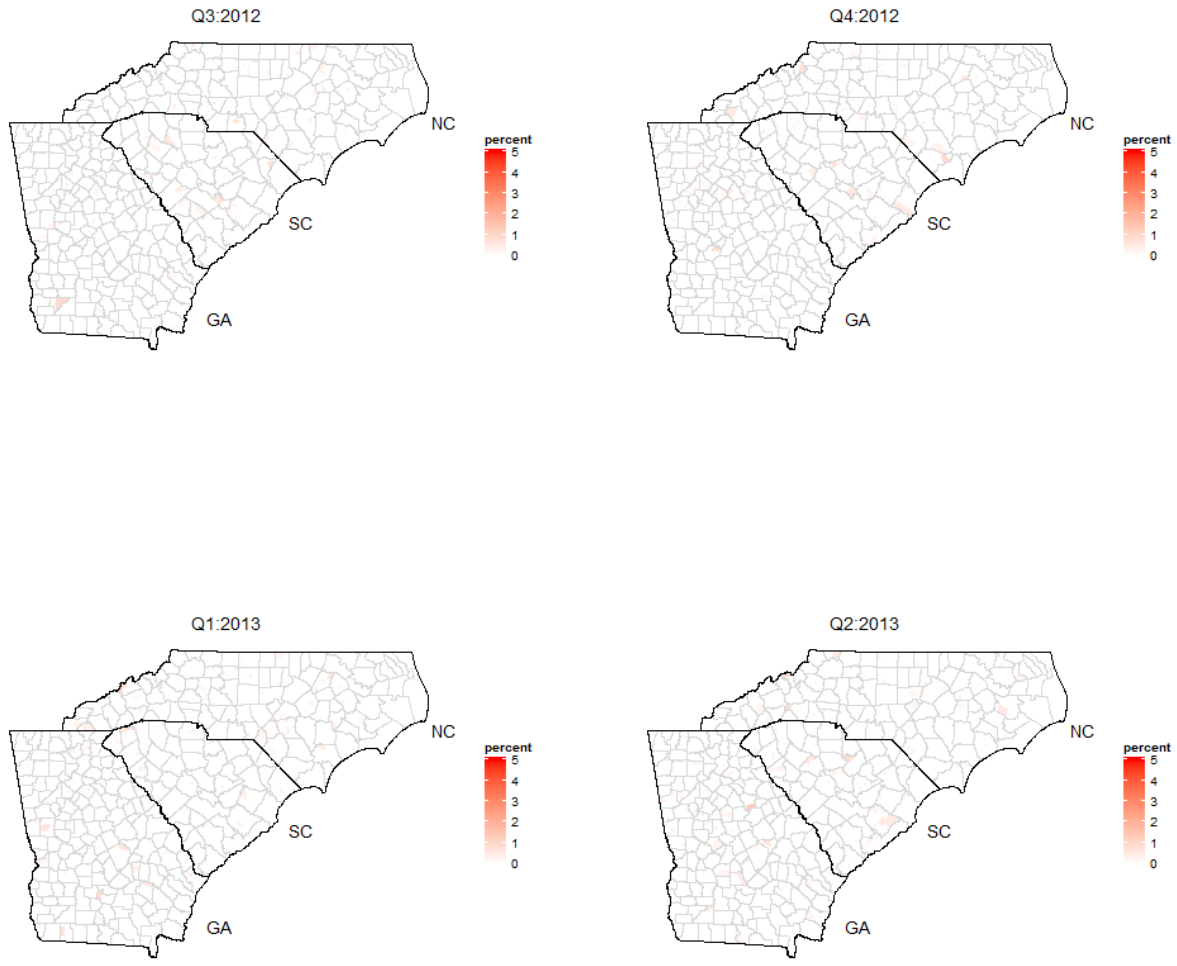
	(1) Initial alerts	(2) Extended alerts	(3) Credit freeze	(4) Credit watch	(5) Opt-out
Number of newspaper articles	1.01920***	1.01680	1.02998**	1.01278***	1.00360
	(0.00688)	(0.01822)	(0.01403)	(0.00387)	(0.00570)
South Carolina in Q4:2012	2.69901***	0.22550	17.07263***	71.00811***	1.54834
	(0.62891)	(0.25674)	(9.12672)	(7.77884)	(0.41248)
South Carolina in Q1:2013	4.32338***	0.82570	25.85916***	41.00240***	3.70233***
	(0.99872)	(0.59887)	(13.96360)	(4.72642)	(0.65381)
South Carolina in Q2:2013	1.55056	1.14096	1.14867	10.02220***	1.06528
	(0.42622)	(0.79233)	(0.77816)	(1.26761)	(0.23330)
News articles in South Carolina in Q4:2012	0.98812	0.92816	1.00071	0.96141***	0.96436**
	(0.01886)	(0.04332)	(0.04980)	(0.00976)	(0.01451)
News articles in South Carolina in Q1:2013	0.99080	0.93020	0.99951	0.97243***	0.96490**
	(0.01893)	(0.04312)	(0.04974)	(0.00987)	(0.01353)
News articles in South Carolina in Q2:2013	0.97238	0.92383*	1.01547	0.98841	0.97078**
	(0.01889)	(0.04289)	(0.05088)	(0.01019)	(0.01389)
Observations	2,690,434	2,787,230	2,803,099	2,178,602	1,955,344
Pseudo R2	0.0208	0.0617	0.0747	0.197	0.0214

Notes: This table presents odds ratios for the likelihood of filing a specific type of protection for independent variables in our dynamic logistic model. These odds ratios come from dynamic logistic regressions with control variables as described in the text and Table 2. Standard errors in parentheses are clustered at the individual level. *** denotes significance at 1 %, ** – at 5 %, and * – at 10 %. Consumers in South Carolina were statistically significantly more likely to file all types of fraud protection during the time of the breach and immediately afterward compared with consumers in other states. News has a small effect on all consumers' filing rates, but does not appear to enhance the response for South Carolina consumers at the time of the breach.

Source: Authors' calculations using data from 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

Appendix

Figure A1. 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

Table A1. Nexis Newspaper and Television Station Coverage

South Carolina	City	Georgia	City
The State	Columbia	*The Augusta Chronicle*	Augusta
The Greenville News	Greenville	*The Atlanta Journal-Constitution*	Atlanta
Post & Courier	Charleston	*The Macon Telegraph*	Macon
The Myrtle Beach Sun-News	Myrtle Beach	*Marietta Daily Journal*	Marietta
Anderson Independent-Mail	Anderson	*The Albany Herald*	Albany
CBS - 7 WSPA	Greenville	*The West Point Times-News*	West Point
The Associated Press State & Local Wire	North Charleston	*Atlanta Business Chronicle*	Atlanta
Aiken Standard	Aiken	*Waycross Journal-Herald*	Waycross
The Post and Courier	Charleston	*The Union-Recorder*	Milledgeville
The Herald	Rock Hill	*The Daily Citizen*	Dalton
The Island Packet	Bluffton	*LaGrange Daily News*	LaGrange
Daily Journal-Messenger	Seneca	*The Newnan Times-Herald*	Newnan
The Herald	Rock Hill	*Columbus Ledger-Enquirer*	Columbus
CBS - 13 WBTW	Florence	*Americus Times-Recorder*	Americus
NBC - 2 WCBD	Charleston	*The Dunwoody Crier*	Dunwoody
The Union Daily Times	Union	*Gwinnett Daily Post*	Lawrenceville
Morning News	Florence	*The Newton Citizen*	Conyers
The Gaffney Ledger	Gaffney	*The Daily Tribune News*	Cartersville
The Lancaster News	Lancaster	*The Rockdale Citizen*	Conyers
The Newberry Observer	Newberry	*The Moultrie Observer*	Moultrie
The Easley Progress	Easley	*Henry Daily Herald*	McDonough
The Pickens Sentinel	Pickens	*Tifton Gazette*	Tifton
The Powdersville Post	Piedmont	*The Thomaston Times*	Thomaston
The Georgetown Times	Georgetown	*Clayton News Daily*	Jonesboro
The Greer Citizen	Greer	*Cherokee Tribune*	Canton
The Herald Independent	Winnsboro	*Forsyth County News*	Cumming
The Cheraw Chronicle	Cheraw	*Creative Loafing*	Atlanta
South Carolina Lawyers Weekly	Columbia	*Valdosta Daily Times*	Valdosta
The Eagle-Record	St. George	*Jackson Progress-Argus*	Jackson
Chester News & Reporter	Chester	*Thomasville Times-Enterprise*	Thomasville
The Tiger Town Observer	Clemson	*Cordele Dispatch*	Cordele
Marion Star & Mullins Enterprise	Marion	*Roswell Neighbor*	Roswell
Pageland Progressive-Journal	Pageland	*Chatsworth Times*	Chatsworth
The Belton & Honea Path News-Chronicle	Belton	*South Metro Neighbor*	Forest Park
Coastal Observer	Pawleys Island	*The Douglas Neighbor*	Douglasville
News & Post	Lake City	*Henry Neighbor*	McDonough
		Northside - Sandy Springs Neighbor	Sandy Springs
		Flagpole	Athens
		DeKalb Neighbor	Decatur
		Paulding Neighbor	Dallas
		Bartow Neighbor	Cartersville
		The Clayton Neighbor	Forest Park

Notes: This table presents a list of newspapers included in our news index along with their respective headquartered cities.

Source: Authors' calculations using the Nexis news database

Table A1. Nexis Newspaper and Television Station Coverage (continued)

North Carolina	City	North Carolina	City
Charlotte Observer	Charlotte	*Tabor-Loris Tribune*	Tabor
Star-News	Wilmington	*Chapel Hill Herald*	Durham
The News & Observer	Raleigh	*The Courier-Tribune*	Asheboro
The Asheville Citizen-Times	Asheville	*The Franklin Times*	Lousiburg
The Pilot	Southern Pines	*Triangle Business Journal*	Raleigh
Winston-Salem Journal	Winston-Salem	*Indy Week*	Raleigh
The Daily Dispatch	Henderson	*The Chronicle*	Winston-Salem
The Daily Courier	Forest City	*The Business Journal of the Greater Triad Area*	Greensboro
High Point Enterprise	Forest City	*The Watauga Democrat*	Boone
CBS - 9 WNCT	Greenville	*The Tribune*	Elkin
News & Record	Greensboro	*North Carolina Lawyers Weekly*	Raleigh
NBC - 17 WNCN	Raleigh-Durham	*Triangle Business Journal*	Raleigh
FOX - 8 WGHP	High Point	*News & Record: Blogs*	Greensboro
The Stanly News and Press	Albemarle	*Cleveland Post*	Cleveland
Holly Springs Sun	Holly Springs	*Independent Tribune*	Concord
Salisbury Post	Salisbury	*The Anson Record*	Wadesboro
The Brunswick Beacon	Shallotte	*The Red Springs Citizen*	Red Springs
Fuquay-Varina Independent	Fuquay-Varina	*Creative Loafing*	Charlotte
The Mt. Airy News	Mount Airy	*The Carteret County News-Times*	Morehead City
The Sampson Independent	Clinton	*Charlotte Business Journal*	Charlotte
The Tryon Daily Bulletin	Tyron	*The Blue Banner: University of North Carolina, Asheville*	Asheville
Richmond County Daily Journal	Rockingham	*The News Reporter*	Whiteville
Garner News	Garner	*Mount Olive Tribune*	Mount Olive
The Laurinburg Exchange	Laurinburg	*Chapel Hill Herald*	Durham
Mooresville Tribune	Mooresville	*The Mecklenburg Times*	Charlotte
The News Herald	Morganton	*The St. Pauls Review*	Saint Pauls
The Robesonian	Lumberton	*The Randolph Guide*	Asheboro
The Nashville Graphic	Nashville	*The Pilot*	Pilot Mountain
The Apex Herald	Apex	*The Pender Post*	Burgaw
The Wilson Daily Times	Wilson	*The Mountain Times*	Boone
The Enquirer-Journal	Monroe	*The Yadkin Ripple*	Yadkinville
Mountain Xpress	Asheville	*Jefferson Post*	Jefferson
The News-Topic	Lenoir	*The Reidsville Review*	Reidsville
The Sylva Herald & Ruralite	Sylva	*The Charlotte Post*	Charlotte
The Daily Southerner	Tarboro	*Spring Hope Enterprise & The Bailey News*	Spring Hope
Charlotte Business Journal	Charlotte	*The Blowing Rocket*	Blowing Rock
Bladen Journal	Elizabethtown	*The Courier-Times*	Roxboro
The Thomasville Times	Thomasville	*The Independent Weekly*	Durham
The Sanford Herald	Sanford		

Notes: This table presents a list of newspapers included in our news index along with their respective headquartered cities.

Source: Authors' calculations using the Nexis news database