# DO US STATE BREACH NOTIFICATION LAWS DECREASE FIRM DATA BREACHES?

Working Paper:  Comments Welcome
This Draft:  March 8, 2022

Brad N. Greenwood♣
School of Business
George Mason University
Enterprise Hall, Room 105
4400 University Drive
MS 1B1
Fairfax , VA 22030
USA
Tel +1 (703) 993-1880
Email brad.n.greenwood@gmail.com
Web http://www.fixedeffects.com/

&

Paul M. Vaaler
Law School & Carlson School of Management
University of Minnesota
3-424 CarlSMgmt
321 19th Avenue South
Minneapolis, MN 55455
USA
Tel +1 (612) 625-4951
Email vaal0001@umn.edu
Web https://carlsonschool.umn.edu/faculty/paul-vaaler

♣ Corresponding Author

# DO US STATE BREACH NOTIFICATION LAWS DECREASE FIRM DATA BREACHES?

## ABSTRACT

From 2003-2018, 50 states and the District of Columbia enacted breach notification laws (BNLs) mandating that firms notify affected persons and undertake mitigation when a data breach occurs. BNLs were supposed to decrease data breaches and develop a market for data privacy where firms could strike their preferred balance between data security quality and cost. We find no evidence for either supposition. Results from two-way difference-in-difference analyses indicate no decrease in data breach incident counts or magnitudes following BNL enactment. Results also indicate no longer-term decrease in data misuse after breaches. These non-effects persist for different firms, time-periods, data-breach types, and BNL types. Apparently inconsistent notification standards, insufficient penalties for untimely notification, and inadequate information dissemination to the public explain BNL ineffectiveness. An alternative federal regime could address these shortcomings and let a national BNL achieve goals state BNLs failed to meet. (142 words)

**Key Words**: Data security, breach notification laws, consumer privacy, difference in difference

# INTRODUCTION

Consumer data breaches have become regular occurrences affecting some of the largest US firms. October 2013 saw 153 million consumer records exposed in a hack at the software publisher, Adobe (*Guardian*, 2013); October 2016 saw 412 million user accounts compromised at the online dating firm, Adult Friend Finder (Computer World, 2016); September 2017 saw the financial information of 147 million people exposed by a breach at the credit assessment giant, Equifax (Equifax, 2019); and April 2021 saw personal information for 533 million Facebook users stolen (ITech, 2021). Breaches draw fines and enforcement actions from different regulators like the US Federal Trade Commission (FTC), but the received wisdom is that these penalties are insufficient to prompt firms to devote more time and money to assure greater data protection and consumer privacy (Winn 2009). If true, then the received wisdom is also troubling. As Becker (1968) noted more than 50 years ago, insufficient incentives for firms to desist from profitable activities that impose costs on society mean the activities will continue.

For their part, state legislatures in the US have sought to adjust those incentives and decrease data breaches by passing breach notification laws (BNLs) (Solove & Schwartz, 2019). California passed the first BNL in 2003. As Table 1 below shows, the next 15 years saw the other 49 states and the District of Columbia follow California's lead. And as Kosseff (2017) and others (*e.g.*, Chesney, 2020) have noted, these 51 BNLs vary on different coverage dimensions such as how data breaches are defined, when data breach notification requirements for firms are triggered, which individuals and organizations firms must then notify, what liabilities firms then have, and what rights and remedies different individuals have in the wake of a data breach and notification.

But no matter how BNLs differ, they share a basic intuition. By compelling timely breach disclosures, BNLs identify and inform consumers, law enforcement officials, and other community members about transgressing firms. In the near term, BNLs should reduce data breaches by imposing timely notification costs and liabilities for untimely notification. Over time, BNLs should also foster the development of a “market” for data privacy where consumers and others can learn which firms are better and worse as data stewards. Firms can position themselves in that market based on their own cost-benefit analysis of data breach likelihoods and prevention. Through this process, BNLs not only bring down overall data breach numbers, but also permit firms to strike their own balance between data security quality and cost. BNLs thus meet the challenge posed by Becker (1968) to let individual choice and market response guide decisions about appropriate sanctions to deter socially undesirable behavior.

----------Insert Table 1 approximately here----------

Does the evidence support that intuition? With few exceptions (Romanosky, Telang, & Acquisti, 2011), little empirical work has been devoted to investigating whether BNLs actually decrease harmful data breaches by firms in the US. This is concerning. Data hacking operations are increasingly sophisticated (Gupta, 2018). Markets for stolen consumer identities on the dark web have more participants (Steel, 2019). Yet, consumers blithely share more personal data online without appreciating professional and personal risks (Acquisti, Brandimarte, & Loewenstein, 2020; Acquisti & Fong, 2020). As the costs of individual data breaches increase, so does the need to understand whether and when BNLs decrease their number and magnitude.

We respond by asking two research questions: 1) Do US state BNLs (BNLs) decrease the count of breach events? 2) Do they decrease the magnitude of records compromised in a breach event? Since BNLs differ along various dimensions, our answers to these two questions also compel investigation about whether certain types of BNLs decrease data breach counts and magnitudes more than others –whether, for example, BNLs providing consumers with a private right of action to sue firms for legal damages. Since malicious actors may instigate data breaches or exploit them after others inadvertently cause data breaches, answer to our questions also compel investigation about whether BNLs decrease follow-on malicious uses like identity theft and fraud.

We generate evidence answering our two research questions using data from the Privacy Rights Clearinghouse (PRC), a California-based, not-for-profit organization aggregating information on data breaches in firms since 2005 (Collins, 2019; Goel & Shawky 2014; PRC, 2021). PRC data include information on breached firms, locations, and numbers of records compromised. PRC data also include information on data breach cause –for example, whether the cause was an error by an employee inside the firm or by an outside hacker. We use PRC data to estimate change in breach event counts and magnitudes by exploiting the phased nature of BNL enactments from 2003-2018. Our estimations utilize a two-way fixed effects approach permitting causal inference about the impact of BNLs on breach event counts and magnitudes in different US states from 2005-2019, that is states (and the District of Columbia) after 2003 BNL enactment in California and 2005 enactment of BNLs in 11 other states listed in Table 1. We implement these estimations for all states, firms, BNL types, and data breach types. We do the same for: specific types of BNLs such as those providing private rights of action (PROAs); specific types of data breaches including those caused by employee errors inside firms and those caused by outside hackers; and specific types of firms such as smaller ones where state corporate domicile and breached customer location tend to overlap. We use the same two-way fixed effects approach to make causal inferences about the impact of BNLs on follow-on counts and magnitudes of identity theft and fraud. For these analyses, we use alternative data from the FTC's Consumer Sentinel Data Book covering the same 15 years. Again, we implement these estimations generally and for specific types.

Our analyses of PRC data indicate no significant decrease either in data breach counts or magnitudes, either generally or for those specific types. Consistent with prior work (Romanosky *et al*., 2011), we do find a significant decrease in identity theft incident magnitudes during early years of BNL enactments (2005-2010). Across all 15 years, however, we observe no significant decreases in counts or magnitudes of identity theft and fraud incidents, either generally of for those specific types. Our different BNL “non-effects” appear to be precisely-estimated nulls. Together, they call into question the principal regulatory policy of state legislatures seeking to decrease data breaches and develop a market for data privacy.

Our findings matter for academic research, related industry practice, and public policy. They provide researchers with the first broad-sample statistical evidence of BNL ineffectiveness derived from the long-term study of data breaches and follow-on misuse of breached data by malicious actors. They confirm earlier research skepticism about the efficacy of state-based regulation of data privacy in firms (Park, 2019) and empirically challenges the conclusion that such state-based regulation decreases related data misuse in the long term.

Our findings also suggest the need for change in data breach standards, (dis-)incentives, and information. Current, consistent technological standards defining data breaches, timely notification, and mitigation would guide firms in adopting industry-wide practices across the US. Stronger penalties and related liabilities for failing to meet such standards will speed their adoption. Readily-accessible public information on firm breach and mitigation response history would guide consumers in choosing firms with the right mix of data security cost and quality. Market development requires both. To that end, we propose an alternative US federal BNL regime featuring the creation of an expert body and supporting staff. This body would set technological standards and publish data in a readily accessible format for consumers, public officials, and other stakeholders. This new regime could spur immediate decrease in data breach counts and magnitudes as well as longer-term development of the data privacy market state BNLs apparently failed to develop over 20 years.

## BACKGROUND INFORMATION AND HYPOTHESES

A brief review of BNLs and related research lays a helpful foundation for our study. BNLs represent the principal regulatory policy approach US state legislatures took to curb data breaches in the 2000s and 2010s. Typically, BNLs compel public agencies and private organizations to inform affected individuals about security breaches of personally identifiable information (PII). The definition of what constitutes a data breach varies across states, as does who must be informed of the breach, and what constitutes PII (Peters, 2014, Solove & Schwartz, 2019). Failure to comply with notification laws typically prompts state civil penalties (Faulkner, 2007). More egregious cases of negligence with consumer data might also draw the attention of US federal authorities like the FTC for enforcement actions and penalties. Table 2 shows that, by 2019, nearly all US federal appellate circuits had established a basis for standing and injury in fact for a data security-based privacy harm. Consumers could then pursue claims against transgressing firms individually or in class actions.

----------Insert Table 2 about here----------

Others have analyzed foreign national (*e.g.*, Kemp, Buil-Gil, Mirò-Llinares, & Lord, 2021) and supranational (*e.g.*, Karyda & Milton, 2016) approaches to data privacy and security regulation, but our interest is the US approach, which has an uneven federal regulatory patchwork. A handful of statutes target specific industries or groups and define specific data security standards: the Gramm Leach Bliley Act and the Fair and the Accurate Credit Transactions Act (FACT) cover financial data; the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act cover healthcare data; and the Children's Online Privacy Protection Act (COPPA) covers data on children under the age of 13 (Faulkner, 2007; Rode, 2006; Stevens, 2012). In 2002, the Sarbanes-Oxley Act (SOX) overhauled financial reporting and investor protections in publicly-listed firms. Although SOX did not explicitly address data breaches, recent US Securities and Exchange Commission (SEC) releases (SEC, 2018) and guidance (SEC, 2020) articulated new disclosure requirements for material cybersecurity risks and data security safeguards as part of broader corporate governance oversight mandated by SOX.

Otherwise, regulation governing data breaches has been left to individual states with BNLs as the principal state response (Peters, 2014; Stevens, 2012; Wolf, 2018). A state-by-state approach has intuitive appeal. It permits experimentation by state policy-makers and gives firms some choice in data privacy regime (Needles, 2009; Rode, 2006). In practice, however, most commentators find the approach wanting (Joerling, 2010; Peters, 2014; Stevens, 2012). BNL application generally follows the state location of the breached individual rather than the state domicile of the firm. Thus, enactment of a BNL in a large population state like California essentially implicates any firm with a national customer base. As discussed by Tom (2010), consumer groups have favored the enactment of a federal BNL setting a single set of standards, penalties, and information on data breaches. Firms are similarly disposed. State laws impose inconsistent requirements and increasing costs for firms dealing with up to 51 different state regulatory regimes (Peters, 2014). In this context, it is not surprising that many legal commentators advocate for federal legislation pre-empting state BNLs and creating a single federal BNL (Faulkner, 2007; Peters, 2014; Picanso, 2006; Tom, 2010).

Empirical work also reflects skepticism about a state-by-state approach for addressing data breaches. Much of this work is anecdotal and bereft of rigorous statistical methods to identify effects. Still, it largely suggests that civil liability in the wake of BNL enactment neither prevents company negligence nor adequately compensates victims (Faulkner, 2007; Joerling, 2010). What statistical work does exist largely corroborates our assessment. Goel and Shawky (2014) use an event study approach to demonstrate that cumulative abnormal share returns to firms after a data breach are negative as expected, but that these negative effects are diminished (not magnified) after BNL enactment. Laube and Böhme (2016) analytically demonstrate that, even under optimistic assumptions, mandatory reporting requirements in BNLs are unlikely to generate substantial data breach reductions because optimal audits and sanctions are difficult to formulate and implement. In perhaps the only encouraging piece of empirical work, Romanosky and colleagues (2011) find that BNLs decrease incidences of identity theft, a frequent consequence of data breaches. That said, the authors also point out that instances of identity theft have become more difficult to identify, perhaps also rendering their findings in more recent data more difficult to replicate.

## EMPIRICAL METHODS

### Data and Sampling

To evaluate evidence on data breach counts and magnitudes following BNL enactments, we rely on PRC data (2021). Founded in 2005, PRC aggregates information on data breaches for research and public policy-making purposes (Ayyagari, 2012; Goel & Shawky, 2014). PRC grew out of an initiative at the University of California San Diego and the State of California where it still sources much of its data breach information. PRC also collects information from government agencies in other states such as Indiana, from US federal government agencies such as the Department of Health and Human Services Office for Civil Rights, and from non-governmental organizations and individuals such as DataBreaches.net. PRC also collects its own data from media reports. As of January 2022, PRC data included information on more than 9,000 instances data breaches at (mostly) firms, as well as government agencies and other types of organizations across the US. It is the largest, publicly-accessible database on firm data breaches traceable to specific states, thus making it a popular source for academic research and related policy analyses on data breach causes and consequences (see, *e.g.*, Edwards, Hofmeyr, & Forrest, 2016).

In addition to sheer quantity, PRC data quality matters for our study. On the one hand, PRC data contain information on both data breach incidents and the number of records associated with each incident. This permits analyses of counts and magnitudes. PRC breach data are also categorized into several different types, including whether the breach was caused by an inside employee handling error of by an outside hacker. This allows us to analyze heterogeneity in the cause of breach counts and magnitudes.

On the other hand, PRC data only start in 2005, that is, two years after BNL enactment in California and in the same year as BNL enactment in 11 other states. Thus, our analyses may understate the impact of early and potentially quite important BNLs. That said, the concern does not undermine the basic validity of our analyses. Empirically, it means that observations from these states will not help in identification of BNL enactment effects, but they will still help in identifying broader time trends. Another concern is that PRC data on breach magnitudes sometime attribute all records breached only to a firm's state of domicile rather than to each of the states where firm customers are located. Such misattribution is more likely for incidents of massive data breaches at large publicly-listed companies such as the 2017 Equifax breach (Equifax, 2019). Thus, our analyses may skew estimates of BNL enactment effects in states with many large publicly-listed companies such as New York. Empirically, it means that we should compare any general analyses of BNL impact on data breach magnitudes sampling with re-analyses using sub-sample including only smaller firms. They are more likely have greater overlap state corporate domicile and customer location. The PRC data permit sub-sampling for these and other robustness analyses.[1]

Our analyses also rely on data about BNLs from Solove and Schwartz (2019) and the National Conference of State Legislatures. Both sources let us identify BNL enactment dates and characteristics: triggers for notification, data subjects and owner to be notified, public agency and private rights of actions arising from data breaches. These data sources comprise the foundation for our core analyses of BNLs and firm data breaches occurring in the US from 2005-2019. They yield a sample of 765 state-year observations of data breach events in 51 "states" including the District of Columbia. Those events occur before and after BNL enactment in each state.

### Variable Definitions

***Dependent Variable*.** We initially define two dependent variables for use in our analyses. The first

[1] We defer for the moment description of FTC data used to test whether BNLs decreased incidents of identity theft and fraud.

dependent variable is the count of data breach events occurring in each state *j* in year *t*. This first dependent variable allows us to assess changes in the annual frequency of data breached after BNL enactment. The second dependent variable is the number of records breached in each state *j* in year *t*. This second dependent variable allows us to assess changes in the annual magnitude of data breached after BNL enactment. This dependent variable can be nearly zero or in the millions. We take the natural log of this dependent variable, thus interpreting magnitude effects as elasticities.

***Independent Variables*****.** The primary independent variable is a 0-1 dummy taking the value of one when a BNL has been enacted in state *j* in year *t.* In deference to heterogeneous definitions of when a breach notification requirement is triggered, we take two approaches. Our first approach defines BNL enactment with the year *t* when any type of BNL comes into force in state *j*. Our second approach defines BNL enactment with the year *t* when a type of BNL creating a private cause of action comes into force in state *j*. Our first approach is broad, but may not account for a sub-set of BNLs using civil liability to individuals to create stronger firm incentives to guard against data breaches. Our second approach narrows BNL enactment criteria but may not account for BNLs that, though they create no private right of action, may still create strong firm incentives to guard against data breaches if vigorously enforced by public officials like state attorneys general. We present results below using both approaches.

***Controls*****.** We employ a difference-in-difference estimation strategy, so we also include two-way state (cross-sectional) and year (time-series) fixed effects. Inclusion of both facilitates the most granular measurement available. Intuitively, state fixed effects should absorb any time invariant heterogeneity between states –for example, California being substantially larger demographically and economically than, say, Rhode Island. Year fixed effects should absorb any universal trends across states changing from year to year –for example, an increasing trend in data breaches across states.

### Model Specification, Estimation, and Hypothesis Tests

We take a two-way fixed effects approach to estimate change in data breach counts and magnitudes after BNLs are enacted. Formally, we estimate effects using the following equation:

$$y_{jt} = \beta_1 x_1 + \varrho_j + \tau_t + \varepsilon$$

$\beta_1$ captures the key difference in difference, that is, the difference in data breach counts and magnitudes in states following BNL enactment. $\varrho$ is a vector of state fixed effects indexed by $j$. $\tau$ is a vector of time (year) fixed effects indexed by $t$. $\varepsilon$ is the error term. When assessing data breach magnitudes, $y_{jt}$ is the natural log of the number of records breached in state *j* in year *t*. To estimate variation in that number, we use an ordinary least squares (OLS) regression. $\beta_1$ is interpreted here as the elastic change in the number of breaches in "treated" states where a BNL has been enacted. When assessing data breach counts, $y_{jt}$ is the number of data breach events in state *j* in year *t*. To estimate variation in this number, we use quasi-maximum likelihood Poisson (Poisson) regression. $\beta_1$is interpreted as the marginal change in absolute counts. This second estimator avoids complications following from logged OLS and fixed effect negative binomial estimators (Allison & Waterman, 2002; Silva & Tenreyro, 2006, 2011). No matter the dependent variable measure or estimator, our hypotheses that BNL enactment decreases data breach counts and magnitudes reduces to tests of whether $\beta_1 < 0$.

### Other Methodological Issues and Innovations

Four additional methodological issues merit brief discussion given our approach to analyzing BNL effects on data breach counts and magnitudes: 1) whether the assumptions of difference-in-difference analysis hold; 2) whether specific data breach categories might be more responsive to BNLs; 3) whether, given the expectation of a null result, we can differentiate between the absence of statistical significance and the absence of any effect; and 4) adjustment for multiple comparisons.

Regarding the first issue about difference-in-difference analysis, the primary assumption is that dependent variable for treatment and control groups is trending in a parallel manner prior to treatment (Angrist & Pischke, 2008). The intuition is simple. If treated states are accelerating in data breaches prior to treatment but untreated states are decelerating in data breaches, then estimation of the treatment effect could be biased and the treatment effect will be inappropriately attributing post-treatment differences to pre-treatment trends. To determine whether treated and untreated states are trending in this parallel manner, we use a variant of the event-study method proposed by Autor and colleagues (2003) and exemplified in previous research using difference-in-difference analysis (Burtch, 2018; Carnahan, 2017; Zamoff *et al*., 2022). In doing so, we estimate the effect semi-parametrically by creating a series of relative time indicators which capture how far state-year *jt* is from the period when *j* receives treatment. This allows us to visualize the effect over time before and after treatment. The *t* and *t*-1 terms are omitted and serve as bases for comparison. Relative time indicators more than four years before treatment (Rel Time *t* - 4) and 10 years after treatment (Rel Time *t* + 10) are collapsed for interpretability.

Regarding the second issue about data breach category, there are two ways that firms might approach the question of limiting data breaches. First, firms might be more concerned about malicious attacks from outside hackers than inside employees making data handling errors. Such a conclusion is reasonable if the firm possesses valuable consumer data which could be exploited by malicious outside agents. Second, owing to the fact that many data breaches stem from poor internal management of employees, it is possible that firms might institute stricter internal policies which prevent their employees from unintentionally disclosing protected data – for example, by requiring uniform data encryption policies (Winn, 2009). We investigate both possibilities. It is plausible that a change in one is not visible with unaddressed data poisoning the pool. Taking this approach further allows us to avoid the “file-drawer” problem, wherein researchers gravitate towards significant and publishable results rather than insignificant ones often failing to reach the public through publication (Dynes & Holbein 2020; Franco, Malhotra,

& Simonovits, 2014; Goldfarb & King 2015).

Regarding the third issue about differentiating insignificant results from precisely-estimated null effects, we turn to research analyzing differentiation in economics, political science, business, medicine, and law (Ahammer, Halla, & Schneeweis, 2020; Dynes & Holbein 2020; McNamara, Vaaler, & Devers, 2003; Walker & Nowacki, 2011). Traditional hypothesis testing relies on rejecting the null hypothesis that two terms are not statistically different. Such testing typically provides an estimate of difference between two groups and the statistically-derived confidence in that difference. This approach becomes problematic when making comparisons failing to reject the null. This situation often arises in underpowered empirical studies (Gelman & Carlin, 2014). Following Dynes and Holbein (2020), we address this third issue by taking two approaches. First, following research on statistical sub-significance, we set 36 percent of a standard deviation as a threshold for what constitutes a meaningful difference from zero (Hartman & Hidalgo, 2018; McCaskey & Rainey, 2015). Second, following work in economics, we discuss minimum detectable effects (MDEs) (Duflo, Glennerster, & Kremer, 2007; Haushofer & Shapiro, 2016). In doing so, we compare the size of any estimated coefficient to MDEs with 95 percent confidence intervals at 80 percent power (Dynes & Holbein, 2020; Haushofer & Shapiro, 2016).

The fourth issue addresses corrections to the standard 95 percent confidence interval when analyses include multiple dependent variables. Again, this relates to the file-drawer issue (Franco *et al.*, 2014). Increasing the number of treatments also increases the likelihood of finding some significant correlation purely by chance. That said, we choose *not* to employ a correction in what follows given our expectation of a null result. A confidence interval correction would widen intervals, thus making it more difficult to observe any significance. But our goal is to make it more difficult *not* to observe significance, thus our non-correction strategy.

# RESULTS

## OLS and Poisson Regression Results for Data Breaches

We start with OLS and Poisson regression results addressing research questions about whether BNLs reduce data breach counts or magnitudes. They are reported in Table 3.  Results indicate no systemic correlation between BNL enactment and change in either data breach magnitudes or counts. Columns 1 and 2 report results regarding data breach magnitudes. Neither enactment of any BNL (Column 1) nor enactment of a BNL with a private right of action (PROA) (Column 2) significantly influences the log number of records breached. Convention also indicates that the effects are a precisely estimated null. The p-values are p = 0.714 (Column 1) and p = 2.88 (Column 2) respectively. The standard deviation of the log number of records breached is 4.83, 36 percent of which is 1.74. Both point estimates thus fit well within what Hartman and Hidalgo (2018) argue constitutes a meaningful difference from zero. Moreover, the estimated effects are positive (not negative), contrary to the intended effect of BNLs.

Columns 3 and 4 of Table 3 report results regarding breach counts. There, we again see no change after Poisson regression estimation, whether BNL enactment is broadly (Column 3) or more narrowly (Column 4) defined. These coefficients again constitute precisely estimated nulls. The p-values are p = 0.766 (Column 3) and p = 0.697 (Column 4), nowhere near conventional thresholds of statistical significance or a third of a standard error from zero. An equivalence test using the Hartman and Hidalgo (2018) approach further passes muster --the threshold being 6.75 or 36 percent of 18.75. Results reported in Table 3 generally indicate no significant relationship between BNL enactment and a change in either data breach counts or magnitudes.

----------Insert Table 3 approximately here----------

Turning next to the event study results in Table 4, we observe neither significant and systemic pre-treatment, nor significant and systemic post treatment, effects. This is striking. In the pre-treatment measurements –for example, effects four years prior to treatment (Rel Time *t-*

4)- there is no systematic trend up or down.  This suggests that the parallel pre-treatment trends assumption of the difference-in-difference analysis is not demonstrably violated (Angrist and Pischke 2008; Autor 2003). Post-treatment estimations are also devoid of significance at generally-accepted levels. Perhaps most striking is that, of the 57 estimated coefficients estimated, only one is significant --Rel Time *t*-4 in Column 3.  This is less than would be predicted by a random draw --1 in 20 at $p < 0.05$. An equivalency test at the 36 percent level passes for all estimations. Not a single coefficient breaches the threshold. Indeed, with the exception of Rel Time *t*+5 and Rel Time *t*+ 9 in Column 1, not a single estimate breaches 10 percent of the Hartman and Hidalgo (2018) thresholds. Once again, these results offer no substantive support for the hypothesis that BNLs reduce data breach counts or magnitudes.

----------Insert Table 4 approximately here----------

Table 5 presents results from OLS and Poisson regression analyses of BNL enactment effects on data breach counts and magnitudes related to external causes such as hacks and internal causes such as employee errors. Here, the intuition is that effects might be concentrated in a single type of breach of greater concern to firms. Once again, we observe no significant effects across the estimations. Most of the coefficients are positive. All equivalency tests at 36 percent easily pass. Again, these results offer no substantive support for the hypothesis that BNLs reduce data breach counts or magnitudes.

----------Insert Table 5 approximately here----------

### Difference-in-Difference Diagnostic Analyses

One concern with multi-site, phased difference-in-difference analysis is the potential for inverse weighting issues. In short, the estimation of the treatment is the sum of weighted comparisons of treated and untreated observations based on when treatment occurs. Each treatment cohort has its own weight on the estimate. Derived coefficients may be biased in a base difference-in-difference analysis. Goodman-Bacon (2018), Callaway and Sant'Anna (2020), and Baker and colleagues (2021) elaborate on these basic points.

Consistent with these studies, we implement two diagnostic analyses. First, a Goodman-Bacon (2018) decomposition analysis assesses weightings associated with each individual treatment. Results are presented in Table 6 and displayed graphically in Figures 1A and 1B. As can be seen, while there is heterogeneity in the effect across the different comparison groups, no inverse weighting problem emerges. This bolsters the case that the estimated effects are not significantly biased. We exclusively model the linear estimations as no Poisson equivalent to the decomposition exists.

----------Insert Table 6 approximately here----------

----------Insert Figures 1A and 1B side by side approximately here----------

Second, we replicate the linear estimations using the group-time average treatment effects estimator created by Callaway and Sant'Anna (2020). As with the decomposition, no Poisson version of this tool exists. The purpose of this estimator is two-fold. First, it recovers the properly weighted difference in difference. Second, it assists in diagnosing the parallel trends assumption. Graphical results of the estimation are presented in Figures 2A and 2B. As can be seen in both figures, there is little in the way of pre-treatment trend. Further, there is no demonstrable dip in the number of records breached after BNL enactment.

----------Insert Figures 2A and 2B side by side approximately here----------

## Equivalency Tests

One concern with traditional econometric approaches to questions like the ones proposed is that hypothesis testing hinges on the rejection of values not equaling zero. Failing to reject the null is not traditionally interpreted as there being zero effect. Hence the adage: The absence of evidence is not evidence of absence. In this context, we seek analyses establishing the similarity of two items. One such analysis used in medical research is equivalency testing (Walker & Nowacki, 2011). Intuitively, the idea is to determine if the confidence intervals of two treatments overlap.

If they do, or the confidence intervals are not different from a randomly generated pseudo estimate, then medical treatments are deemed to have similar efficacy. Such an approach is appealing here because it allows us to examine whether the treatment effect is outside the bounds of a randomly generated pseudo effect.

To examine if the effects are demonstrably similar to an effect generated at random, we replicate the estimations reported in Table 3. However, instead of using the actual treatment, we randomize the treatment based on an identical portion of the sample. Using this randomization, we then estimate the pseudo effect, that is, the effect that might appear purely by chance. This process is executed 1000 times for each estimation with the coefficient stored each time. Using these pseudo-estimates, we then conduct a mean-equivalence t-test. The appeal of this approach is that we can directly observe if the treatment is superior or inferior to a random draw.

Results are reported in Table 7. In Column 1, the test rejects the assertion that the randomly generated treatment is either larger (Pr ($T > t1$)) or smaller (Pr ($T > t2$)) than the actual coefficient. The same is true for Columns 2 and 4, once again underscoring the precisely estimated nature of the null effects. Results in Column 3 are less clear. On the one hand, they indicate that the random effect is not larger than the estimated effect. On other hand, they also indicate that random coefficient is smaller than the estimated effect. Indeed, the estimated effect is more than two standard deviations *larger* than the randomly generated effect. This difference indicates that the estimated breach count is *not falling* after BNL enactment.

----------Insert Table 7 approximately here----------

Taken together, Tables 3-6 and Figures 1-2 indicate the following:  1) BNL enactment did not decrease data breaches whether measured as counts or magnitudes and whether caused internally or externally; and 2) BNL null effects are generally estimated with precision.

### OLS and Poisson Regression Results for Identity Theft and Fraud

These core findings are consistent with the position that BNLs have neither significantly decreased data breaches nor developed a market for data privacy where firms can choose deterrence levels and consumers can observe and respond to those choices. Critics might respond that BNLs have a more limited aim. They are supposed to deter related data misuse due to, say, identity theft or fraud. Data breaches are not themselves problematic. It is the combination of data breaches and then misuse of breached data by malicious actors. Thus, the motivation for BNLs is data crime rather than data breach decrease. And timely notice of data breaches is related to whether consumers can take timely reparative actions to avoid victimization by malicious actors. For example, timely notice of breaches in their credit card data would give the credit card holders opportunities to cancel credit cards and freeze credit reports before misuse by malicious actors.

Evidence from prior research suggests that BNLs may decrease incidences of identity theft (Romanosky *et al.* 2011). That said, this evidence is based on data from the 2000s when, as Table 1 indicates, the wave of BNL enactments was still building. We can re-evaluate this evidence after BNL enactments across all states. We can also evaluate this evidence after the substantial evolution of identity theft and fraud practices in the 2010s (Gupta 2018; Irshad & Soomro, 2018; Steel, 2019). That decade saw larger and more sophisticated instances of identity theft and fraud (Gupta, 2018). It also saw the development of markets for trading stolen identities through the so-called dark web locations such as the Tor network (Steel, 2019). It also saw the rise of social media creating new public points where data might fall into the hands of malicious actors (Irshad & Soomro, 2018). In this context, we should understand whether the initially-suppressive effect of BNLs enacted in the 2000s had longer-term effects.

To gain that understanding, we draw on data from the FTCs Consumer Sentinel Report (FTC). Used widely in prior work (Anderson, 2019; Raval, 2020; Romanosky *et al.*, 2011), the FTC data provide information on incidents of identity theft and fraud in each state. Consistent with our prior sampling approach, we collect information on these incidences for all states from

2005-2019. Unlike data from the PRC, we have no information on the underlying cause of such data misuse. We simply know that a theft or claim of fraud was recorded in a given state and year. We therefore estimate the effect using the log of files misused using OLS regression and the count of misuse incidences, no matter the number of files involved, using a Poisson regression. These two dependent variable measures parallel the data breach count and magnitude measures.

We first replicate prior work by Romanosky and colleagues (2011) documenting that BNLs enacted from 2005-2010 decreased incidents of identity theft. Replication study results are reported in Table 8. OLS regression of logged identity fraud magnitudes following BNL enactment during the same time-period yields the same negative sign (-0.0514) significant at the 10 percent level. These results suggest a concordance of data and methods, and increase confidence in follow-on study of longer-run effects reported in Tables 9-10.

----------Insert Table 8 approximately here----------

Table 9 reports results from OLS and Poisson regression of identity theft and fraud incident counts and magnitudes following BNL enactment from 2005-2019. Results there indicate no significant negative BNL enactment effects. Indeed, we observe in Column 4 a positive (not negative) effect of BNL enactment coefficient (0.174) significant at the 10 percent level. The count of fraud incidents in a state *increased* after enactment of a BNL. Comparison of the estimated coefficients to the Hartman and Hidalgo (2018) thresholds also suggest precisely estimated  nulls except in the case of the Column 4 coefficient. Excepting the Column 4 coefficient, p-values for others are nowhere near conventional thresholds of significance (averaging at $p = 0.4155$).

----------Insert Table 9 approximately here----------

Table 10 reports on pre-treatment and post-treatment trends. We observe some initial declines (Column 3) in the number of thefts when the effect is estimated semi-parametrically, but these effects do not appear to persist in the longer term. Moreover, there do not appear to be any persistent pre-treatment trends across the estimations, suggesting no egregious violations of the parallel trends assumption important in difference-in-difference analyses. A replication of the effect over time using the Callaway and Sant'Anna (2020) approach corroborates both the lack of persistent significant effect and the absence of significant pre-treatment trending. Finally, we note that none of the estimated coefficients, even those that are significant at commonly-accepted levels, breach the effect size threshold offered by Hartman and Hidalgo (2018). Taken together, these results indicate that BNLs have not little in the longer term to reduce either identity theft or fraud that may follow in the wake of data breaches.

----------Insert Table 10 approximately here----------

----------Insert Figures 3A and 3B side by side approximately here----------

### Evaluating and Dismissing Alternative Explanations

While the above analyses constitute a broad evidentiary basis for concluding that BNLs have had no meaningful effect on either data breaches or the follow-on misuse of breached data, our evidence is vulnerable to various rebuttals. Here are four: 1) BNLs may have had temporary early deterrence effect in the same way they did on incidences of identity theft; 2) BNLs may be effective in deterring data breaches in smaller firms operating across fewer if any state lines and less able to insulate top managers from liabilities imposed by BNLs; 3) BNLs may be effective in decreasing data breaches in firms when enacted with other state data security laws; and 4) BNLs with certain characteristics other than private rights of action may be effective in decreasing data breaches. We briefly discuss and then investigate evidence related to each possible rebuttal.

***Early BNL Effects***. Much like Romanosky and colleagues (2011) found with identity theft, it may be that early BNL enactments decreased data breach counts and magnitudes, but later BNL enactments were essentially meaningless because conforming firms had already reacted to early enactments, including the initial BNL enactment in California in 2003. While we see no evidence of this trend in our relative time estimations, it may still be observable in regression estimations.

Along these lines, Table 11 replicates our OLS and Poisson estimations using two data sub-samples. The first is 2005-2015 (Columns 1-4), the second is 2005-2010 (Columns 5-8). The intuition behind this sub-sampling strategy is straightforward. By shaving years off the end of the sample we are better able to capture effects from earlier BNL enactments. Results across all columns of Table 11 indicate no significant decrease in data breach counts or magnitudes following BNL enactment. Though not reported here, we also find no pre-treatment trends.[2] This absence of an effect is especially interesting given previous evidence that follow-on incidents of identity theft did decrease temporarily after enactment of BNLs in early-moving states. Taken together, these results suggest that early BNL enactments did not deter firms from data breaches even if they did temporarily deter data misuse by malicious actors after those breaches.

----------Insert Table 11 approximately here----------

***Smaller Firm BNL Effects***: Another possibility is that BNLs have a significant effect on smaller firms operating in only one or a few states rather than larger firms operating nationally. We see at least two justifications for this possibility. One justification links firm size to improved bargaining power with various suppliers, including suppliers of liability insurance. As noted by Baker and Griffith (2007), firm leadership is often slow to address legal miscues in their firms if they are insulated from those miscues by often overly-generous levels of coverage in their Directors & Officers (D&O) insurance policies. Thus, to the extent that leaders at larger firms benefit from higher D&O policy limits, and to the degree that they also enjoy great bargaining power to cajole or coerce coverage in the event of a data breach, then leaders in these larger firms will be less motivated to deter data breaches and related legal liability.

A second justification relates firm size to their geographic scope of operations. Larger firms typically have broader geographic scope. Social media giants like Google or diversified

[2] These results are available upon request from the authors.

manufacturing giants like 3M have customers across all 50 states and most countries abroad. BNL enactment in any state will implicate their customers and data records. By contrast, a smaller firm operating in only a few states may have customers and data records in those states. Until BNLs are enacted there, incentives to reducer data breaches may be insufficient.[3]

Both justifications suggest that smaller firms will be more likely to decrease data breach counts and magnitudes with enactment of BNLs after the initial enactment in California. To investigate this empirically, we create a sub-sample of firms which are not part of the S&P 500, that is, the 500 largest companies listed on public exchanges in the US. We then replicate our OLS and Poisson estimations. Results reported in Table 12 again indicate no significant decrease in data breach counts or magnitudes. Though not reported here, we also find no pre-treatment trends.[4] This evidence suggests smaller firms are no more likely to deter data breaches following BNL enactment than larger firms.

----------Insert Table 12 approximately here----------

***BNL Effects After Enactment of Other State Data Security Laws***: BNLs are only one of four data security laws states have been enacting since 2003. The other three are laws regulating security arrangements for personal data held by firms, the same for state agencies, and laws regulating data disposal by firms and public agencies. By 2019, most states had enacted versions of these other data security laws. Importantly for our study, these other data security laws were often *not* enacted in the same years that BNLs were enacted. In this context, it could be that BNLs alone have little or no data breach deterrence effect until combined with other data

[3] A third and closely-related justification relates to the potential noise in PRC data for larger, publicly-listed firms. Again, PRC data on breach magnitudes sometime attribute all records breached to the firm's state of domicile rather than to each of the states where firm customers are located. Such misattribution is more likely with incidents of massive data breaches at large publicly-listed companies such as the 2017 Equifax breach (Equifax, 2019). Thus, our analyses may skew estimates of BNL enactment effects for states with many large publicly-listed companies such as New York. Analyses limited to smaller firms reduces such noise as smaller firms tend have greater overlap in corporate state domicile and customer location.

[4] These results are available from the authors.

security laws defining standards for data security and disposal. Such a possibility is not unreasonable, notably as it is often challenging to demonstrate negligence absent an explicit set of statutory requirements for data handling.

To investigate such a possibility, we first collect information on enactment dates for the other three data security laws from the National Conference of State Legislatures (NCSL, 2021). We then replicate our OLS and Poisson estimations with three additional $\beta$ terms accounting for: 1) a Firm Data Security Law Enacted; 2) an Agency Data Security Law Enacted; and 3) a Data Disposal Law Enacted. Results in Table 13 suggest that BNLs and these other three data security laws did not significantly decrease data counts and magnitudes. These findings extend our criticism of BNLs to the broader regime of state data security laws. The broader state-based data security legal regime appears to be as toothless as BNLs appear to be.

----------Insert Table 13 approximately here----------

***BNL Effects and Other BNL Characteristics***. Table 1 shows that BNLs like Connecticut's require notification when data are accessed without authorization. Other BNLs like Delaware's require notification when data is acquired by someone lacking authorization. All BNLs require firms to notify individuals when their personal data has been breached, but some BNLs like Hawaii's also require notification of data "owners" that might also have rights to the use of these data. Other BNLs like Idaho's require the same notification to the state attorney general. Still other BNLs like Maryland's require individual, owner, and attorney general notification as well as a PROA for individuals and owners. Our earlier OLS and Poisson regression results did not account for these other differences. We only accounted for BNLs with PROAs.

Our fourth investigation goes beyond PROAs. We assess the impact of BNLs with other coverage dimensions including notification triggers based on unauthorized data access, notification triggers based on unauthorized data acquisition, post-breach individual notification requirements, post-breach owner notification requirements, and post-breach attorney general notification requirements. To do so, we first create five additional $\beta$'s for these different BNL coverage dimensions accounting for: Access Protocol (Columns 1, 6); Acquisition Protocol (Columns 2, 7); Individual Notification (Columns 3, 8); Owner Notification (Columns 4, 9); and AG Notification (Columns 5, 10). Results across all 10 columns of Table 14 again reveal no significant negative effects on data breach counts or magnitudes when BNL enactment is based on any of these different coverage dimensions. Though not reported here, we also find no pre-treatment trends.[5] No matter how we define BNL enactment, they fail to decrease data breaches.

----------Insert Table 14 approximately here----------

## DISCUSSION

### Key Research Questions and Findings

Recall the motivation of this study. 51 different BNLs comprise the main public deterrent to data breaches affecting millions of consumers each year. And these state BNLs comprise the main public repository of information to create a market for data privacy firms can use to signal consumers about data security and vigilance. We asked whether BNLs do either.

Analyses clearly indicated that BNLs have failed in achieving their objective. From 2005-2019, they neither reduced data breach counts nor magnitudes, neither generally nor for specific types of BNLs. BNL enactments from 2005-2019 also failed in the longer-term to reduce follow-on data misuse by malicious actors. Our findings were derived from well-calibrated empirical methods designed to detect causal effects from BNLs. The null BNL effects we instead observed are precisely estimated. Related descriptive trends before and after BNL enactment confirm this.

### Implications for Research, Practice, and Public Policy

***Implications for Research***. Our findings matter for many constituencies starting with researchers studying BNLs. We provide the first evidence based on broad-sample statistical analysis across all states over nearly the entire period of BNL enactment. This constitutes a substantial advance

[5] These results are available from the authors.

on anecdote or single state-based (*e.g*., Park, 2019) evidence. Our findings reinforce skepticism about BNL effectiveness voiced by legal researchers (Joerling, 2010; Peters, 2014) and push back on earlier statistical evidence indicating BNL effectiveness against the malicious use of breached data from information technology and public policy researchers (Romanosky *et al.*, 2011).

***Implications for Practice and Public Policy*.** Our study also matters for various policy-makers writing and enforcing current BNLs, as well as executives and professionals in law, management, and information technology coping with them. The general ineffectiveness of BNLs at curbing data breaches begs the question of why. Cybersecurity consultants and insurers tout multi-million dollar costs and months-long time-lines to identify and contain practically any instance of data breach at US-based firms. In 2021, cybersecurity service providers at IBM set that average data breach incident cost at $9.05 million and average time-line for data breach incident identification and containment at 287 days (IBM, 2021). But details regarding costs and inconveniences mention neither BNLs nor their related triggers, notification requirements, prospective state investigations, penalties, civil suits, or publication mandates.

It could be that BNLs add little to other much stronger business and legal deterrents to data breaches. A notorious hack of credit card files in late 2013 at the Minneapolis-based retailer Target led to data breaches affecting an estimated 70 million customers. Target incurred multi-million dollar liabilities to those credit card customers. But a substantial share of the estimated $248 million to $2.2 billion in business and legal costs Target paid also went to other credit card industry players victimized by the hack: banks and financing companies, payments network providers. BNL provisions made little or no difference for those players (Weiss & Miller, 2015).

That said, there is little doubt that BNL notification requirements lead to more notices to consumers of data breaches sooner than they would otherwise receive. And there is some evidence that consumers have responded with, for example, greater willingness to pay for credit monitoring services to guard against malicious data use after breaches (Peters, 2014). But such measures indicate a shift in the cost of data breaches to consumers rather than internalization by firms to encourage fewer data breaches. Some combination of BNL-prompted cost-shifting and superfluousness may explain the failure of BNLs to prompt more data security vigilance from firm executives and professionals.

What about the policy makers writing and enforcing BNLs? Recall again their aims. BNLs were designed to decrease data breaches and prompt the creation of a market for data privacy where firms could position themselves. We just noted two reasons why BNL deterrents may have been insufficient to prompt a reduction in data breaches. The market motivation for BNLs might still be effective if standards define product quality and cost consistently, and if information permits consumers to understand where firms have positioned themselves regarding those standards. The current set of BNLs undermines development of standards for assessing data security quality and cost at firms. Tom (2010: 1570) describes BNL variation as "so numerous that it is virtually impossible to convert these state laws into the more manageable format..." Even basic standards about notification are inconsistent. For firms doing business with customers in three different states, a given data breach could easily prompt review of three different notification triggers for three different potential recipients manding three different types of notification information.

Even if there were consistent standards, the current set of BNLs undermines the dissemination of actionable information to consumers regarding where firms have positioned themselves regarding data security quality and cost. By mid-2021, only 19 of the 51 BNL regimes published an archive of breach incidents accessible to consumers (IAPP, 2021). Published archives provide little information on any given incident and then with substantial variation across archives. A data breach at Volkswagen America and Audi America (VWA) discovered in March 2021 exposed PII of more than three million customers located throughout the US. Malicious actors allegedly put some of these data up for sale on the dark web. VWA only started filing notifications under various state BNLs in June 2021. Aside from affected actual and potential VWA car owners, millions of consumers in 32 states without any BNL publication archives had little reason to know of the breach incident, let alone understand how to assess VWA's response. Consumers in 19 states with published archives probably fared little better. Searchable archives included no notification information about the VWA incident in Hawaii, Maryland, Montana, Oklahoma, Oregon, Texas, Washington State, and Wisconsin. Archives in California, Delaware, Iowa, Indiana, Maine, Maryland, Massachusetts, New Hampshire, North Dakota, New Jersey, and Vermont do note the VWA incident, but information quantity varies: Indiana's archive comprises a single line item listing the date notification was sent (June 11, 2021), the number of state residents affected (875), and the "total" number individuals affected (90,184); North Dakota's archive provides samples of breach notification forms sent by VWA to affected consumers as well as a cover letter from VWA's lawyers to the state attorney general describing the incident and mitigating actions VWA was taking; New Jersey's archive summarizes breach details in a short paragraph with a hyperlink directing viewers to the *Maine* archive for additional detail. There is no consistency in the presentation of this information. There is little or no guidance given to consumers regarding how to assess the incident and the transgressing firm's actions to mitigate harm.[6]

Obvious public policy responses include a revamp of state BNLs to provide current and consistent standards and information to guide consumers on breach incidents and response effectiveness. They also include replacement with a single federal-level BNL including uniform standards and information to guide consumers and stronger penalties for non-compliance. Along with many other research and public policy commentators (Peters, 2014; Stevens, 2015; Tom, 2010), we prefer the federal response. For standards setting, Congress could authorize the creation

[6] Archived information for these three states is available from the authors.

of an expert body drawn from information technology, legal services, business management, and consumer protection communities to propose, review, and regularly update data security and breach notification standards and best practices. That same body could also recommend sanctions for non-compliance creating substantially stronger deterrents –for example, liability for statutory damages, court costs, and attorneys' fees for consumers harmed by tardy notification.

For information development and dissemination, Congress could create a publication system akin to the US Federal Aviation Administration's Airline Service Quality Performance System assessing on-time departure and arrival of airlines operating in the US (FAA, 2021). A "Data Breach Deterrence and Security Assurance System" could publish and archive standard information on firm data breaches and mitigation efforts. Perhaps more importantly for consumers trying to assess firm performance, the system could also publish and publicize criteria-based, ordinally-graded assessments of firm mitigation. Agency staff might generate those assessments or outside organizations could be enlisted for the same purpose. The SEC designates certain credit rating agencies (*e.g*., Moody's Investor Services) as Nationally Recognized Statistical Rating Organizations assessing the ability and willingness of borrowers to meet their financial obligations (SEC, 2021). Expert outside organizations like the American National Standards Institute might provide similar assessments as Nationally Recognized Data Breach Response Rating Organizations.[7] Solutions of both types have ample precedent and offer certain advantages (Freeman, 2000). They could spur near-term development of a data privacy market state BNLs have apparently failed to develop over nearly 20 years.

## Limitations and Future Research Directions

Like any study, ours has limitations. We emphasize innovations in data and difference-in-

[7] An alternative model to consider is the HIPAA Reporting Tool maintained by the US Department of Homeland Security's Office of Civil Rights (HIPAA, 2021). Also known as the "Wall of Shame," the Reporting Tool website archive is similar to many state BNL website archives we reviewed. While a good start, the Reporting Tool lacks other important information on current data security and data breach response standards. Both strike us as important for the development of a data privacy market.

difference methods permitting causal inference about the (in)effectiveness of BNLs, but those data and methods are not fool-proof. First, as is evident from the legislative history of breach notification laws, they are not assigned at random. This is simply a challenge of secondary macro policy work. And while diagnostics suggest that assumptions of our difference-in-difference analysis are not violated, it still bears note. However, given the absence of significance and expectation of a null result, any confound would statistically point the effect towards zero.

Second, there is the potential for bleeding effects across jurisdictions. BNL enactment in one state may affect firm behavior there and in other states. A firm might react to BNL enactment in its headquarters state by changing behavior in all other states where it operates. This is potentially problematic as it would mean the counterfactual is incorrectly specified. While the fraud and identity theft analysis safeguard against this to some extent, further work will be needed to investigate this possibility. That work might investigate BNL effectiveness on a multi-state basis, taking advantage of the fact that several states enacted BNLs in the same years.

Third, there is always the possibility of measurement error in the dependent variables. As hacking operations become more sophisticated, it is plausible that firms will not know they have been breached, or that consumers will be unaware that their identity has been stolen. These developments should be unrelated to BNL enactments, instead being a general trend captured by time fixed effects. Even so, the prospect merits closer investigation. Future work might account for the changing sophistication of hacking practices with, say, expert assessments of hacking practices across different types of data and industries.

Finally, there is the possibility of firm "migratory" behavior following BNL enactments. Firms could flee emerging BNL regimes as they come into force. While this is theoretically possible, we think it unlikely given substantial costs associated with such moves and, as we suggested earlier, the less substantial (than initially projected) BNL compliance costs. This possibility also prompts greater interest in replicating our results with BNLs and data breaches in state agencies and enterprises with little or no capacity to migrate elsewhere. These and other follow-on areas of research should help us understand more broadly and deeply whether and how BNLs meant to reduce data breaches and create a market for data privacy can achieve that aim to the benefit of firms, consumers, and broader society.

## REFERENCES

Acquisti, A. 2013. What will a future without secrets look like? *TED: Ideas Worth Spreading*. October 17. Available electronically on November 1, 2021 at https://www.ted.com/talks/alessandro_acquisti_what_will_a_future_without_secrets_look_like.

Acquisti, A., Brandimarte, L., & Loewenstein, G. 2020. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4)**:** 736-758.

Acquisti, A. &  Fong, C. 2020. An experiment in hiring discrimination via online social networks. *Management Science*, 66(3)**:** 1005-1024.

Ahammer, A., Halla, M., & Schneeweis, N. 2020. The effect of prenatal maternity leave on short and long-term child outcomes. *Journal of Health Economics,* 70: 102250.

Allison, P. & Waterman, R.P. 2002. Fixed–effects negative binomial regression models. *Sociological Methodology*, 32(1)**:** 247-265.

Anderson, K. 2019. Mass-market consumer fraud in the United States: A 2017 update. US Federal Trade Commission: Washington, DC. Available electronically on November 1, 2021 at https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf.

Angrist, J. & Pischke, J. 2008. *Mostly harmless econometrics: An empiricist's companion*. Princeton University Press: Princeton, NJ.

*Attias*. 2017. *Attias v. Carefirst, inc*., 865 F.3d 620.

Autor, D. 2003. Outsourcing at will: The contribution of unjust dismissal doctrine to the growth of employment outsourcing. *Journal of Labor Economics*, 21(1): 1-42.

Autor, D., Levy, F., & Murnane, R. 2003. The skill content of recent technological change: An empirical exploration. *Quarterly Journal of Economics*, 118(4): 1279-1333.

Ayyagari, R. 2012. An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security*, 8(2)**:** 33-56.

Baker, A., Larcker, D., & Wang, C. 2021. How much should we trust staggered difference-in-differences estimates? *SSRN Working Paper #3794018*.  Available electronically on November 1, 2021 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3794018.

Baker, T. & Griffith, S. 2007. The missing monitor in corporate governance: The directors' & officers' liability insurer. *Georgetown Law Journal*, 95:1795-1842.

Becker, G. 1968. Crime and punishment: An economic approach. *Journal of Political Economy*, 76(2): 169-217.

Burtch, G., Carnahan, S., & Greenwood, B. 2018. Can you gig it? An empirical examination of the gig-economy and entrepreneurial activity. *Management Science*, 64(12): 5497-5520.

Callaway, B. & Sant'Anna, P. 2020. Difference-in-differences with multiple time periods. *Journal of Econometrics*, 225(2): 200-230.

Carnahan, S. 2017. Blocked but not tackled: Who founds new firms when rivals dissolve? *Strategic Management Journal*, 38(11): 2189-2212.

Collins, J. 2019. Check on data breaches at the privacy rights clearinghouse. *Journal of Accountancy*, 228(3) 67. Available electronically on November 1, 2021 at https://www.journalofaccountancy.com/issues/2019/sep/data-breaches-privacy-rights-clearinghouse.html.

Computer World. 2016. Biggest hack of 2016: 412 million friendfinder networks accounts exposed. November 14. Computer World: Needham, MA. Available on November 1, 2021 at https://www.computerworld.com/article/3141290/biggest-hack-of-2016-412-million-friendfinder-network-accounts-exposed.html.

Duflo, E., Glennerster, R., & Kremer, M. 2007. Using randomization in development economics research: A toolkit. *Handbook of Development Economics*, 4: 3895-3962.

Dynes, A. & Holbein, J. 2020. Noisy retrospection: The effect of party control on policy outcomes. *American Political Science Review*, 114(1): 237-257.

Edwards, B., Hofmeyr, S., & Forrest, S. 2016. Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity*, 2(1): 3-14.

*Equifax. 2019. In re Equifax*. 362 F. Supp. 3d 1295.

FAA. 2021. Airline service quality performance system. US Federal Aviation Aministration: Washington, DC. Available electronically on November 1, 2021 at https://aspm.faa.gov/aspmhelp/index/Airline_Service_Quality_Performance_(ASQP).html.

Faulkner, B. 2007. Hacking into data breach notification laws. *Florida Law Review,* 59**:** 1097.

Franco, A., Malhotra, N., & Simonovits, G. 2014. Publication bias in the social sciences: unlocking the file drawer. *Science*, 345(6203): 1502-1505.

Freeman, J. 2000. The private role in the public governance. *NYU L Rev.* 75 543.

*Galaria.* 2016. *Galaria v. Nationwide mutual insurance company,* No. 15-3386.

Goel, S. & Shawky, H. 2014. The impact of federal and state notification laws on security breach announcements. *Communications of the Association for Information Systems*, 34(1): 3.

Goldfarb, B. & King, A. 2015. Scientific apophenia in strategic management research: Significance tests & mistaken inference. *Strategic Management Journal*, 37(1): 167-176.

Goodman-Bacon, A. 2021. Difference-in-differences with variation in treatment timing. *Journal of Econometrics*, 225(2): 254-277.

*Guardian*. 2013. Did your Adobe password leak? Now you and 150m others can check. November 7. *The Guardian*: London, UK. Available on November 1, 2021 at https://www.theguardian.com/technology/2013/nov/07/adobe-password-leak-can-check.

Gupta, A. 2018. The evolution of fraud: Ethical implications in the age of largescale data breaches and widespread artificial intelligence solutions deployment. *International Telecommunication Union Journal*, 1: 0-7.

Hartman, E. & Hidalgo, F. 2018. An equivalence approach to balance and placebo tests. *American Journal of Political Science*, 62(4)**:** 1000-1013.

HIPAA. 2021. Breach reporting tool. US Department of Health and Human Services Office of Civil Rights: Washington, DC. Available electronically on November 1, 2021 at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

*Horizon*. 2017. *In re horizon healthcare services inc. data breach*, 846 F.3d 625.

*Hutton.* 2018. *Hutton v. Nat. bd. of examiners in optometry, Inc*. 2018. 892 F. 3d 613, No. 17-1506.

IAPP. 2021. U.S. state data breach lists (listing states with breach publication websites). International Association of Privacy Professionals: Portsmouth, NH. Available electronically on November 1, 2021 at https://iapp.org/resources/article/u-s-state-data-breach-lists/.

IBM. 2021. Cost of a data breach report 2021. Available on November 1, 2021 at https://www.ibm.com/security/data-breach.

Irshad, S. & Soomro, T. 2018. Identity theft and social media. *International Journal of Computer Science and Network Security*, 18(1): 43-55.

ITech. 2021. Facebook data breach 2021 exposes personal info of 1.5 billion users: 2 tools to check if your data have been leaked. October 7. ITech Post. Tech Times LLC: New York, NY. Available on November 1, 2021 at https://www.itechpost.com/articles/107257/20211007/facebook-data-breach-2021-exposes-personal-info-1-5-billion.htm.

Joerling, J. 2010. Data breach notification laws: An argument for a comprehensive federal law to protect consumer data. *Washington University Journal of Law & Policy,* 32**:** 467-488.

Karyda, M. & Mitrou, L. 2016. Data breach notification: Issues and challenges for security management. MCIS Proceedings. Mediterranean Conference on Information Systems: Paphos, Cyprus. Available electronically on November 1, 2021 at https://aisel.aisnet.org/mcis2016/60/.

Kemp, S., Buil-Gil, G., Mirò-Llinares, F., & Lord, N. 2021. When do businesses report cybercrime? Findings from a UK study. *Ciminology & Criminal Justice,* https://doi.org/10.1177/17488958211062359.

*Katz*. 2012. *Katz v. Pershing, LLC,* 672 F.3d 64.

*Krottner.* 2010. *Krottner v. Starbucks Corp*, 628 F. 3d 1139, No. 09-35823.

Laube, S. & Böhme, R. 2016. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*. 2(1) 29-41.

*Lewert*. 2016. *Lewert v. PF Chang's China bistro, Inc.*, 819 F.3d 963.

McNamara, G., Vaaler, P., & Devers, C. 2003. Same as it ever was: The search for evidence of increasing hypercompetition. *Strategic Management Journal*, 24(3): 261-278.

Mintz.com. 2021. The U.S. supreme court raises the bar on standing in privacy and data breach class actions. Mintz - Privacy and Cybersecurity Viewpoints. June 25. Mintz, Levin, Cohn, Ferris, Glovsky, and Popeo Law Firm. Boston, MA. Available electronically on November 1, 2021 at https://www.jdsupra.com/legalnews/the-u-s-supreme-court-raises-the-bar-on-8964854/.

Needles, S. 2009. The data game: Learning to love the state-based approach to data breach notification law. *North Carolina Law Review,* 88**:** 267-310.

NCSL. 2021. Security breach notification laws. National conference of state legislatures: Washington, DC. Available electronically on November 1, 2021 at https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx#1.

Park, S. 2019. Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics*, 58: 132-145.

Peters, R. 2014. So you've been notified, now what: The problem with current data-breach notification laws. *Arizona Law Review*, 56(4): 1171-1202.

Picanso, K. 2006. Protecting information security under a uniform data breach notification law. *Fordham Law Review* 75(1): 355-390.

PRC. 2021. Privacy rights clearinghouse. San Diego, CA. Available electronically on November 1, 2021 at: https://privacyrights.org/.

Raval, D. 2020. Which communities complain to policymakers? Evidence from consumer sentinel. *Economic Inquiry*, 58(4)**:** 1628-1642.

*Ramirez*. 2021. *Transunion LLC v. Ramirez,* 594 U.S. ___ (2021), 141 S.Ct. 2190 (2021).

*Resnick.* 2012. *Resnick v. Avmed, Inc,* 693 F. 3d 1317.

Rode, L. 2006. Database security breach notification statutes: Does placing the responsibility on the true victim increase data security. *Houston Law Review*, 43(5): 1597-1634.

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

*Rudolph*. 2019. *Rudolph v. Hudsons Bay Co*., No. 18 cv 8472.

SEC. 2018. Commission statement and guidance on public company cybersecurity disclosures. Release Nos. 33-10459; 34-82746. February 26. US Securities and Exchange Commission: Washington, DC.

SEC. 2020. Cybersecurity and resiliency observations. Guidance from the office of compliance inspections and enforcement. US Securties and Exchange Commission: Washington, DC.

SEC. 2021. Office of credit ratings. US Securities and Exchange Commission: Washington, DC. Available electronically on November 1, 2021 at https://www.sec.gov/page/ocr-section-landing.

Silva, J., & Tenreyro, S. 2006. The log of gravity. *The Review of Economics and Statistics*. 88(4) 641-658.

Silva, J., & Tenreyro, S. 2011. Further simulation evidence on the performance of the poisson pseudo-maximum likelihood estimator. *Economics Letters*, 112(2)**:** 220-222.

Solove, D. & Schwartz, P. 2019. *Privacy law fundamentals*. International Association of Privacy Professionals: Portsmouth, NH.

Steel, C. 2019. Stolen identity valuation and market evolution on the dark web. *International Journal of Cyber Criminology*, 13(1)**:** 70-83.

Stevens, G.. 2012. *Data security breach notification laws*. Congressional Research Service Washington, DC.

Tom, J.. 2010. A Simple compromise: The need for a federal data breach notification law. *St. John's University Law Review*, 84(4): 1569-1603.

Walker, E. & Nowacki, A. 2011. Understanding equivalence and noninferiority testing. *Journal of General Internal Medicine*, 26(2)**:** 192-196.

Weiss, N. & Miller, R. 2015. The Target and other financial data breaches: Frequently asked questions. Congressional Research Service: Washington, DC.

Winn, J. 2009. Are better security breach notification laws possible. *Berkeley Technology Law Journal,* 24**:** 1133.

Wolf, J. 2018. Why it's so hard to punish companies for data breaches. October 16. *New York Times*.

*Wyndham.* 2015. *FTC v. Wyndham worldwide corp*, 799 F. 3d 236, No. 14-3514.

Zamoff, M., Greenwood, B., & Burtch, G. 2022. Who watches the watchmen: Evidence of the effect of body-worn cameras on New York City policing. J*ournal of Law, Economics, & Organization*, 38(1): 161-195.

## Table 1: Summary Information on State BNLs

| State | Citation | Year | Trigger for Notification | No Harm Exception | Individual Notification | Owner Notification | AG Notification | Private Right of Action |
|---|---|---|---|---|---|---|---|---|
| Alabama | Ala. Code § 8-38-1 et seq. | 2018 | Acquisition | No Harm | yes | yes | yes | |
| Alaska | Alaska Stat. § 45.48.010 et seq. | 2009 | Acquisition | No Harm | yes | yes | yes | yes |
| Arizona | Ariz. Rev. Stat. § 18-551 to -552 | 2006 | Risk of Misuse | No Harm | yes | yes | | |
| Arkansas | Ark. Code §§ 4-110-101 et seq. | 2005 | Acquisition | No Harm | yes | yes | | |
| California | Cal. Civ. Code §§ 1798.29, 1798.82 | 2003 | Acquisition | | yes | yes | yes | yes |
| Colorado | Colo. Rev. Stat. § 6-1-716 | 2006 | Acquisition | No Harm | yes | yes | | |
| Connecticut | Conn. Gen Stat. §§ 36a-701b, 4e-70 | 2012 | Access | No Harm | yes | yes | yes | |
| Delaware | Del. Code tit. 6, § 12B-101 et seq. | 2005 | Acquisition | No Harm | yes | yes | | |
| DC | D.C. Code §§ 28- 3851 et seq., 2020 B 215 | 2007 | Acquisition | | yes | yes | | yes |
| Florida | Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i) | 2014 | Access | No Harm | yes | | yes | |
| Georgia | Ga. Code §§ 10-1-910 to -912; 46-5-214 | 2005 | Acquisition | | yes | | | |
| Hawaii | Haw. Rev. Stat. § 487N-1 et seq. | 2007 | Misuse or Risk of Misuse | No Harm | yes | yes | | yes |
| Idaho | Idaho Stat. §§ 28-51-104 to -107 | 2006 | Misuse or Risk of Misuse | No Harm | yes | yes | yes | |
| Illinois | 815 ILCS §§ 530/1 to 530/25, 815 ILCS 530/55 (2020 S.B. 1624) | 2006 | Acquisition | | yes | yes | yes | yes |
| Indiana | Ind. Code §§ 4-1-11 et seq., 24-4.9 et seq. | 2006 | Acquisition | | | | | |
| Iowa | Iowa Code §§ 715C.1, 715C.2 | 2008 | Acquisition | No Harm | yes | yes | yes | |
| Kansas | Kan. Stat. § 50-7a01 et seq. | 2007 | Access | | yes | yes | | |
| Kentucky | KRS § 365.732, KRS §§ 61.931 to 61.934 | 2014 | Acquisition | | yes | yes | | |
| Louisiana | La. Rev. Stat. §§ 51:3071 et seq. | 2006 | Access | No Harm | yes | yes | yes | yes |
| Maine | Me. Rev. Stat. tit. 10 § 1346 et seq. | 2006 | Misuse or Risk of Misuse | No Harm | yes | yes | yes | |
| Maryland | Md. Code Com. Law §§ 14-3501 et seq., Md. State Govt. Code §§ 10-1301 to -1308 | 2008 | Acquisition | No Harm | yes | yes | yes | yes |
| Massachusetts | Mass. Gen. Laws § 93H-1 et seq. | 2007 | Acquisition | | yes | yes | yes | |
| Michigan | Mich. Comp. Laws §§ 445.63, 445.72 | 2007 | Access | No Harm | yes | | | |
| Minnesota | Minn. Stat. §§ 325E.61, 325E.64 | 2005 | Acquisition | | yes | yes | | yes |
| Mississippi | Miss. Code § 75-24-29 | 2011 | Acquisition | No Harm | yes | yes | | |
| Missouri | Mo. Rev. Stat. § 407.1500 | 2009 | Access | No Harm | yes | yes | yes | |
| Montana | Mont. Code §§ 2-6-1501 to -1503, 30-14-1704, 33-19-321 | 2006 | Acquisition | | yes | yes | yes | |
| Nebraska | Neb. Rev. Stat. §§ 87-801 et seq. | 2006 | Acquisition | No Harm | yes | yes | yes | |
| Nevada | Nev. Rev. Stat. §§ 603A.010 et seq., 242.183 | 2005 | Acquisition | | yes | yes | | yes |
| New Hampshire | N.H. Rev. Stat. §§ 359-C:19, 359-C:20, 359-C:21 | 2007 | Acquisition | No Harm | yes | yes | yes | yes |
| New Jersey | N.J. Stat. § 56:8-161, 163 | 2005 | Access | | yes | yes | | |
| New Mexico | N.M. Stat. §§ 57-12C-1 | 2017 | Acquisition | No Harm | yes | yes | yes | |
| New York | N.Y. Gen. Bus. Law § 899-AA | 2005 | Acquisition | | yes | yes | yes | |
| North Carolina | N.C. Gen. Stat §§ 75-61, 75-65, 14-113.20 | 2005 | Access | No Harm | yes | yes | yes | yes |
| North Dakota | N.D. Cent. Code §§ 51-30-01 et seq. | 2005 | Acquisition | | yes | yes | yes | |
| Ohio | Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192 | 2006 | Access | No Harm | yes | yes | | |
| Oklahoma | Okla. Stat. §§ 74-3113.1, 24-161 to -166 | 2008 | Access | | yes | yes | | |
| Oregon | Oregon Rev. Stat. §§ 646A.600 to .628 | 2007 | Acquisition | No Harm | yes | yes | yes | yes |
| Pennsylvania | 73 Pa. Stat. §§ 2301 et seq. | 2006 | Access | No Harm | yes | yes | | |
| Rhode Island | R.I. Gen. Laws §§ 11-49.3-1 et seq. | 2006 | Acquisition | No Harm | yes | yes | yes | yes |
| South Carolina | S.C. Code § 39-1-90 | 2009 | Acquisition | No Harm | yes | yes | | yes |
| South Dakota | S.D. Cod. Laws §§ 20-40-19 to -26 | 2018 | Acquisition | No Harm | yes | | yes | |
| Tennessee | Tenn. Code §§ 47-18-2107; 8-4-119 | 2005 | Acquisition | | yes | yes | | yes |
| Texas | Tex. Bus. & Com. Code §§ 521.002, 521.053 | 2009 | Acquisition | | yes | yes | | |
| Utah | Utah Code §§ 13-44-101 et seq. | 2007 | Acquisition | | yes | yes | | |
| Vermont | Vt. Stat. tit. 9 §§ 2430, 2435 | 2012 | Acquisition | | yes | yes | yes | |
| Virginia | Va. Code §§ 18.2-186.6, 32.1-127.1:05 | 2008 | Access | | yes | yes | yes | yes |
| Washington | Wash. Rev. Code §§ 19.255.010, 42.56.590 | 2005 | Acquisition | No Harm | yes | yes | yes | |
| West Virginia | W.V. Code §§ 46A-2A-101 et seq. | 2008 | Access | | yes | yes | | |
| Wisconsin | Wis. Stat. § 134.98 | 2006 | Acquisition | No Harm | yes | yes | | |
| Wyoming | Wyo. Stat. § 6-3-901(b), §§ 40-12-501 to -502 | 2007 | Access | No Harm | yes | yes | | |

Data on individual statutes is originally sourced from Solove and Schwartz (2019) and supplemented with information from the National Conference of State Legislatures: https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

## Table 2: US Circuit Court of Appeals Decisions Establishing Standing and Injury in Fact Related to Data Breaches

| Decision | Year | Summary | Circuit |
|---|---|---|---|
| ***Attias*** *v. Carefirst, Inc.,* 865 F.3d 620 (D.C. Cir. 2017). | 2017 | Plaintiff consumers have standing under Article III if sensitive information was stolen during a data breach. This is especially true if the stolen data "plausibly" include Social Security numbers (SSNs) and CC numbers (CCNs). | DC Circuit |
| ***Katz*** *v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012). | 2012 | Contrary holding to other circuits. Plaintiffs do ***not*** have standing if they cannot identify actual harm (injury) rather than the mere threat of harm in the future. | 1st Circuit |
| ***Rudolph*** v. Hudsons Bay Co., No. 18 cv 8472 (PKC) (S.D.N.Y. 2019). | 2019 | Overturns *Whalen v Michaels Stores*. Plaintiff identified and particularized loss as a result of time spent dealing with the breach and getting a new CC. This constituted an injury with Article III standing. | 2nd Circuit |
| *In Re* **Horizon** *Healthcare Services Inc. Data Breach*, 846 F.3d 625 (3d Cir. 2017). | 2017 | Laptop stolen from healthcare insurer leads to plaintiff claims under Fair Credit Reporting Act (FCRA). Unlawful disclosure creates a de facto injury under FCRA conferring Article III standing. | 3rd Circuit |
| ***Hutton*** *v. Nat. Bd. of Examiners in Optometry, Inc*, 892 F.3d 613 (4th Cir. 2018). | 2018 | Database hack led to ID theft and fraudulent CC charges harming plaintiffs. Out-of-pocket costs resulting from and time lost responding to breach constitute injury with Article III standing. | 4th Circuit |
| ***Galaria*** *v. Nationwide Mutual Insurance Company*, No. 15-3386 (6th Cir. Sept. 12, 2016). | 2016 | Hackers breached a computer network and stole plaintiff's data, leading to expenses for plaintiff associated with dealing with the fallout of this hack. This constitutes an injury with Article III standing. | 6th Circuit |
| ***Lewert*** *v. PF Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016). | 2016 | Data breach at a Chinese restaurant. CCNs and other data were stolen. Increased risk of fraudulent charges and ID theft constitutes an injury to plaintiff with Article III standing. | 7th Circuit |
| **Krottner** v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010). | 2010 | Theft of a laptop with personal data about plaintiffs caused anxiety and threat of future harm. This constitutes an injury with Article III standing. | 9th Circuit |
| ***Resnick*** *v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012). | 2012 | Theft of a laptop resulted in identity theft and fraud causing financial loss to plaintiff. This constitutes an injury with Article III standing. | 11th Circuit |

Initial Source: Solove and Schwartz (2019) and subsequently updated. Cases referenced in bibliography based on party in **bold** type and year of decision.

## Table 3: Effect of BNLs on Data Breach Counts and Magnitudes

| | (1) | (2) | (3) | (4) |
|---|---|---|---|---|
| Dependent Variable | ln(Records) | ln(Records) | numEvents | numEvents |
| Estimator | Log-OLS | Log-OLS | Poisson | Poisson |
| Treatment | Any BNL | BNL w/ Private Right of Action (PROA) | Any BNL | BNL w/ PROA |
| Any BNL Enacted | 0.258 | | -0.0349 | |
| | (0.700) | | (0.117) | |
| BNL w/ PROA Enacted | | 1.035 | | 0.136 |
| | | (0.963) | | (0.349) |
| State Fixed Effects | Yes | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes | Yes |
| Observations | 765 | 765 | 765 | 765 |
| R-squared | 0.543 | 0.544 | | |
| Number of Groups | 51 | 51 | 51 | 51 |

Robust standard errors clustered on states in parentheses

*** p<0.01, ** p<0.05, * p<0.1

## Table 4: Effect of BNLs on Data Breach Counts and Magnitudes in Relative Time

| | (1) | (2) | (3) | (4) |
|---|---|---|---|---|
| Dependent Variable | ln(Records) | numEvents | ln(Records) | numEvents |
| Estimator | Log-OLS | Poisson | Log-OLS | Poisson |
| Treatment | Privacy Law | Privacy Law | PROA | PROA |
| Rel Time t-4+ | -0.746 | -0.168 | | |
| | (0.917) | (0.225) | | |
| Rel Time t-4 | -1.376 | -0.0908 | -5.878*** | |
| | (1.320) | (0.188) | (1.654) | |
| Rel Time t-3 | -0.184 | -0.231 | -1.219 | -0.865 |
| | (1.234) | (0.162) | (2.881) | (0.448) |
| Rel Time t-2 | -0.899 | 0.00651 | -0.711 | -0.344 |
| | (0.735) | (0.102) | (1.327) | (0.248) |
| | Omitted Periods To Avoid Dummy Variable Trap | | | |
| Rel Time t+1 | 0.189 | 0.128 | -0.496 | -0.106 |
| | (0.619) | (0.136) | (1.173) | (0.207) |
| Rel Time t+2 | 0.115 | 0.0115 | 0.764 | -0.101 |
| | (0.745) | (0.138) | (0.953) | (0.167) |
| Rel Time t+3 | -0.384 | -0.103 | -0.510 | -0.198 |
| | (0.731) | (0.143) | (0.794) | (0.180) |
| Rel Time t+4 | 0.115 | -0.0226 | -0.924 | -0.0836 |
| | (0.873) | (0.168) | (1.311) | (0.209) |
| Rel Time t+5 | -0.919 | -0.0340 | -0.677 | -0.105 |
| | (0.821) | (0.218) | (0.871) | (0.217) |
| Rel Time t+6 | -0.0283 | 0.190 | -0.763 | 0.405 |
| | (1.000) | (0.356) | (1.151) | (0.529) |
| Rel Time t+7 | -0.185 | 0.0242 | 0.264 | 0.00136 |
| | (1.105) | (0.224) | (1.235) | (0.216) |
| Rel Time t+8 | -0.426 | -0.0644 | -1.264 | -0.0851 |
| | (1.244) | (0.255) | (1.215) | (0.170) |
| Rel Time t+9 | 1.467 | -0.0947 | 0.815 | -0.0503 |
| | (1.283) | (0.278) | (1.334) | (0.148) |
| Rel Time t+10 | 0.387 | 0.117 | 0.195 | 0.174 |
| | (1.373) | (0.292) | (1.466) | (0.256) |
| Rel Time t+10 + | -0.258 | 0.201 | -1.318 | 0.244 |
| | (1.539) | (0.322) | (1.001) | (0.265) |
| State Fixed Effects | Yes | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes | Yes |
| Observations | 765 | 765 | 765 | 763 |
| R-squared | 0.553 | | 0.552 | |

Robust standard errors clustered on states in parentheses

*** p<0.01, ** p<0.05, * p<0.1

## Table 5: Effect of BNLs on Data Breach Counts and Magnitudes Partitioned by Internal and External Causes

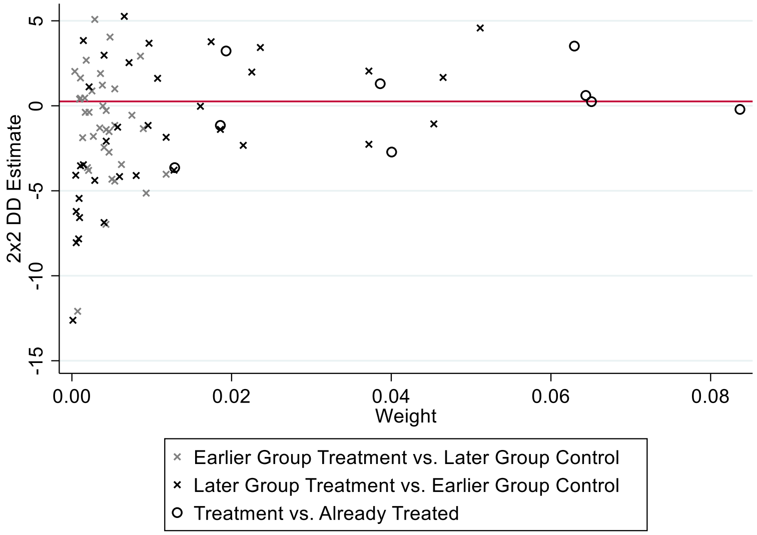
| | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) |
|---|---|---|---|---|---|---|---|---|
| Dependent Variable | ln(Records) | ln(Records) | numEvents | numEvents | ln(Records) | ln(Records) | numEvents | numEvents |
| Sample | Externally-Caused Data Breaches (*e.g.*, Hack) | | | | Internally-Caused Data Breaches (*e.g.*, Employee Error) | | | |
| Estimator | Log-OLS | Log-OLS | Poisson | Poisson | Log-OLS | Log-OLS | Poisson | Poisson |
| Treatment | Any BNL | BNL w/ PROA | Any BNL | BNL w/ PROA | Any BNL | BNL w/ PROA | Any BNL | PBNL w/ PROA |
| Any BNL Enacted | 0.135 | | -0.0188 | | 1.000 | | 0.0957 | |
| | (0.790) | | (0.153) | | (0.573) | | (0.151) | |
| BNL w/ PROA Enacted | | 0.709 | | 0.292 | | 1.596 | | 0.229 |
| | | (1.134) | | (0.516) | | (1.057) | | (0.608) |
| State Fixed Effects | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Observations | 765 | 765 | 765 | 765 | 765 | 765 | 765 | 765 |
| R-squared | 0.457 | 0.458 | | | 0.491 | 0.492 | | |
| Number of Groups | 51 | 51 | 51 | 51 | 51 | 51 | 51 | 51 |

Robust standard errors clustered on states in parentheses
*** p<0.01, ** p<0.05, * p<0.1

## Table 6: Results from Goodman-Bacon (2018) Decomposition Analysis

| Base Analysis | Weight | DD Avg |
|---|---|---|
| Earlier T vs. Later C | 0.144 | -1.394 |
| Later T vs. Earlier C | 0.451 | 0.587 |
| T vs. Already treated | 0.406 | 0.478 |
| T = Treatment; C = Control | | |
| PCOA Analysis | Weight | DD Avg |

## Figure 1A: Graphical Representation of the Goodman-Bacon (2018) Decomposition Estimation (Any BNL Enacted)



## Figure 1B: Graphical Representation of the Goodman-Bacon (2018) Decomposition Estimation (BNL w/ PROA Enacted)

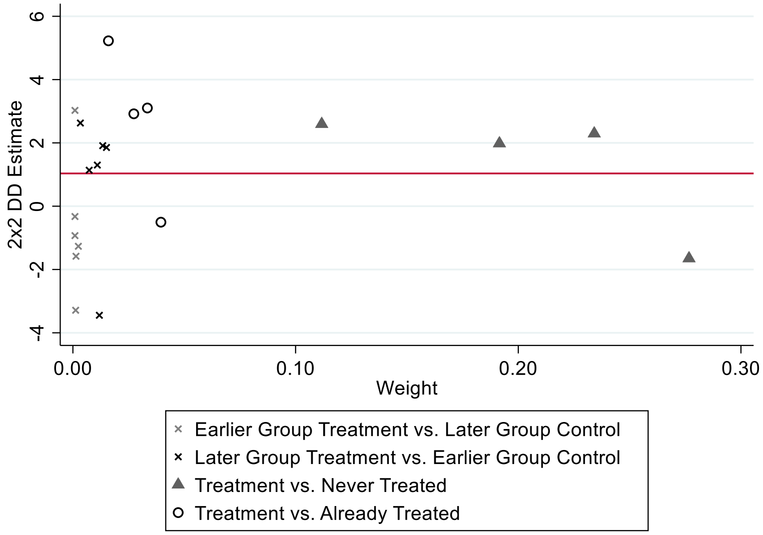


**Figure 2A: Graphical Representation of Callaway and Sant'Anna (2020) DID Estimation (Any BNL Enacted)**

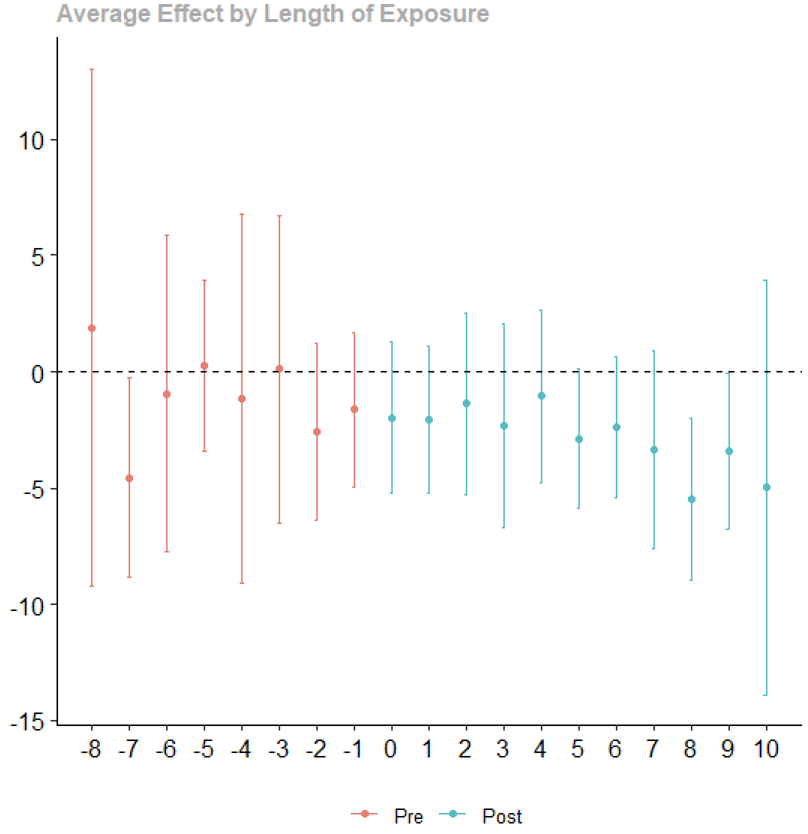
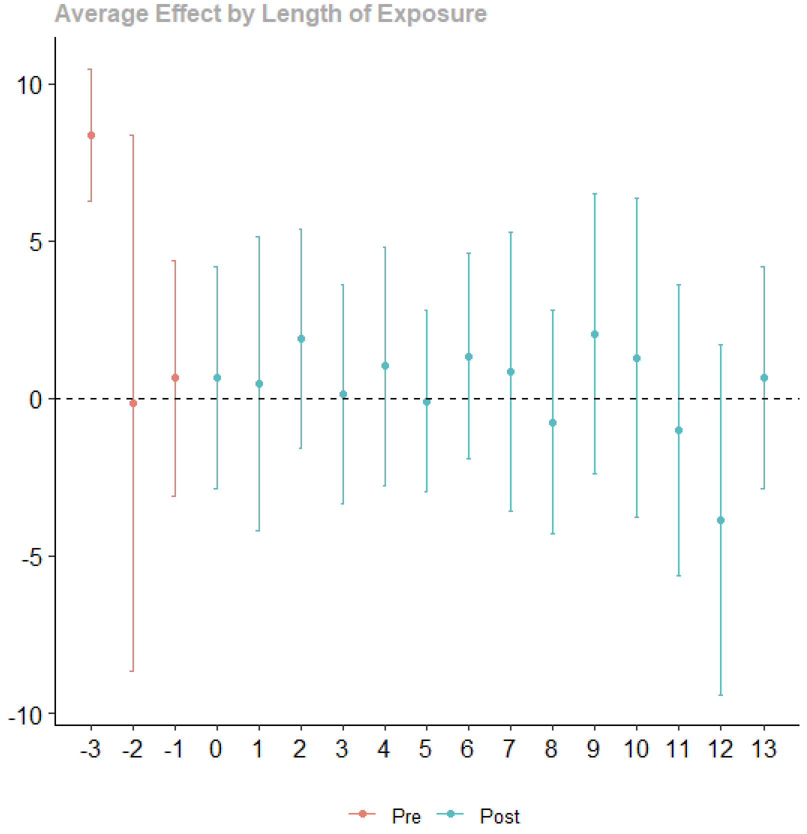


**Figure 2B: Graphical Representation of Callaway and Sant'Anna (2020) DID Estimation (BNL w/ PROA Enacted)**



## Table 7: Equivalency Test

| | (1) | (2) | (3) | (4) |
|---|---|---|---|---|
| Dependent Variable | ln(Records) | numEvents | ln(Records) | numEvents |
| Estimator | Log-OLS | Poisson | Log-OLS | Poisson |
| Treatment | Any BNL | Any BNL | BNL w/ PROA | BNL w/ PROA |
| Estimated Effect | 0.2580 | -0.0349 | 1.035 | 0.136 |
| Randomly Generated Effect | 0.0012 | 0.0050 | 0.0106 | -0.0020 |
| Standard Deviation | 0.3189 | 0.0731 | 0.2789 | 0.0654 |
| Pr(T > t1) - Superior | 0.0000 | 0.0000 | 0.0000 | 0.0000 |
| Pr(T > t2) - Inferior | 0.0000 | 0.0000 | 0.9974 | 0.0000 |

## Table 8: Replication of Romanosky et al. (2011) Restricting FTC Data to 2005-2010

| | (1) |
|---|---|
| Dependent Variable | ln(ID Theft) |
| Estimator | Log-OLS |
| Sample | 2005 - 2010 |
| Treatment | Any BNL |
| Any BNL Enacted | -0.0514* |
| | (0.0211) |
| State Fixed Effects | Yes |
| Year Fixed Effects | Yes |
| Observations | 306 |
| R-squared | 0.997 |
| Number of Groups | 51 |

Robust standard errors clustered on states in parentheses
*** p<0.01, ** p<0.05, * p<0.1

## Table 9: Effect of BNLs on Identity Theft and Fraud Counts and Magnitudes

| | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) |
|---|---|---|---|---|---|---|---|---|
| Dependent Variable | ln(ID Theft) | ln(Fraud) | numTheft | numFraud | ln(ID Theft) | ln(Fraud) | numTheft | numFraud |
| Estimator | Log-OLS | Log-OLS | Poisson | Poisson | Log-OLS | Log-OLS | Poisson | Poisson |
| Treatment | Any BNL | Any BNL | Any BNL | Any BNL | BNL w/ PROA | BNL w/ PROA | BNL w/ PROA | BNL w/ PROA |
| Any BNL Enacted | -0.0289 | -0.0111 | -0.0539 | 0.174* | | | | |
| | (0.0274) | (0.0572) | (0.0654) | (0.0745) | | | | |
| BNL w/ PROA Enacted | | | | | -0.0316 | -0.124 | 0.0206 | -0.129 |
| | | | | | (0.0514) | (0.121) | (0.0730) | (0.0834) |
| State Fixed Effects | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Observations | 765 | 765 | 765 | 765 | 765 | 765 | 765 | 765 |
| R-squared | 0.986 | 0.975 | | | 0.986 | 0.975 | | |
| Number of Groups | 51 | 51 | 51 | 51 | 51 | 51 | 51 | 51 |

Robust standard errors clustered on states in parentheses
*** p<0.01, ** p<0.05, * p<0.1

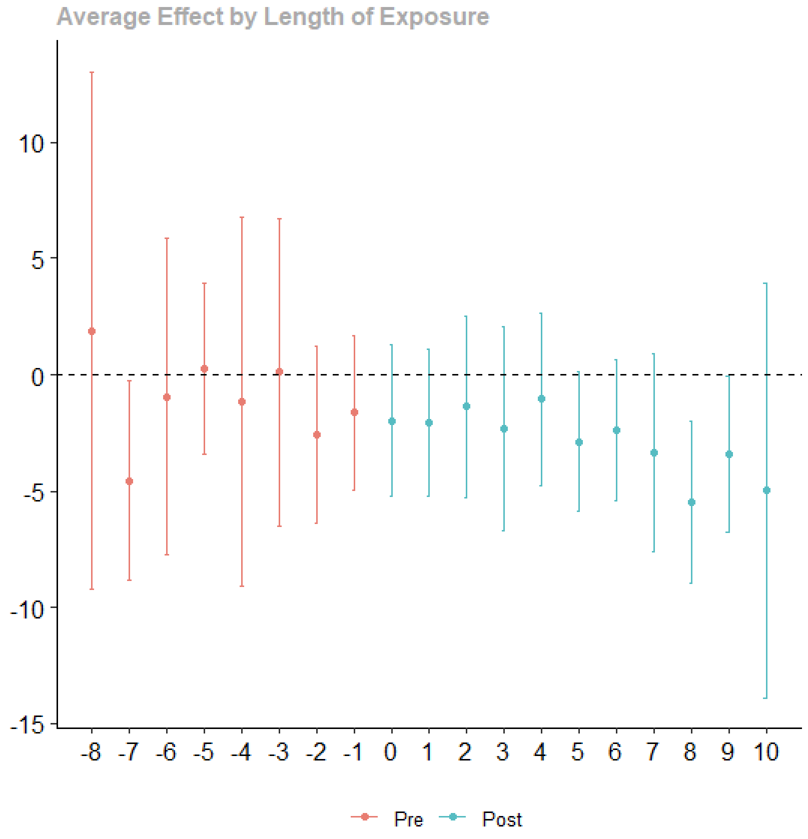
# Table 10: Effect of BNLs on Identity Theft and Fraud Counts and Magnitudes in Relative Time

|  | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) |
|---|---|---|---|---|---|---|---|---|
| Dependent Variable | ln(ID Theft) | ln(Fraud) | numTheft | numFraud | ln(ID Theft) | ln(Fraud) | numTheft | numFraud |
| Estimator | Log-OLS | Log-OLS | Poisson | Poisson | Log-OLS | Log-OLS | Poisson | Poisson |
| Treatment | Any BNL | Any BNL | Any BNL | Any BNL | BNL w/ PROA | BNL w/ PROA | BNL w/ PROA | BNL w/ PROA |
| Rel Time t-4+ | -0.0185 | -0.136 | -0.124 | -0.253* |  |  |  |  |
|  | (0.0741) | (0.146) | (0.195) | (0.121) |  |  |  |  |
| Rel Time t-4 | -0.0255 | -0.0209 | -0.0293 | -0.162** | -0.0119 | 0.356* | -0.273** | 0.217* |
|  | (0.0556) | (0.0768) | (0.126) | (0.0541) | (0.163) | (0.161) | (0.0887) | (0.101) |
| Rel Time t-3 | 0.00166 | -0.0468 | 0.0691 | -0.144 | -0.0240 | -0.0167 | -0.112 | -0.00922 |
|  | (0.0385) | (0.0552) | (0.0626) | (0.0755) | (0.0668) | (0.0588) | (0.0666) | (0.0374) |
| Rel Time t-2 | 0.0246 | 0.0493 | 0.214 | 0.0220 | 0.0433 | 0.140 | -0.0372 | 0.0939 |
|  | (0.0395) | (0.0460) | (0.114) | (0.0493) | (0.0472) | (0.0955) | (0.0566) | (0.0635) |
|  |  |  |  | Omitted Periods To Avoid Dummy Variable Trap |  |  |  |  |
| Rel Time t+1 | -0.0302 | -0.0127 | -0.0938* | 0.0589 | -0.00118 | -0.0339 | 0.00106 | -0.000534 |
|  | (0.0214) | (0.0343) | (0.0467) | (0.0504) | (0.0164) | (0.0554) | (0.0169) | (0.0280) |
| Rel Time t+2 | -0.0374 | -0.0247 | -0.134* | 0.0140 | 0.00745 | -0.0189 | 0.0284 | -0.00978 |
|  | (0.0238) | (0.0479) | (0.0666) | (0.0401) | (0.0288) | (0.0745) | (0.0271) | (0.0393) |
| Rel Time t+3 | -0.0354 | -0.0712 | -0.179* | -0.0561 | 0.00181 | -0.0642 | 0.00298 | -0.0188 |
|  | (0.0392) | (0.0542) | (0.0853) | (0.0844) | (0.0346) | (0.104) | (0.0404) | (0.0424) |
| Rel Time t+4 | -0.0688 | -0.0979 | -0.239* | -0.0807 | -0.0128 | -0.0844 | -0.0659 | -0.0783 |
|  | (0.0461) | (0.0528) | (0.100) | (0.0701) | (0.0357) | (0.0901) | (0.0625) | (0.0529) |
| Rel Time t+5 | -0.0703 | -0.0701 | -0.220* | -0.0826 | -0.0294 | -0.0179 | -0.0690 | -0.0648 |
|  | (0.0575) | (0.0781) | (0.112) | (0.0926) | (0.0475) | (0.179) | (0.0751) | (0.0643) |
| Rel Time t+6 | -0.0760 | -0.144 | -0.222 | -0.0975 | -0.0459 | -0.0923 | -0.138 | -0.163* |
|  | (0.0705) | (0.0717) | (0.145) | (0.108) | (0.0458) | (0.107) | (0.107) | (0.0676) |
| Rel Time t+7 | -0.0762 | -0.110 | -0.276 | -0.109 | -0.00611 | -0.0837 | -0.124 | -0.188 |
|  | (0.0779) | (0.0820) | (0.160) | (0.115) | (0.0556) | (0.120) | (0.161) | (0.115) |
| Rel Time t+8 | -0.0781 | -0.131 | -0.259 | -0.172 | -0.0187 | -0.0506 | -0.0591 | -0.149 |
|  | (0.0934) | (0.0856) | (0.184) | (0.110) | (0.0541) | (0.107) | (0.106) | (0.104) |
| Rel Time t+9 | -0.0581 | -0.126 | -0.257 | -0.194 | -0.0156 | -0.0533 | -0.0895 | -0.137 |
|  | (0.115) | (0.0968) | (0.231) | (0.126) | (0.0602) | (0.123) | (0.120) | (0.112) |
| Rel Time t+10 | -0.0967 | -0.136 | -0.331 | -0.240 | -0.0268 | -0.0286 | -0.137 | -0.152 |
|  | (0.130) | (0.104) | (0.276) | (0.155) | (0.0772) | (0.101) | (0.135) | (0.122) |
| Rel Time t+10 + | -0.0810 | -0.131 | -0.405 | -0.224 | 0.0757 | -0.0483 | -0.00146 | -0.138 |
|  | (0.136) | (0.116) | (0.270) | (0.150) | (0.0511) | (0.0950) | (0.0783) | (0.0902) |
| State Fixed Effects | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Observations | 765 | 765 | 765 | 765 | 765 | 765 | 765 | 765 |
| R-squared | 0.986 | 0.976 |  |  | 0.986 | 0.976 |  |  |

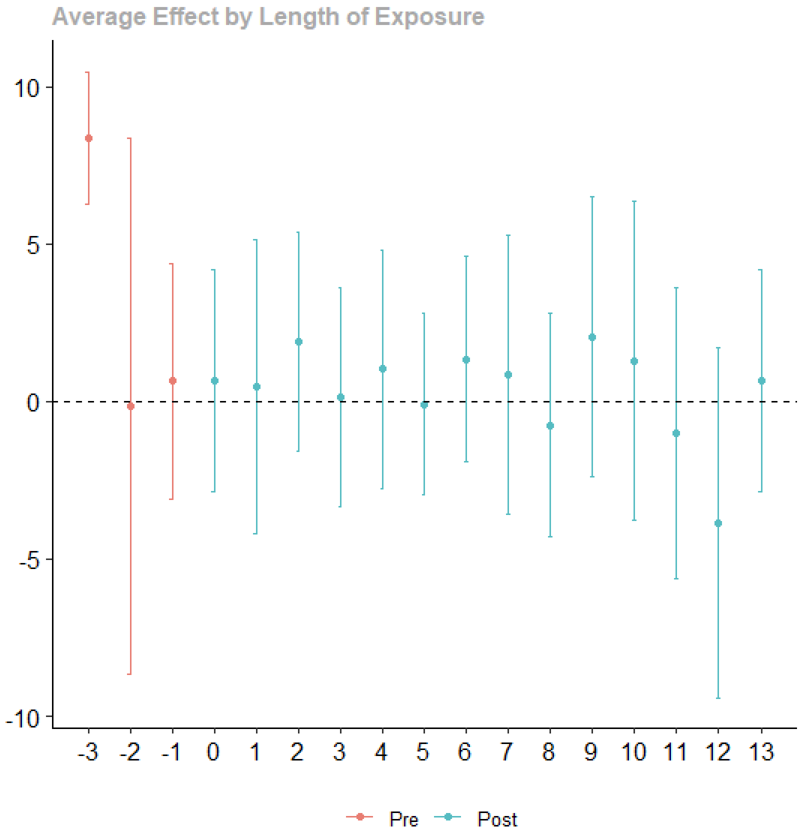
Robust standard errors clustered on states in parentheses

*** p<0.01, ** p<0.05, * p<0.1

## Figure 3A: Graphical Output of Callaway and Sant'Anna (2020) DID Estimation (Base Estimation)



## Figure 3B: Graphical Output of Callaway and Sant'Anna (2020) DID Estimation (PROA Estimation)



## Table 11 – Effect of BNLs on Data Breach Counts and Magnitudes Based on Alternative Time Periods

| | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) |
|---|---|---|---|---|---|---|---|---|
| Dependent Variable | ln(Records) | ln(Records) | numEvents | numEvents | ln(Records) | ln(Records) | numEvents | numEvents |
| Sample | 2005-2015 | 2005-2015 | 2005-2015 | 2005-2015 | 2005-2010 | 2005-2010 | 2005-2010 | 2005- 2010 |
| Estimator | Log-OLS | Log-OLS | Poisson | Poisson | Log-OLS | Log-OLS | Poisson | Poisson |
| Treatment | Any BNL | BNL w/ PROA | Any BNL | BNL w/ PROA | Any BNL | BNL w/ PROA | Any BNL | BNL w/ PROA |
| Any BNL Enacted | 0.283 | | -0.0106 | | 0.389 | | 0.0929 | |
| | (0.683) | | (0.128) | | (0.804) | | (0.127) | |
| BNL w/ PROA Enacted | | 1.262 | | 0.248 | | 1.008 | | -0.0305 |
| | | (0.965) | | (0.374) | | (0.984) | | (0.219) |
| State Fixed Effects | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Observations | 561 | 561 | 561 | 561 | 306 | 306 | 306 | 306 |
| R-squared | 0.535 | 0.537 | | | 0.593 | 0.594 | | |

Robust standard errors clustered on states in parentheses

*** p<0.01, ** p<0.05, * p<0.1

## Table 12 – Effect of BNLs on Data Breach Counts and Magnitudes For Non-S&P 500 Firms

| | (1) | (2) | (3) | (4) |
|---|---|---|---|---|
| Dependent Variable | ln(Records) | ln(Records) | numEvents | numEvents |
| Estimator | Log-OLS | Log-OLS | Poisson | Poisson |
| Treatment | Any BNL | BNL w/ PROA | Any BNL | BNL w/ PROA |
| Any BNL Enacted | 0.182 | | -0.0517 | |
| | (0.706) | | (0.114) | |
| BNL w/ PROA Enacted | | 0.993 | | 0.119 |
| | | (0.933) | | (0.347) |
| State Fixed Effects | Yes | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes | Yes |
| Observations | 765 | 765 | 765 | 765 |
| R-squared | 0.535 | 0.535 | | |

Robust standard errors clustered on states in parentheses

*** p<0.01, ** p<0.05, * p<0.1

## Table 13 – Effect of BNLs on Data Breach Counts and Magnitudes Given Other State Data Laws

| | (1) | (2) | (3) | (4) |
|---|---|---|---|---|
| Dependent Variable | ln(Records) | ln(Records) | numEvents | numEvents |
| Estimator | Log-OLS | Log-OLS | Poisson | Poisson |
| Treatment | Any BNL | BNL w/ PROA | Any BNL | BNL w/ PROA |
| Any BNL Enacted | 0.434 | | -0.0654 | |
| | (0.816) | | (0.133) | |
| BNL w/ PROA Enacted | | 1.283 | | 0.161 |
| | | (0.927) | | (0.324) |
| Firm Data Security Law Enacted | -0.274 | -0.125 | 0.0470 | 0.0133 |
| | (0.747) | (0.679) | (0.101) | (0.0840) |
| Agency Data Security Law Enacted | 0.734 | 0.762 | 0.285 | 0.290 |
| | (0.579) | (0.587) | (0.218) | (0.216) |
| Data Disposal Law Enacted | -0.321 | -0.455 | 0.0243 | -0.0114 |
| | (0.772) | (0.698) | (0.121) | (0.0998) |
| State Fixed Effects | Yes | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes | Yes |
| Observations | 765 | 765 | 765 | 765 |
| R-squared | 0.545 | 0.546 | | |

Robust standard errors clustered on states in parentheses
*** p<0.01, ** p<0.05, * p<0.1

## Table 14: Effect of BNLs on Data Breach Counts and Magnitudes Based on Alternative Definitions of Treatment

| | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) |
|---|---|---|---|---|---|---|---|---|---|---|
| Dependent Variable | ln(Records) | ln(Records) | ln(Records) | ln(Records) | ln(Records) | numEvents | numEvents | numEvents | numEvents | numEvents |
| Estimator | Log-OLS | Log-OLS | Log-OLS | Log-OLS | Log-OLS | Poisson | Poisson | Poisson | Poisson | Poisson |
| Treatment | BNL w/Access Protocol | BNL w/ Acquisition Protocol | BNL w/ Individual Notification | BNL w/ Owner Notification | BNL w/ AG Notification | BNL w/ Access Protocol | BNL w/ Acquisition Protocol | BNL w/ Individual Notification | BNL w/ Owner Notification | BNL w/ AG Notification |
| Access Protocol | -0.143 | | | | | -0.155 | | | | |
| | (0.677) | | | | | (0.0913) | | | | |
| Acquisition Protocol | | -0.435 | | | | | -0.0587 | | | |
| | | (0.593) | | | | | (0.104) | | | |
| Individual Notification | | | -0.415 | | | | | -0.0599 | | |
| | | | (0.592) | | | | | (0.104) | | |
| Owner Notification | | | | -0.330 | | | | | -0.0192 | |
| | | | | (0.652) | | | | | (0.128) | |
| AG Notification | | | | | -0.711 | | | | | -0.0200 |
| | | | | | (0.696) | | | | | (0.138) |
| State Fixed Effects | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Year Fixed Effects | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Observations | 765 | 765 | 765 | 765 | 765 | 765 | 765 | 765 | 765 | 765 |
| R-squared | 0.543 | 0.543 | 0.543 | 0.543 | 0.544 | | | | | |
| Number of Groups | 51 | 51 | 51 | 51 | 51 | 51 | 51 | 51 | 51 | 51 |

Robust standard errors clustered on states in parentheses
*** p<0.01, ** p<0.05, * p<0.1