Data Breach Notification Laws

By Richard J. Sullivan and Jesse Leigh Maniff

Data breaches, which expose sensitive data often used for payment fraud and identity theft, have recently worsened in the United States. Exposed records provide essential data for identity thieves, who in 2014 victimized 17.6 million people in the United States (Harrell). As a consequence, policymakers are placing greater emphasis on procedures to protect consumers from harm.

Breach notification laws are one such approach. Forty-seven state laws and some sector-specific federal laws already require organizations suffering a breach to disclose the incident and notify consumers if their data were exposed. In theory, breach notification laws serve two purposes important to public policy. First, they provide an incentive for organizations to protect sensitive data, as publicly disclosed security failures may harm their reputation and trigger costly remediation activities. Second, they inform individuals whose records were exposed, allowing them to react quickly to mitigate potential damages.

Research has shown that identity theft declines after a state adopts a data breach notification law (Romanosky and others). Research is less conclusive regarding how specific provisions in these laws might affect identity theft. In this article, we study recent identity theft complaints to investigate how provisions of state data breach notification laws affect identity theft. We find five provisions in notification laws associated with less identity theft. We also find three provisions associated

Richard J. Sullivan is a senior economist at the Federal Reserve Bank of Kansas City. Jesse Leigh Maniff is an analyst at the bank. Joshua Hanson, a research associate at the bank, helped prepare the article. This article is on the bank's website at ***www.KansasCityFed.org***

with more identity theft. These results may help guide public policy concerning breach notifications to protect the public after a breach and encourage organizations to improve data security.

Section I discusses organizations' legal duty to protect data and reviews prior research on whether notification laws incentivize organizations to protect data and inform customers in the event of a breach. Section II describes the various provisions in states' data breach notification laws. Section III presents a statistical analysis of the effect of 10 breach notification law provisions on identity theft.

I. The Case for Data Breach Notification Laws

An increase in the number of data breaches in the United States has led to public concern about protection against identity theft. In 2014, 1,343 breaches in the United States exposed more than 512 million records (Risk Based Security 2015). Policymakers have responded by enacting state and federal laws that require organizations to notify customers whose data are exposed in a security breach to allow them to take actions to reduce the potential harm from exposed data.

Although a few large, well-publicized breaches have drawn attention to data security recently, publicly disclosed data breaches have been increasing in the United States since 2009.[1] More than 600 breaches occurred in 2009, 1,054 in 2013, and 1,343 in 2014 (Risk Based Security 2015, 2014a; Sullivan 2012). The number of records exposed has also increased in recent years, largely due to a rise in the number of megabreaches—breaches exposing more than 10 million records (Sullivan 2014). As personally identifiable information is the most common type of information exposed during breaches, the increase in breaches is likely to result in greater instances of identity theft.

Over the past few years, the types of fraud committed using victims' information have evolved, particularly in the financial services sector. According to the Federal Trade Commission, the share of identity theft due to bank fraud and credit card fraud has steadily increased (Consumer Sentinel Network). The share of identity theft due to credit card fraud increased from 13.6 percent in 2012 to 16.9 percent in 2013 to 17.4 percent in 2014. Similarly, the share of identity theft due to

Table 1
States with Data Breach Notification Laws, 2003–14

Year	Number	Year	Number
2003	1	2009	45
2004	1	2010	45
2005	10	2011	46
2006	25	2012	46
2007	38	2013	46
2008	41	2014	47

Notes: Year is determined by the time the law took effect.
Sources: Perkins Coie and authors' calculations.

bank fraud rose from 6.4 percent in 2012 to 7.7 percent in 2013 to 8.2 percent in 2014.

Legal duty to protect data and notify consumers

In 2002, concerns over consumer privacy and data security on the Internet led lawmakers in California to enact a law requiring breached organizations to inform consumers whose personal data were exposed. Since California's law took effect in 2003, an additional 46 states have enacted data breach notification laws (Table 1).

An organization's legal duty to secure personal information can arise from tort law or legislation (Johnson). In tort law, an organization may have a duty to protect its customers if the organization increases the foreseeable risk of harm from third-party criminals (Bishop). If customers cannot prove this duty exists, they will be unable to satisfy a negligence claim against a breached organization. Even if customers prove this duty exists, they must then prove that the organization breached its duty, that the breach caused the harm, and that damages ensued. In previous cases, customers have had difficulty proving how they were harmed by the breach (Tabuchi).

To fill the gap, many state legislatures have enacted statutes affirming organizations' legal duty to secure personal information and codifying potential consequences of their failure to do so.[2] The most common way states have created this legal duty is by enacting data breach notification laws that require organizations to notify customers if a breach

occurs. These laws have their foundation in environmental law's "community right to know" (CRTK) provisions (Winn).[3]

The CRTK model, when applied to security breaches, would alert consumers when a breach occurs and allow them to take the necessary steps to protect themselves against identity theft. The model would also encourage organizations to improve their security and prepare for potential breaches.[4] Critics of CRTK laws, however, claim incentives are misaligned—for example, organizations may be reluctant to disclose information that could ultimately be used against them. Furthermore, organizations with weak security features may not be able to detect that a breach has even occurred. Still, 47 states currently have breach notification laws in place.

Research on data breach notification laws

Research on breach notification laws is at an early stage but has nevertheless shed some light on the mechanisms and effects of disclosure. For example, some research has shown that notification laws can reduce the rate of identity theft, but oversight might be needed to encourage compliance. What information organizations disclose to consumers after a breach may also be important to consumer protection.

Empirical evidence suggests data breach notification laws reduce identity theft. Romanosky and others investigate the relationship between notification laws and the rate of identity theft in the United States from 2002 to 2009. Consistent with the mechanism of a CRTK law, they hypothesize that after a law is passed, more consumers will be notified of breaches and in turn will take steps to protect themselves. The authors find that adopting a notification law reduced identity theft during the period of study by an estimated average of 6.1 percent, resulting in a mean reduction in the cost of identity theft of $93 million.

However, certain aspects of notification laws can strongly influence their effectiveness. Organizations that suffer a breach have some incentive *not* to notify customers to avoid the costs and consequences of disclosure. Stefan and Böhme investigate this incentive in a theoretical model and show that including a periodic audit requirement for security systems can greatly enhance the effectiveness of notification laws.

The language used to notify consumers can also influence these laws' effectiveness. Breach notification laws provide organizations some

latitude in how they inform customers about a breach, which can lead to suboptimal outcomes for affected consumers. Bisogni studies a sample of notification letters sent in 2014 to consumers whose data were exposed and finds that while these letters comply with notification laws, some organizations sending them understated the seriousness of the breach to reduce their reputational damage.

Furthermore, a notification law's efficacy can depend on how quickly it requires organizations to act in the event of a breach. In the organizations Bisogni studies, consumers were at risk for a considerable time prior to notification: the average time between an organization discovering a breach and notifying consumers was 35 days. More troubling, the average time between when a breach actually occurred and notification was 117 days. In other words, organizations are often unaware of the breach for an extended period in which potential harm could occur.

II. Provisions in State Data Breach Notification Laws

While research has shown that the presence of a data breach notification law reduces identity theft, few studies have examined the effects of variations in these laws on reported rates of identity theft.[5] To examine these differences, we review state notification laws from 2006 to 2014 to determine if a state's law includes one or more of 10 provisions. We begin our review in 2006 because it is the first year for which consistent state-level data on identity theft are available. The provisions are as follows:

State Enforcement provisions allow the attorney general or another designated state entity to enforce organizations' failure to comply with the statute.

Risk of Harm provisions require a breached organization to notify customers only if the organization determines that the breach constitutes a reasonable likelihood of harm to the customer.

Baseline Encryption Exemption provisions exempt an organization from notifying consumers if the data stolen in the breach were redacted or encrypted.[6]

Notification Policy Exemption provisions allow an organization that maintains its own notification procedures to be deemed in compliance

with the state notification law so long as the organization does, in fact, disclose breaches.

Notify AG/Credit Agencies provisions require organizations to notify one or more parties, such as the attorney general or a credit reporting agency, when a breach occurs.

Cap on Civil Penalty provisions limit the financial civil penalty imposed on organizations found in violation of the statute.

Doing Business in State provisions specify that the notification law only covers organizations that conduct business in the state. In states without this provision, organizations that do not conduct business in the state are still required to notify if a customer whose personal information is breached is a resident of the state.

Expanded Definition of Personal Information provisions indicate whether the notification law covers more information than meets the standard definition of personal information (PI). States typically define PI as a first name or initial in combination with a last name and a Social Security number, driver's license number, state ID card number, or financial account number. An expanded definition of PI includes other personal data, most often health and medical information.

Private Right of Action provisions allow customers whose data were exposed to sue organizations for failure to comply with the data breach notification statute.

Explicit Time Limit to Notify provisions specify that organizations must notify affected customers within a given number of days (usually 30 or 45). Notification laws without a specific time limit require notification as quickly as possible and without unreasonable delay.

Notification laws are present in 84.7 percent of our sample observations, but the prevalance of provisions within the laws varies across state and time (Table 2). The most common provision is State Enforcement, which is present in 76.2 percent of the 450 state and year observations in our data. Other common provisions are Risk of Harm (65.3 percent), Baseline Encryption Exemption (57.8 percent), and Notification Policy Exemption (57.3 percent); the least common provisions are Explicit Time Limit to Notify (6.8 percent), Private Right of Action (23.1 percent), Expanded Definition of PI (36.2 percent), and Doing Business in State (50 percent).

Table 2
Implementation of Data Breach Notification Laws Across States

Provision	Share of observations with the provision (percent)
State Enforcement	76.2
Risk of Harm	65.3
Baseline Encryption Exemption	57.8
Notification Policy Exemption	57.3
Notify AG/Credit Agencies	55.8
Cap on Civil Penalty	55.1
Doing Business in State	50.0
Expanded Definition of PI	36.2
Private Right of Action	23.1
Explicit Time Limit to Notify	6.7

Note: The sample contains 450 state and year observations.
Sources: Steptoe & Johnson, Schar and Gibbins, and authors' tabulation.

The share of states with the various provisions varies by year. One reason for this variation is that 22 states implemented notification laws during our sample period. A second reason is that four states amended existing notification laws during this period and added provisions we examine in this study. For our purposes, the variation is valuable in the statistical analysis we conduct.

III. Examining the Effects of Notification Law Provisions on Identity Theft

The CRTK effect of data breach notification laws enables victims to take actions to protect against identity theft. But provisions within notification laws may vary in how quickly and effectively they provide this opportunity. To examine whether certain provisions are more or less effective in reducing identity theft, we first rank individual states by their records on identity theft over the 2006–14 period. We then compare these rankings with the use of specific provisions in the notification laws of each state.

State records on identity theft

Ranking states' records on identity theft presents two challenges. First, more populous states will inherently have more identity theft than

Table 3
Sample Summary Statistics: Notification Law Provisions

	State identity theft per million persons				Deviation from the state average rate		
Record	Number of states	Average, 2006–09	Average, 2011–14	Change, 2011–14 minus 2006–09	Average, 2006–09 (percent)	Average, 2011–14 (percent)	Change, 2011–14 minus 2006–09 (percent)
Better	16	867	774	-93.4	23.8	3.8	-20.0
Mixed	19	592	628	35.2	-15.6	-16.0	-0.5
Worse	15	662	873	210.8	-5.7	16.2	22.0
All states	50	701	748	46.7			

Sources: Steptoe & Johnson, Schar and Gibbins, and authors' calculations.

smaller states, making direct comparisons unfair. To adjust for this difference, we consider identity theft per million persons. Second, forces may contribute to a rise or fall in identity theft that affects multiple states. Perpetrators of data breaches look for vulnerable databases in any location, but the data they obtain may be from customers in multiple states. Consequently, a rise in breaches nationwide can lead to a rise in identity theft in any of the states. To adjust for national fluctuations, we compute the difference of a particular state's identity theft per million persons from the average of identity theft per million persons for all states.

We evaluate the performance of states in deterring identity theft by first calculating the identity theft complaints per million persons for each of two periods: 2006–09 and 2011–2014.[7] States perform better if there is a reduction in identity theft over the two periods. Identity theft nationwide averaged 701 incidents per million persons in 2006–09 and 748 incidents per million persons in 2011–14 (Table 3).

We then calculate the annual percent deviation of identity theft per million persons for each state from the average rate nationwide. We then average the annual deviations over the 2006–09 and 2011–14 periods. The change in the percent deviation of identity theft per million persons is our basic measure of each state's record on identity theft. If the change is negative, then the state's identity theft per million persons has fallen relative to the national average, indicating a better record on identity theft. If the change is positive, then the state's identity theft per million persons has risen relative to the national average, indicating a worse record on identity theft.

We then sort states by the change in the difference of identity theft complaints per million persons relative to the national average and split them into three groups. States with a notable improvement over the 2006–09 and 2011–14 periods are labeled "Better," states with a notable decline are labeled "Worse," and states with little change from one period to the next are labeled "Mixed."[8] Details on how we group states and assess provisions' effects on identity theft are available in the Appendix.

While the overall rate of identity theft per million persons rose from 2006–09 to 2011–14, individual state records of identity theft varied considerably. In the Better group, 16 states had an average decline of 93.4 identity theft complaints per million persons from the 2006–09 period to the 2011–14 period (Table 3). By contrast, 19 states in the Mixed group had an average increase of 35.2 identity theft complaints per million persons over the same period. In the Worse group, the increase was much more dramatic: 15 states saw an average increase of 210.8 identity theft complaints per million persons. Relative to the national average rate, the change in identity theft per million persons was -20 percent for the Better group, -0.5 percent for the Mixed group, and 22 percent for the Worse group.

Provisions in data breach notification laws and the record of state identity theft

To assess how provisions in state data breach notification laws might affect identity theft, we examine the prevalence of various provisions in the Better, Mixed, and Worse groups of states. We consider a provision to be associated with less identity theft if it is common in the Better states, uncommon in the Worse states, and neither common nor uncommon in Mixed states. For example, in the 2006–09 period, 81.3 percent of states in the Better group had the State Enforcement provision compared with 67.1 percent of states in the Mixed group and 51.7 percent of states in the Worse group, suggesting the State Enforcement provision is associated with lower identity theft (Table 4).

Conversely, we consider a provision to be associated with increased identity theft if it is uncommon in Better states, common in Worse states, and neither common nor uncommon in Mixed states. For example, in the 2006-09 period, 43.8 percent of states in the Better group

Table 4

Identity Theft and Provisions in U.S. Notification Laws, 2006–14

Panel A: 2006–09

	Percent of states with provision									
Identity theft record	State Enforcement	Risk of Harm	Baseline Encryption Exemption	Notification Policy Exemption	Notify AG/Credit Agencies	Cap on Civil Penalty	Doing Business in State	Expanded Definition of PI	Private Right of Action	Explicit Time Limit to Notify
Better	81.3	43.8	40.6	59.4	57.8	68.8	43.8	37.5	26.6	0.0
Mixed	67.1	67.1	63.2	59.2	46.1	48.7	59.2	26.3	22.4	5.3
Worse	51.7	58.3	51.7	33.3	33.3	21.7	28.3	28.3	8.3	13.3
P-value	0.002**	0.020**	0.029**	0.003**	0.024**	0.000**	0.002**	0.326	0.027**	0.007**

Panel B: 2011–14

	Percent of states with provision									
Identity theft record	State Enforcement	Risk of Harm	Baseline Encryption Exemption	Notification Policy Exemption	Notify AG/Credit Agencies	Cap on Civil Penalty	Doing Business in State	Expanded Definition of PI	Private Right of Action	Explicit Time Limit to Notify
Better	93.8	50.0	43.8	68.8	68.8	81.3	50.0	50.0	31.3	0.0
Mixed	78.9	78.9	68.4	63.2	67.1	57.9	63.2	34.2	31.6	5.3
Worse	80.0	86.7	73.3	53.3	53.3	46.7	46.7	40.0	13.3	18.3
P-value	0.044**	0.000**	0.001**	0.194	0.129	0.000**	0.094*	0.182	0.026**	0.000**

** Significant at the 5 percent level.
* Significant at the 10 percent level.

Notes: The Better, Mixed, and Worse groups include 16, 19, and 15 states, respectively. We study four years in each period, which yields 64, 76, and 60 observations for the performance groups. The p-values are for chi-square statistics that test whether the percentage of states with the breach law notification provisions are different from one another across the Better, Mixed, and Worse groups. Asterisks indicate the significance level at which a null hypothesis of equal adoption of the provisions across performance groups is rejected.

Table 5

Associations between Notification Law Provisions and State Identity Theft

Provisions associated with lower identity theft	Strength of evidence
State Enforcement	Medium
Notify AG/Credit Agencies	Medium
Cap on Civil Penalty	High
Private Right of Action	Medium
Notification Policy Exemption	Low
Provisions associated with higher identity theft	**Strength of evidence**
Risk of Harm	Medium
Baseline Encryption Exemption	Low
Explicit Time Limit to Notify	High

Notes: The Doing Business in State and Expanded Definition of PI provisions have mixed or no association with identity theft. The strength of evidence designation is based on a statistical test of whether records of identity theft across the Better, Mixed, and Worse groups of states are equal; the pattern of use of a provision across the groups; and the extent to which the pattern is consistent across time periods.

had the Risk of Harm provision compared with 67.1 percent of states in the Mixed group and 58.3 percent of states in the Worse group, suggesting the Risk of Harm provision may be associated with higher identity theft.

The statistical analysis does not always point to a clear association between variables. Accordingly, we also assess the strength of evidence for a particular relationship. The evidence for an association is stronger if the pattern of use across the states is clear, rising or falling across all three groups. The evidence is also stronger if the pattern is consistent over both the 2006–09 and 2011–14 periods. Finally, we conduct a statistical test for whether provisions are equally prevalent across the three groups of states. If a provision is equally common in the Better, Mixed, and Worse groups of states, the provision is unlikely to have a strong association with identity theft.[9]

We apply this method to the results from Table 4 and find five provisions associated with lower identity theft (Table 5). Two of these, State Enforcement and Notify AG/Credit Agencies, signify formal involvement of state government in enforcing or managing responses to data breaches. These provisions may signal the commitment of state resources to fighting identity theft, which may, in turn, encourage

organizations to comply with notification requirements when they suffer a data breach.

Two other provisions associated with lower identity theft, Cap on Civil Penalty and Private Right of Action, manage the options that victims of data breaches have when their personal information is exposed. Both provisions may also encourage organizations to comply with notification requirements and thus reduce identity theft. A cap on civil penalties may provide greater certainty to organizations regarding the costs and consequences of disclosing a data breach. A private right of action, on the other hand, allows victims to pursue recourse when their data are exposed, an option that an organization can preclude by disclosing a breach.

Finally, the Notification Policy Exemption is also associated with lower identity theft. To secure an exemption, organizations must have data security policies that may be part of a comprehensive security strategy. To the extent the provision signals how seriously an organization attempts to protect electronic data, it may both reduce a state's actual data breaches and enable breach victims to protect themselves against identity theft.

We find three provisions associated with higher identity theft. Two of these provisions, Risk of Harm and Baseline Encryption Exemption, may make it easier for organizations to legally avoid disclosing a data breach. If an organization misinterprets the risk of harm from a breach and chooses not to notify victims, then preventable identity theft may occur. Likewise, if an organization with a weak encryption system does not notify victims, then the breach's perpetrators may be able to decrypt the stolen data and consequently steal identities.

A third provision, Explicit Time Limit to Notify, is also associated with higher identity theft. While this provision requires timely notifications, the short timeframe may result in organizations deciding to notify consumers when they would not have otherwise. Without this provision, a business may have more time to weigh the costs and benefits of disclosure, and, in some cases, decide not to disclose. Thus, Explicit Time Limit to Notify may lead to consumers being oversaturated with notifications, some of which are not necessary, and subsequently choosing to ignore them after a certain point.[10]

IV. Summary and Conclusion

In this article, we present evidence of data breach notification laws' "right to know" effect through which increased disclosure of breaches is associated with reduced identity theft. We find states with provisions that signal active state enforcement have lower rates of identity theft. Likewise, states with provisions that provide incentives to organizations to comply with notification requirements have lower identity theft. Finally, states with a provision that exempts organizations from notification laws if they have internal policies to notify customers also have lower identity theft.

Some provisions are associated with higher identity theft. In some cases, these provisions give an organization control regarding notification, such as exempting the organization from notification if it determines there is little potential harm to an exposed consumer or if it adopts a relatively weak method of encrypting sensitive data. In both cases, the provision may block the "right to know" mechanism after serious breaches and thus lead to greater identity theft.

Although policymakers are rightly concerned about data theft, fraudulent use of the data is the real danger. Thieves can use payment data to replicate credit cards and make fraudulent purchases, and they can use medical insurance data to perpetrate fraud for medical services. They can use nonpayment data to receive tax refunds and open new accounts to draw on lines of credit. Further progress is needed to ward off fraud, particularly as attacks shift to industries with weaker security practices.

Appendix

Methodology

The method we use to rank how states perform in deterring identity theft accounts for both the size of each state and the nationwide average of identity theft.

The ranking is based on the record of identity theft in each state for the 2011–14 period compared with the 2006–09 period. We exclude 2010 for two reasons. First, it allows us to compare periods with the same number of years. Second, starting the later period in 2011 provides a one-year lag that allows the laws of the four states that adopted notification laws in 2009 to have a more observable effect on identity theft as state enforcement is established and news of notification requirements spreads among eligible organizations.

Including 2010 in either the first or the second period does not change our results. None of the patterns of provision prevalence across the groups of states is affected. In one case (Doing Business in State), the p-value falls to 0.04, a smaller value than the 0.094 reported in Table 4. However, the prevalence pattern for Doing Business in State is not consistent with either a worse or better record on identity theft, and thus we would not include the provision in Table 5 even with a lower p-value.

The states of Oklahoma, Kansas, and Missouri provide examples of states classified, respectively, as Better, Mixed, and Worse performers. The three states' records of identity theft per million persons are similar in the 2006–09 period, ranging from 648 to 681. In the 2011–14 period, identity theft per million persons declined to 630 in Oklahoma, a change of -51.1; rose to 663 in Kansas, a change of 15.1; and rose to 829 in Missouri, a change of 154.8 (Table A-1). Thus, identity theft declined in Oklahoma, increased somewhat in Kansas, and increased more dramatically in Missouri.

To adjust for national trends, we subtract each state's annual identity theft per million persons from the 50 state average, then divide that number by the 50 state average and multiply it by 100. The result is the annual percent difference of the state's identity theft per million persons from the national average. The annual percent differences are then averaged over 2006–09 and 2011–14.

Table A-1
State Records of Identity Theft

State	Identity theft per million persons		
	2006–09	2011–14	Change, 2006–09 to 2011–14
Oklahoma	681	630	-51.1
Kansas	648	663	15.1
Missouri	674	829	154.8

Table A-2
State Versus Nationwide Identity Theft

State	Difference from national average		
	2006–09 (percent)	2011–14 (percent)	Change, 2006–09 to 2011–14 (percent)
Oklahoma	-2.7	-15.6	-12.9
Kansas	-7.5	-10.7	-3.2
Missouri	-3.6	10.9	14.6

In Oklahoma, identity theft per million persons averaged 2.7 percent less than the national average in 2006–09, and 15.6 percent less than the national average for 2011–14, a net change of -12.9 percent (Table A-2). In Kansas, identity theft per million persons was below the national average in both 2006–09 and 2011–14, at -7.5 percent and -10.7 percent, respectively, for a net change of -3.2 percent. Missouri's identity theft per million persons was below the states' average by 3.6 percent for 2006–09, but above the states' average by 10.9 percent for 2011–14, a net gain of 14.6 percent.

To determine the cutoff point for the Better, Mixed, and Worse performance levels, we estimate trend lines for each state's identity theft per million persons as a percentage of the states' average.[11] The model is

$$y_{it} = \alpha + \beta\ year_{it} + \varepsilon_{it},$$

where y_{it} is identity theft per million persons as a percent of the states' average, and β is the trend coefficient. The trend coefficients in the estimated equations are significantly different from zero for half of the states (both positive and negative). The cutoff point for the Better performing states is determined by the state with a significant and negative trend coefficient and the smallest percent reduction of identity theft per million persons. The cutoff point for the Worse performing states is determined by the state with a significant and positive trend coefficient and the smallest percent increase of identity theft per million persons. State performance groups are as follows:

Better: AZ, CA, CO, HI, IL, IN, MN, MA, NC, OK, NM, NV, NY, TX, UT, VA

Mixed: AK, CT, NE, ID, KS, KY, LA, MD, ME, MT, ND, NH, NJ, OH, OR, PA, RI, SD, TN

Worse: AR, AL, DE, FL, GA, IA, SC, MI, MO, MS, WA, WI, WV, WY

To assess the strength of evidence for relationships between certain provisions in state notification laws and state performance with identity theft, we use three criteria. First, we use statistical analysis to test a hypothesis that a provision is equally common across all three groups of states. The test generates a probability value (p-value) that, if sufficiently small (0.05 or less), rejects the hypothesis. If the test rejects the hypothesis, then we have more confidence that differences in the effect of notification law provisions in states are unlikely to be a result of random sample variation.

The other two criteria consider a provision's pattern of use across the groups of states and whether the pattern is similar across the 2006–09 and 2011–14 periods. If a provision is more common in states in the Better group, then the provision may be effective at deterring identity theft. Conversely, if a provision is more common in states in the Worse group, then the provision may not be effective at deterring identity theft. The evidence for these associations is stronger if the patterns are similar across the two periods.

When we apply these criteria to the State Enforcement provision, the most common provision in our sample, we find the groups of states have low p-values for both periods, suggesting the variation in use is not due to random sample variation (see Table 4). In the 2006–09 period, the Better, Mixed, and Worse groups of states had this provision in place in 81.3 percent, 67.1 percent, and 51.7 percent of observations, respectively. This finding suggests the provision is associated with lower identity theft. In the 2011–14 period, the Better, Mixed, and Worse groups of states had the provision in 93.8 percent, 78.9 percent, and 80 percent of observations, respectively. The statistical pattern suggests the State Enforcement provision helps reduce identity theft; however, because the pattern of use is not consistent across the two time periods, we assign a medium score to the strength of evidence.

The second most common provision, Risk of Harm, has similarly low p-values in both periods. In the 2011–14 period, the Better group had the provision in 50 percent of observations, the Mixed group in 78.9 percent of observations, and the Worse group in 86.7 percent of observations, suggesting that a Risk of Harm provision is associated with increased identity theft. The pattern is muddier in the 2006–09 period: the Mixed group had the provision in 67.1 percent of observations, slightly more than the Worse group (58.3 percent). The Better group had the provision in only 43.8 percent of observations in the 2006–09 period, consistent with the pattern in the 2011–14 period. We again assign a medium score to the strength of evidence.

Table 5 shows the results from this method. Five provisions are associated with lower identity theft, and three are associated with higher identity theft. The strength of evidence varies for each provision.

Endnotes

[1]The breaches at Target in 2013 and Home Depot in 2014, which exposed 110 million and 109 million records, respectively, are possibly best known among recent breaches (Risk Based Security 2015). Other recent breaches include 152 million records exposed at Adobe Systems in 2013, 173 million records exposed at the New York City Taxi & Limousine Commission in 2014, and 145 million records exposed at eBay in 2014.

[2]Federal statues regarding security breaches are fragmentary. Statutes include the Federal Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act. In addition, the Federal Trade Commission has used its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, to challenge unfair data security practices.

[3]CRTK notifications provide the public with information about potential hazards, allowing those in the community to protect themselves. Additionally, notifications encourage improvements that prevent hazards by exposing the risk within an organization.

[4]In a 2007 study, chief security officers stated breach notification obligations led to new access controls, auditing measures, and encryption (Samuelson).

[5]Romanosky and others do not find any significant relationship between simple measures of notification law features that influence strictness and identity theft. However, our approach digs deeper by studying a more complete characterization of data breach disclosure laws.

[6]Some states with this provision add requirements such as a strong encryption standard or an uncompromised encryption key. Because these states require more than baseline encryption, we do not count them as having this provision.

[7]We exclude 2010 to compare periods of equal length and because starting the later period in 2011 provides a one-year lag allowing the laws of four states that adopted notification laws in 2009 to have an effect on identity theft. Including 2010 in either the early or late period does not affect our results (see Appendix).

[8]The term "notable" is based on a statistically significant trend in percent deviation of identity theft per million persons for each state from the nationwide average rate (see Appendix).

[9]More specifically, the statistics do not allow rejection of equal prevalence of the provision across the three groups of states. A hypothesis of equal prevalence of the provisions across the three groups of states could not be rejected in the case of Expanded Definition of PI for both the 2006–09 and 2011–14 time periods. The hypothesis is rejected in the case of Doing Business in State for the 2006–09 period and marginally rejected for the 2011–14 period, but there is no clear pattern of how the provision affects identity theft. As a consequence, we find no association of these provisions with state records on identity theft.

[10]Note that only 6.7 percent of observations have this provision.

[11]We also estimate a similar model that accounts for the years in which states implemented a data breach notification law and find results consistent with the simpler model.

References

Bishop, Derek A. 2006. "To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information?" *Shidler Journal of Law, Commerce, & Technology,* vol. 3.

Bisogni, Fabio. 2015. "Data Breaches and the Dilemmas in Notifying Customers," *The 14th Annual Workshop on the Economics of Information Security*, Delft University, June 23–25.

Federal Bureau of Investigation. 2014. "Estimated Property Crime Total," *Uniform Crime Reports.*

Federal Trade Commission. 2015. *Consumer Sentinel Network Data Book.*

———. 2014. *Consumer Sentinel Network Data Book.*

Harrell, Erika. 2015. "Victims of Identity Theft, 2014," U.S. Department of Justice Bureau of Justice Statistics *Bulletin*, September**.**

Johnson, Vincent R. 2005. "Cybersecurity, Identity Theft, and the Limits of Tort Liability," *South Carolina Law Review*, vol. 57, pp. 255–311.

Laube, Stefan, and Rainer Böhme. 2015. "The Economics of Mandatory Security Breach Reporting to Authorities," *The 14th Annual Workshop on the Economics of Information Security*, Delft University, June 23–25.

Perkins Coie Privacy and Security Group. 2014. "Security Breach Notification Chart," October, available at www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

Risk Based Security. 2015 "Data Breach Quick View: 2014 Data Breach Trends," February.

———.2014a. "Data Breach Quick View: 2013 Data Breach Trends," February.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management*, vol. 30, no. 2, pp. 256–286.

Samuelson Law, Technology & Public Policy Clinic. 2007. "Security Breach Notification Laws: Views from Chief Security Officers," University of California-Berkeley School of Law, available at https://www.law.berkeley.edu/files/cso_study.pdf.

Schar, Reid J., and Kathleen W. Gibbons. 2013. "Complicated Compliance: State Data Breach Notification Laws," *Bloomberg BNA Privacy and Security Law Report*, no. 32, August.

Simitian, Joseph. 2009. "How a Bill Becomes Law, Really," *Berkley Technology Law Journal,* vol. 23, no. 3, pp. 1009–1018.

Steptoe & Johnson LLP. 2015. "Comparison of U.S. State and Federal Security Breach Notification Laws," *Privacy and Security Law Report*, August, available at www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf.

Sullivan, Richard J. 2014. "Controlling Security Risk and Fraud in Payment Systems," Federal Reserve Bank of Kansas City, *Economic Review,* vol. 99, no. 3, pp. 47–78.

———. 2012. "The Federal Reserve's Reduced Role in Retail Payments: Implications for Efficiency and Risk," Federal Reserve Bank of Kansas City, *Economic Review*, vol. 97, no. 3. pp. 79–106.

Tabuchi, Hiroko. 2015. "$10 Million Settlement in Target Data Breach Gets Preliminary Approval," *The New York Times,* March 19.

U.S. Census Bureau. 2014. "Annual Estimates of the Resident Population for the United States, Regions, States, and Puerto Rico: April 1, 2000 to July 1, 2014."

———. 2013a. *American Community Survey.*

———. 2013b. *Statistics of U.S. Businesses.*

Winn, Jane K. 2009. "Are 'Better' Security Breach Notification Laws Possible?" *Berkeley Technology Law Journal*, vol. 24, no. 3, pp. 1133–1165.