Proving Limits of State Data Breach Notification Laws: Is a Federal Law the Most Adequate Solution?

Bisogni, F.

DOI
10.5325/jinfopoli.6.2016.0154

Publication date
2016

Document Version
Final published version

Published in
Journal of Information Policy

Proving Limits of State Data Breach Notification Laws: Is a Federal Law the Most Adequate Solution?

Author(s): Fabio Bisogni

Source: *Journal of Information Policy*, 2016, Vol. 6 (2016), pp. 154-205

Published by: Penn State University Press

Stable URL: https://www.jstor.org/stable/10.5325/jinfopoli.6.2016.0154

PROVING LIMITS OF STATE DATA BREACH NOTIFICATION LAWS

Is a Federal Law the Most Adequate Solution?

Fabio Bisogni

ABSTRACT

This article investigates the adequateness of data breach notification laws and the possible impact of a federal law in the United States. Based on the analysis of 445 notifications issued in 2014, three observations for law development are presented. First, the question about underreporting is raised and a possible option for facilitating its emergence is proposed. Second, the specification of the dates of the breach detection and of the breach itself are identified as essential to foster consumers' reaction. Finally, a stricter regulation of the content of the notification is suggested to avoid firms minimizing the actual risk.

Keywords: data breach notification laws, data breach disclosure, bad-news messages

Introduction

It seems that the debate about security and data breaches has reached its apex due to both the media coverage of significant breaches involving thousands of records and the maturation at the institutional level of the issue. During the time frame 2005 to 2014, there have been 4,695 breaches exposing 633 million records, according to the nonprofit Identity Theft Resource Center, with an average cost of a breach to an organization estimated in 2014 at $3.5 million.[1]

In the United States, with the exception of Alabama, Kentucky, New Mexico, and South Dakota, every state as well as the District of Columbia, Puerto Rico, and the US Virgin Islands has enacted legislation requiring

Fabio Bisogni: Faculty of Technology, Policy and Management – Delft University of Technology
Formit Foundation

1. Ponemon Institute LLC.

JOURNAL OF INFORMATION POLICY, Volume 6, 2016

notification of security breaches involving personal information in order to counteract such a phenomenon. For an organization having a customer base in more than one state, it is necessary to deal with compliance with multiple state laws. In fact, the applicability of the US notification laws relates not to the residence of the breached organization, but to the residence of the affected customers. This means that a company dealing with customers residing in different states has to follow various state laws.

These differ in many elements, including who—apart from the customer—must be notified, the level of risk that triggers a notice, the nature of the notification, and exceptions to the requirements. Therefore, one must perform an analysis of all applicable state regulations, in order to be sure that each customer's state law has been fully followed in all its provisions. Table 1 summarizes the key questions[2] a state data breach notification law answers, defining its severity and features.

In order to better understand the diversity of the forty-seven state laws and the impact of such diversity, we will shortly describe the core elements deriving from those questions.

The first US data breach notification law, enacted in California,[3] requires any business that had suffered a data breach, or believes that it has suffered a data breach that might entail an unauthorized acquisition of unencrypted and computerized personal information, to notify California residents about the incident. Also, the attorney general needs to be notified if more than 500 residents' data are involved in the security breach. A law enforcement agency can request a delay if the notification would impede a criminal investigation. Individuals are to be notified within a time frame

TABLE 1 Questions Shaping the Data Breach Notification Laws

What entities are covered? Is there a requirement for service providers?	What data are covered?	Has there been a breach? Is there a risk of harm analysis?	Who receives notice?	When must notice be given? May notice be delayed?	How must notice be given? Is substitute notice available?	Is there an exemption or safe harbor?	Enforcement? Penalties? Is there a private right of action?

2. Steptoe.
3. California Civil Code § 1729.98(a).

that is expedient and without unreasonable delay. Notifications can take different forms including by postal letter, electronic notification, or substitute notice, which entails "conspicuous posting" on the organization website or via state media sources. However, some data breaches are exempt from notification. These include encrypted personal information or "good faith acquisition" of personal information by an employee or agent of the breached entity.

The other US states may diverge from the Californian model according to local decisions taken in regard to different legislative elements; however, the notification law implementation is always seen as a potential remedy to address the multifaceted problems of personal information protection, inadequate corporate information security measures, and the rapid increase of identity theft crimes.

The scope of the laws in terms of Personal Information definition may vary. The BakerHostetler law firm provides a standard definition of personal information based on the definition commonly used by most states.[4] Twenty-five states have a broader definition for Personal Information than this standard one, consequently broadening also the definition of the data breach. Moreover, in some states the trigger for notification is given not only by the data acquisition, as in California, but also by data access. In six states, the breach of security is not only limited to electronic records, but involves also paper records. In terms of coverage in all forty-seven states, the notification requirements describe the categories of entities to which the law is applicable. There are two broad categories: entities that own or license computerized data and entities that maintain computerized data. Whereas all the state laws apply to entities that own or license personal information, one-fourth of the state laws also apply to entities that maintain personal data. Almost all states foresee notification exemptions in case of, for example, encrypted data (thirty-eight) or publicly available government records (all). Exemptions are also provided by some states for investigation purposes by law enforcement, for breaches that are either immaterial or not "reasonably likely to subject the customers to unauthorized disclosure of personal information" after a required proper risk of harm analysis. Exemptions are also foreseen in case of other sectoral legislation, as in the Gramm–Leach–Bliley Act for financial institutions or the Health

4. BakerHostetler, "State Data Breach," 2014.

Insurance Portability and Accountability Act for healthcare providers, or compliance with rules, regulations, procedures, or guidelines established by a primary regulator.

Also, the level and the limit of penalties vary. It is important to highlight that there are two possible limits foreseen by some of the laws related to the single security breach or to the number of records accessed/acquired thanks to the breach. Apart from twenty-three states that left the maximum measure of a penalty undefined, other states have included a limit either for a single breached record (six), or for a single breach (eight), or both (ten). The limit of penalties can be linked to the duration of the missing notification, to the size of the caused damage or be expressed in absolute value, ranging from $10,000 (Arizona) to $750,000 (Michigan). The penalties, and therefore the financial burden for companies, can become more severe in case of a private cause of action, which may result in civil and penal consequences for the involved organizations. Only in thirteen states do residents also have the right to take private action against companies that disclose their information; in the remaining ones this activity can be performed by the attorney general.

Another relevant element, which takes into consideration the reputational risk of companies, is the compulsoriness of notifications to be delivered to authorities in addition to those delivered to residents whose data have been subject to access or acquisition. Few states decided to include such notifications to third parties, specifically to the attorney general and/or consumer reporting agencies (eighteen and thirty, respectively).

The regulated mandatory content of the notice to be sent to residents, specified in the law provisions of fifteen states, also plays a role in evaluating the potential reputational effects of a breach for a firm.

Finally, the timing of the notice, with all states requiring that the notice be provided in the most expedient time and manner possible and without unreasonable delay, is consistent with the legitimate need of law enforcement. Only a few states add to this statement a specific maximum timeline of forty-five days after the breach discovery (Florida, Ohio, Vermont, and Wisconsin).

From such an overview, it is clear that great efforts have been made to address the data breach issue, but while the current state data breach notification laws provide consumers with valuable information regarding the security of their personal information, these laws are far from perfect and

for several reasons do not sufficiently address the problems created for both consumers and businesses by data breaches.[5] The core problem is generated by the large patchwork of state laws that make corporate compliance difficult and costly. The first solution that may be considered is a federal law on the issue. We will now depict core challenges of such a law, embedding the analysis with concrete findings coming from actual notifications sent in 2014.

State of the Art

On January 12, 2015, President Obama proposed the Personal Data Notification & Protection Act, which would create a federal standard for data breach notifications. The draft bill follows a long line of legislative proposals that have failed to gain passage despite the rising incidence of high-profile data breaches. In the last two years, five data breach notification bills were introduced in the Senate alone, yet none garnered sufficient support for passage.[6]

The implementation of a federal law raises a certain number of questions and the different actors involved may see such event as good or bad news also according to the features of the law itself. The key elements of the Personal Data Notification & Protection Act are as follows:

- The definition of personal information would be more expansive than most state breach notification laws, including home address, telephone number, mother's maiden name, and date of birth as data elements;
- Companies would be required to implement and maintain reasonable security measures and practices to protect and secure personal information;
- Companies would not be required to provide notice if there is no reasonable risk of identity theft, economic loss, economic harm, or financial harm;

5. Joerling.

6. Data Security Act of 2014, S. 1927, 113th Cong. (Sens. Carper & Blunt); Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (Sen. Rockefeller); Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (Sen. Leahy); Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (Sen. Blumenthal); Data Security and Breach Notification Act of 2013, S. 1193, 113th Cong. (Sen. Toomey).

- Companies would be required to provide notice to affected individuals within thirty days after discovery of a breach;
- The law would preempt all state data breach notification laws;
- Enforcement would be by the Federal Trade Commission (FTC) or state attorneys general; and
- No private right of action would be permitted.

Actors involved in the discussion include business groups that support federal legislation because it creates a single breach notification standard, reasoning that even a tougher federal standard would be simpler to comply with than the current patchwork of forty-seven different—and often conflicting—state laws.[7] Consumer protection groups and attorneys general were concerned because the federal legislation would preempt state data breach notification laws, including those that offer greater protection than the proposed federal standard. With a letter sent on July 7, 2015, the National Association of Attorneys General (NAAG) addressed congressional leaders, urging them to consider the state laws that have been put in place to protect consumers, and not to diminish the role that state attorneys general play in enforcing data security and protection laws.

The letter urges Congress not to make changes to federal data breach notification and data security laws that would lessen the protections that have been put in place by the states. The letter calls for Congress to refrain from introducing data security and data breach notification laws that preempt those introduced in each state, stating that "Preemption interferes with state legislatures' democratic role as laboratories of innovation," and stressing how "any federal legislation on data breach notification and data security should recognize the important role of State Attorneys, on the front lines responding to data breaches, and not hinder States that are helping their residents."

In order to contribute to this debate, our analysis followed an approach that was not based on the past investigations about data breach trends or evaluation of data breach costs, but that relied on a vast dataset represented by the data breach notifications themselves.

The findings presented so far by other researchers on impacts breach notifications for breached organizations in terms of their performance provide, however, a relevant context for our study.

---

7. Brendan.

Romanosky, Telang, and Acquisti[8] suggest that the adoption of state-level data breach disclosure laws could reduce identity thefts from these breaches by, on average, 6.1%. Telang and Wattal's research[9] highlights how software vendors' stock prices suffer if information about their products' vulnerability is announced. Acquisti, Friedman, and Telang[10] investigate by means of an event study the impact on stock market prices for firms that incur a privacy breach and find a negative and relevant reduction of 0.6% on the day of the breach disclosure. Campbell et al.[11] find a significant and negative effect on the stock price of the breached company for data breaches caused by "unauthorized access to confidential information" (p. 1). Cavusoglu, Mishra, and Raghunathan[12] find that the disclosure of a security breach results in the loss of $2.1 of a firm's market evaluation. On the other hand, Ko and Dorantes[13] study four financial quarters following a security breach and find that, although breached firms' overall performances were lower (relative to firms that incurred no breach), their sales increased significantly (again, relative to firms that incurred no breach). Laube and Böhme[14] devised a principal–agent model to analyze the economic effect of mandatory security breach reporting to authorities, proving that it may be difficult to adjust the level of sanctions such that security breach notification laws are socially beneficial. Edwards, Hofmeyr, and Forrest[15] developed Bayesian Generalized Linear Models applied to a public dataset to investigate trends in data breaches in the United States, showing that neither size nor frequency of data breaches has increased over the past decade. Kwon and Johnson[16] used a propensity score matching technique to investigate how data breaches affect subsequent outpatient visits and admissions in the United States, finding that the cumulative effect of breach events (and also of number of breached records) over a three-year period significantly decreases the number of outpatient visits and admissions. Veltsos[17] analyzed thirteen data breach notification templates from state and federal agencies confirming that the direct pattern may be an effective way to inform users as required by law, to overcome optimism

8. Romanosky, Telang, and Acquisti.
9. Telang and Wattal.
10. Acquisti, Friedman, and Telang.
11. Campbell et al.
12. Cavusoglu, Mishra, and Raghunathan.
13. Ko and Dorantes.
14. Laube and Böhme.
15. Edwards, Hofmeyr, and Forrest.
16. Kwon and Johnson.
17. Veltsos.

bias and rational ignorance. Finally, Bisogni[18] investigated the phenomenon of data breach notification letters, identifying six letter types used by the US companies in 2014.

Our approach is based on forty-seven[19] state data breach notification laws and selected extensive reports issued by law firms and available online,[20] thoroughly examined to identify—where available—mandatory elements of the notification letters and on the content of all data breach notifications made available in the United States in 2014. The sample includes 445 notifications sent in 2014 from breached organizations to consumers[21] downloaded from the attorney general websites of four different states used to verify the choices made by the affected companies. The methodological steps followed in order to conduct an in-depth analysis are described here.

1. Identify the states that make available the data breach notification letters issued by affected companies.
2. Download all letters included in the list available in the time frame January 1, 2014, to December 31, 2014, identifying the letters sent out in more than one of the four states.
3. Based on the content of the missive, isolate specific letter elements and create a database to code each characteristic at the paragraph level to understand the order of the letter contents, and at the sentence level to identify the content and purpose.
4. Perform a data analysis aimed at investigating:
   - possible schemes in the sent notifications
   - the timing of such missive and their related usefulness to support a lower consumer harm

Looking at the Sample

From our desk research in 2014, only six states out of forty-seven make notifications available through the government website, specifically through the attorney general websites. These states are California, Maryland, New

18. Bisogni.

19. Alabama, New Mexico, and South Dakota are now the only US states that have not yet enacted a data breach notification law.

20. CLLA; Levin; BakerHostetler, "State Data Breach," 2014; Perkins.

21. An additional forty-five letters were discarded because either they were second communications or some information was not visible in the downloaded letter.

Hampshire, and Vermont.[22] Another two states, Maine and Indiana, make available the list of data breaches relevant for the state residents, but do not provide a copy of the sent notifications. Full letter availability in the six states is the consequence of a specific state law requirement, the government notice. Such a requirement made the notification mandatory, in case of a breach, not only to residents, but also to the office of the state attorney general so that they have an overview of the state breach situation and can decide about the level of visibility of the missives (eighteen states in 2014). They in fact act as collector of all data breach notifications affecting state residents. Only the first four listed above (California, Maryland, New Hampshire, and Vermont) out of eighteen made the letters public in 2014.

The number of analyzed letters taking out the duplications (same letter sent to different states) amounts to 445, with the following split of unique letters by state: 130 for Vermont, 169 for California, 250 for Maryland, and 161 for New Hampshire. The overlapping between the four states can be seen in the Figure 1. There were 291 notifications sent only in one of the four states, seventy-five in two states, forty-five in three states, and finally thirty-four letters were sent to residents in all four states.

It is important to point out the relevance of the sample used. In fact, even if the number of the analyzed letters can be perceived as low, taking into consideration the phenomenon of data breaches, it is worth noticing

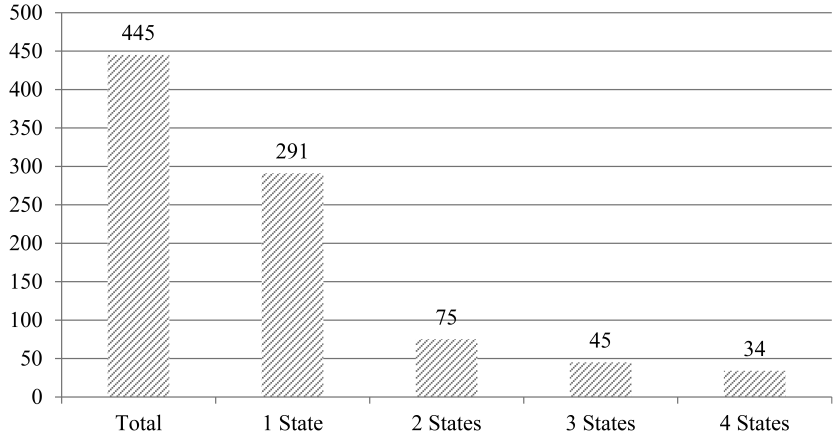


FIGURE 1 Data breach sample January 1, 2014–December 31, 2014.

22. Washington and Oregon started, respectively, from mid-2015 and 2016 to give such visibility, after law revision.

that 445 letters represent 56.83% of the 783 cases collected totally in the United States in the same period by different sources, as the Data Breach Report 2014[23] shows. The total of cases collected comes from the ITRC (Identity Theft Resource Center) breach list, a compilation of data breaches confirmed by various media sources and/or notification lists from state governmental agencies, representing the total number of breaches known to the public thanks to media operators, attorneys general offices, other governmental bodies such as the US Department of Health and Human Services, and specific sectoral databases making data breaches available.[24]

Observation 1: The high percentage of notifications from four states to the total number of breaches in the United States can raise the question of underreporting and stress the role of the government notice requirement as emergence facilitator.

While the number of letters collected is comforting about the representativeness of the sample analyzed in this work, it makes us reflect on the existence of a plausible high number of hidden data breaches that are not publicly disclosed. Since forty-three states are left out from the analysis (as they do not make notifications publicly accessible), we would expect a much higher number than 783 as the total of data breaches in the United States in the analyzed twelve-month period. In fact, the four states only represent 14.37% of the total number of firms in the United States, according to Economic Census 2012 statistics,[25] and 14.98% of residents, according to Census 2010.[26]

Additionally, based on the letter downloaded in the four states and looking at the sectors where breaches took place, we can identify approximately 15% of notifications belonging to local retail business, service, or medical centers acting locally, where we can assume that the place of the breach and the residency of the affected individuals coincide. For example, on September 30, 2014, at Gold's Gym, a member was required by an associate to provide their credit card three-digit security number, even if Gold's Gym does not require such information. Or BringItToMe.com, an online restaurant marketing and delivery service active in San Diego, California. Their online ordering software provider informed them that they identified unauthorized modifications in their software that could potentially

23. Identity Theft Resource.

24. A list of ITRC resources for data breaches is available at http://www.idtheftcenter.org/index.php/id-theft/data-breaches.html.

25. Economic Census.

26. Census Brief.

allow new payment credit card information entered between October 14, 2013, and January 13, 2014, to have been obtained by an unauthorized user. We can assume that similar events happen throughout the United States, with a similar percentage of firms per sector affected by local data breach affecting only one state's resident.

The organization that makes data breach data available, ITRC, states, "we are certain that our ITRC Breach List underreports the problem."[27] Additionally, considering the current statistics about cybercrime and cyber-attacks,[28] it is hardly conceivable that in a year, fewer than 800 data breaches were registered across the United States.[29] According to the survey of about 300 attendees at the RSA Conference, more than 89% of security incidents went unreported in 2007.[30] It is also significant that in dedicated reports such as the 2014 Data breach investigation report,[31] the dataset has been extended to all confirmed security incidents in 2013, more than 63,000 globally, no longer restricting the analysis to confirmed data breaches only.[32]

We focus here only on those breaches known by the affected organization, not entering into the debate regarding the unknown breaches, such as undetected malware, and the measures that could be taken to intercept such events. It is important to distinguish between two possible reasons for not having public evidence of a data breach, known by affected organizations. Either the company decides not to disclose the breach, or the notified parties have no reason or incentive to inform the public about the received notification.[33]

---

27. Identity Theft Resource Center.

28. In 2001, the annual total loss of complaints referred to the Internet Crime Complaint Center (IC3) amounted to approximately 17.8 million US dollars and grew to 781.84 million US dollars in 2013. In 2012, the amount was 581.44 million US dollars. Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2015. Statista 2015.

29. Note that the Maine attorney general only lists data breaches without providing letters for consultation. Maine was therefore not included in the analysis. However, this list allows us to observe that with the addition of a fifth state to the sample there would be additional 62 data breaches, bringing the total to 507 (64.75% of total data breaches then would be covered by 5 states out of 47).

30. Claburn.

31. Verizon.

32. Verizon uses the following definitions: Security incident: Any event that compromises the confidentiality, integrity, or availability of an information asset. Data breach: An incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party.

33. There is also a third reason, but it is a temporary one—notifications may in fact be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security.

Regarding the first point, in the past, the topic of underreporting had been discussed and the input suggested that organizations might prefer to focus on profit margins instead of security of personal data. Therefore, organizations may underreport data breaches, mainly out of concern for their business liability and reputation. Disclosure makes traceable an otherwise untraceable security breach, bringing publicity to an event and perhaps thereby prompting costly legal action or regulatory scrutiny.[34] According to a white paper[35] from ThreatTrack released in 2013, polling 200 security professionals in US enterprises, 57% had experienced a data breach that they did not disclose.

Regarding the second reason, it is clear that companies, once having complied with the legal provision to inform affected consumers, have no incentives to inform media or other third parties about the breach to avoid reputational damages. On the contrary, it is uncertain why attorneys general in fourteen states do not make this information public, even if notified by companies according to the State Data Breach Notification Laws. We could expect a delay in informing the public if investigations are ongoing, but a complete lack of information would have no clear motivation, apart from an additional organizational burden. AG offices would need to properly manage the incoming notification flows and set proper procedure for the letter publication on their websites, possibly increasing the amount of contact with the involved public.

From the percentages highlighted above, those AG offices in the notification loop that do not publicly disclose known data breaches throughout their websites or in other ways may generate a counterproductive limitation of the perception of the issue. In fact, from the presented numbers we can easily assume that in those states where attorneys general do not disclose because they are not in the loop or because they decided not to do so, the media and the other actors mostly fail in identifying and recording those data breaches, even if the customers are notified.

To be more specific, attorneys general can play a decisive role in the emergence of the nonreported data breaches, if supported by the necessary law requirements (government notice requirement) in the first place. It is, however, also a matter of their willingness to foster the visibility of the received data breach notifications. In fact, currently, in twelve states attorneys general prefer not to disclose to the public such information,

34. Schwartz and Janger.

35. ThreatTrack Security.

limiting therefore the effect of the data breach notification laws. A federal law would facilitate such an option, having the opportunity to centrally manage the visibility of the notifications received by the companies and, more generally, would allow for collection of accurate national data breach statistics.

Looking at the Missive Content

The requirements of the laws in the forty-seven states vary from one state to another. These differences generate a significant complexity for organizations dealing with customers residing in multiple states. Unfortunately, there is no single form letter that guarantees compliance with all of these laws and most state breach notification laws do not set out specific requirements for the notice's content.[36] However, an assessment can be performed based on the state breach notification statutes that do set out minimum requirements in order to identify the most frequent elements and therefore could be recommended to include in the letter. Such minimum requirements are determined by fifteen states' legislation out of forty-seven. From the analysis of these legislations, notifications can contain a certain number of mandatory requirements, listed in Table 2.

Bearing in mind that in thirty-two states the content of the missive is not formalized in any way by the data breach notification law in place, we notice in Figure 2 that thirteen states out of fifteen (87%) require the letters to include the type of personal information subject to an unauthorized access or acquisition. A high number of states (80%) require the notifications to specify the reporting entity's name and contact information so that affected individuals can obtain additional information. Only in 60% of the cases do laws require that companies provide consumers with specific information on what has happened (a general description of the breach incident). It is worth noting that general advice on actions that affected individuals should take is mandatory in only four states out of fifteen. Other state legislations have opted for more explicit requirements. Specifically, a statement indicating that individuals can obtain information from specific sources such as the FTC and consumer reporting agencies and a

36. Some organizations opt for filling the gap with an annex, which fulfills case by case each state's legislation.

TABLE 2 Mandatory Elements of Data Breach Notification by State

State	No. of elements included in legislation	
California	7	63.64%
Hawaii	5	45.45%
Illinois	3	27.27%
Iowa	4	36.36%
Maryland	5	45.45%
Massachusetts	2	18.18%
Michigan	5	45.45%
Missouri	5	45.45%
New Hampshire	4	36.36%
New York	2	18.18%
North Carolina	8	72.73%
Oregon	6	54.55%
Vermont	5	45.45%
Virginia	5	45.45%
West Virginia	4	36.36%

reminder of the need to remain vigilant for incidents of fraud and identity theft, are mandatory, respectively, in five and four states.[37]

Only four states made mandatory the specification of the date of the breach, highlighting a controversial aspect of the notification.

If it is true that the Data Breach Notification laws generally serve two purposes, (1) to enable individuals to mitigate against the risks arising from a data breach, particularly in relation to identity theft crimes promoting an individual's *right to know*;[38] and (2) to provide a market-based incentive for the enhancement of organizational information security measures in relation to the protection of personal information, "disinfecting" organizations of shoddy security practices,[39] then the specification of two dates would surely support the achievement of these purposes: the date of the breach and the date of the breach discovery.

37. Table 1 does not include a requirement set in California, where the letter has to specify whether notice was delayed as a result of law enforcement investigation.

38. Schwartz and Janger.

39. Ranger.

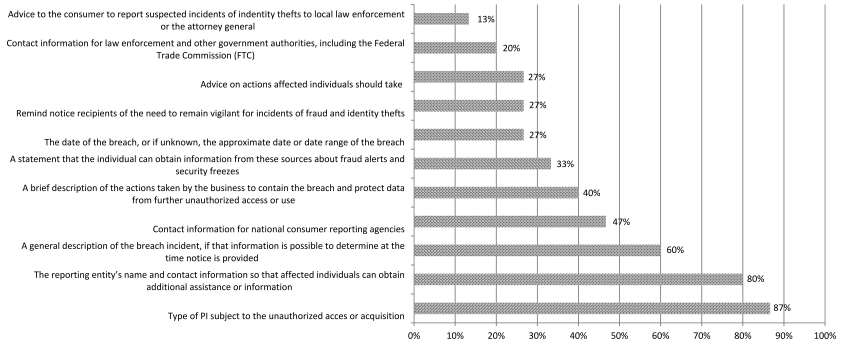


FIGURE 2 Mandatory elements of data breach notification.

The first date is essential in order to support the consumer in evaluating the seriousness of the situation and the need for a prompt reaction. The second date highlights the organization's speed in communicating breaches in a timely manner to consumers. Both dates enable one to assess the organization's capacity to detect breaches. Based on our sample, the situation is as follows: 272 letters out of 445 indicate at least the date of the breach discovery within the organization, while 268 indicate at least the date of the breach or, if unknown, the approximate date or date range of the breach. There are 166 letters that specify both and 70 that specify none.

From the 272 letters in which the time of the event identification is specified, we could calculate the average time in days from the discovery of the event to the moment of the communication to consumers and related medians. We define it as *notification time*, the time the organization needs to assess the situation after breach detection, to finalize the letter, and to activate the necessary communication channels toward customers and other relevant parties (e.g., attorney general, customer credit reporting agencies). The result[40] is 38 days (see Table 3), with only 124 cases under 30 days. The median value is 32.50. From the data presented in Table 3, we notice that some sectors are more reactive than others.

The classification used to record breaches across seven primary industries (Financial and Insurance Services—BSF, Retail/Merchant—BSR, Educational Institutions—EDU, Government and Military—GOV, Healthcare–Medical Providers—MED, Nonprofit—NGO, and Other Business—BSO) supported us in investigating how financial and insurance services and retail/merchant sectors have similar behavior,

40. Once eliminated six outliers according to the z score rule.

TABLE 3 Notification Time

Sectors	Notifications	Average (days)	Over 15 days	Over 30 days	Over 45 days	Over 60 days	Median (days)
Financial and Insurance Services	42	34.19	83.33%	47.62%	19.05%	9.52%	29.00
Other Business	67	34.27	77.61%	47.76%	26.87%	11.94%	28.00
Retail/ Merchant	48	34.92	79.17%	52.08%	27.08%	8.33%	33.00
Educational Institutions	25	50.28	84.00%	64.00%	44.00%	32.00%	41.00
Government and Military	17	41.35	82.35%	47.06%	29.41%	17.65%	28.00
Healthcare–Medical Providers	59	41.51	84.75%	64.41%	44.07%	11.86%	39.00
Nonprofit	8	36.25	87.50%	37.50%	37.50%	25.00%	22.00
Total	**266**	**38.00**	**81.58%**	**53.38%**	**31.58%**	**13.53%**	**32.50**

Types of event	Notifications	Average (days)	Over 15 days	Over 30 days	Over 45 days	Over 60 days	Median (days)
Hacking or Malware	120	39.03	82.50%	52.50%	33.33%	14.17%	32.50
Insider	26	44.92	80.77%	65.38%	38.46%	15.38%	40.50
Payment Card Fraud	2	39.00	100.00%	100.00%	0.00%	0.00%	39.00
Physical Loss, Portable and Stationary Device	46	38.80	89.13%	63.04%	41.30%	13.04%	36.00
Unintended Disclosure	69	32.87	75.36%	42.03%	20.29%	11.59%	28.00
Unknown or Other	3	41.67	66.67%	66.67%	33.33%	33.33%	34.00
Total	**266**	**38.00**	**81.58%**	**53.38%**	**31.58%**	**13.53%**	**32.50**

(*Continued*)

TABLE 3 Notification Time (*Continued*)

PII	Notifications	Average (days)	Over 15 days	Over 30 days	Over 45 days	Over 60 days
SSN	59	35.41	81.36%	49.15%	28.81%	10.17%
Account/ credit card or debit card number	57	34.37	78.95%	50.88%	26.32%	10.53%
Email/ password/ user/ID card number	9	23.00	55.56%	22.22%	11.11%	0.00%
Personal health information	11	31.55	72.73%	54.55%	36.36%	0.00%
SSN and account/ credit card or debit card number	41	38.88	75.61%	39.02%	31.71%	21.95%
Other combinations	89	43.95	89.89%	67.42%	38.20%	16.85%
Total	**266**	**38.00**	**81.58%**	**53.38%**	**31.58%**	**13.53%**

using on average thirty-four days to complete the notification process, while government and military and healthcare–medical providers require forty-one days on average. Educational institutions react even slower (fifty days).

Running a nonparametric *k*-sample test on the equality of medians,[41] we notice that in terms of notification time the *k* samples (six sectors[42]) were drawn from populations with different medians with probability = 0.040 and Pearson chi^2(5) = 11.6503. In case of type of event (4[43]) we have Pearson chi^2(3) = 10.9090 and probability = 0.012.

If we look at the breached personal identifiable information (PII), we notice that the type of PII accessed or acquired does not seem to generate a

41. Shapiro–Wilk W test confirmed that group data (grouped both by sector and type of event), specifically notification time, do not show a normal distribution.

42. NGO sector is not taken into consideration given the limited number of observations (eight).

43. Payment card fraud and others are not taken into consideration given the limited number of observations.

relevant impact on the notification time. In fact, when only social security numbers are accessed the average is thirty days. We find similar values when only bank account, credit, or debit card numbers are the breach target.

Finally, the role of the event in the notification time was investigated. The definition of the type of event is derived by privacyrights.org, which classifies the events that generate notifications as follows: unintended disclosure (sensitive information posted publicly on a website, mishandled, or sent to the wrong party via e-mail, fax, or mail), physical loss (lost, discarded, or stolen nonelectronic records, or portable or stationary devices), insider (someone with legitimate access intentionally breaches information—such as an employee or contractor), hacking and malware (electronic entry by an outside party, malware, or spyware), payment card fraud (fraud involving debit and credit cards that is not accomplished via hacking), and unknown or other (all other cases).

It seems that organizations need more time from the breach discovery to assess the situation and initiate the notification process in case of insider (forty-five days) and less in case of unintended disclosure (thirty-three days). We can assume that this is related to the internal investigation dynamics, very straightforward in case of a human error and more complex in case of fraud.

There are 268 letters that indicate also the date of the breach, in particular, when the generating event took place or started (and so the potential harm). In case of unintended disclosure, this could be when the file has been sent out; in case of insiders this could be the date when the employee might have started his criminal interventions. We define the time between the breach and the notification date and as *uninformed exposure time*. During this period, customers are not aware of the risk they are exposed to and cannot undertake any defensive action. These data reveal a worrying situation. We identified in fact the average of 132 days[44] (see Table 4) between the communication and the day when the potential harm started, with 29% of the cases[45] over three months.

Both a nonparametric *k*-sample test on the equality of medians and a Kruskal–Wallis equality-of-populations rank test were performed on the sectors.[46] The first showed the following result: Pearson $chi^2(5) = 20.0929$ and probability = 0.001, highlighting that the *k* samples (six sectors[47]) were

44. Once eliminated three outliers represented by four insider cases, discovered more than three years after the potential data breach.

45. Information extracted from the created database.

46. Shapiro–Wilk W test confirmed that group data (grouped both by sector and type of event), specifically uninformed exposure time, do not show a normal distribution.

47. NGO sector not taken into consideration given the limited number of observations (eight).

TABLE 4 Uninformed Exposure Time

Sectors	Notifications	Average (days)	Over 30 days	Over 60 days	Over 120 days	Over 180 days	Median (days)
Financial and Insurance Services	49	60.43	55.10%	22.45%	14.29%	10.20%	36.00
Other Business	67	113.60	62.69%	47.76%	25.37%	16.42%	41.00
Retail/ Merchant	58	166.14	87.93%	65.52%	39.66%	27.59%	98.00
Educational Institutions	17	214.41	76.47%	64.71%	47.06%	47.06%	102.00
Government and Military	14	128.07	64.29%	50.00%	35.71%	28.57%	47.50
Healthcare–Medical Providers	56	168.84	83.93%	46.43%	30.36%	21.43%	60.00
Nonprofit	4	29.50	25.00%	25.00%	0.00%	0.00%	21.00
Total	**265**	**132.90**	**71.70%**	**47.55%**	**29.06%**	**21.13%**	**58.00**

Type of event	Notifications	Average (days)	Over 30 days	Over 60 days	Over 120 days	Over 180 days	Median (days)
Hacking or Malware	122	157.38	80.33%	63.11%	37.70%	30.33%	88.50
Insider	24	258.38	83.33%	75.00%	54.17%	33.33%	147.50
Physical Loss, Portable and Stationary Device	55	50.47	58.18%	20.00%	5.45%	3.64%	34.00
Unintended Disclosure	62	112.44	62.90%	32.26%	24.19%	14.52%	36.00
Unknown or Other	2	35.50	50.00%	0.00%	0.00%	0.00%	35.50
Payment Card Fraud	0	-	0.00%	0.00%	0.00%	0.00%	-
Total	**265**	**132.90**	**71.70%**	**47.55%**	**29.06%**	**21.13%**	**58.00**

drawn from populations with different medians. Also, the second test showed that there is a statistically significant difference in uniformed exposure time between the six groups, with $chi^2 = 20.914$ with 5 d.f., probability = 0.0008.

On breach events, results confirm also statistically significant difference with $chi^2 = 40.397$ with 3 d.f.,[48] probability = 0.0001.

48. Payment card fraud and others not taken into consideration given the limited number of observations.

Finally, it is also important to point out the delay between the date of discovery and the start of the potential harm, which can be calculated in 163 cases in which both dates are available. We define it as *breach detection time*. The average amounts to 113.10 days, while specific data breach types show great differences. Table 5 suggests exploring the opportunity to differentiate the approach and regulations according to the data breach type. Notifications sent for data breaches generated by insiders and hacking arrive to customers already late even if sent on the same date of the discovery. The related time span is in fact over six months. On the contrary, data breaches due to physical loss and unintended disclosure could be better addressed by prompt notifications as organizations find out about the data breach more rapidly (in eighteen and seventy-eight days, respectively).

Observation 2: The understanding and open communication of breach detection time, notification time, and the resulting uninformed exposure time is essential to enable consumers reaction and sectoral intervention.

The conducted timing analysis alone shows that the law's first purpose, the right to know, seems not to be suitably served. In fact, the resulting timing poorly matches the individuals' need to defend themselves promptly against potential identity theft. Criminals may use as their advantage the speed of action toward customers, given the late notifying reaction by breached organizations. And the fact that many state statutes do not yet provide minimum mandatory information in terms of the content of the notification provides organizations with elements of discretion that may not always support customers' conscious reactions to the breach.

Additionally, timing information enables sectoral analysis for policy purposes. It could raise company awareness about the risks related to different types of events that generate data breaches and about specific dynamics driven by these events that put customers' data at risk for various periods of time. In fact, as we estimated, in cases of hacking or insiders,

TABLE 5 Breach Detection Time

Type of event	Notifications	Average (days)
Hacking or Malware	71	158.10
Insider	12	249.83
Physical Loss, Portable and Stationary Device	33	17.70
Unintended Disclosure	46	78.33
Unknown or Other	1	26.00
Total	**163**	**113.10**

organizations need at least ninety days more to identify a data breach in comparison to physical loss or unintended disclosure.

Based on the data summarized earlier, Figures 3, 4, and 5 illustrate the different dynamics related to three types of breach generating events (hacking or malware, unintended disclosure, and insider) applied to specific sectors. Specific breach detection time, notification time, and the resulting uninformed exposure time highlight the good performance of the financial sector in comparison to the others but also show how the

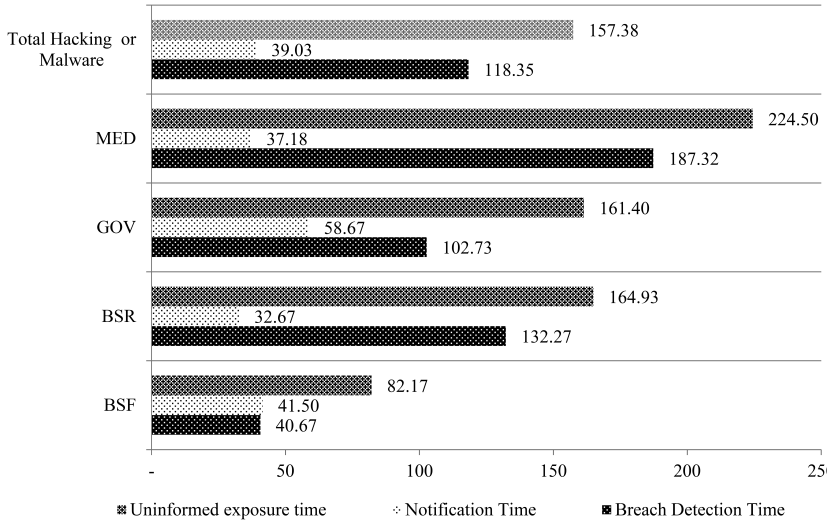


FIGURE 3 Hacking or malware.

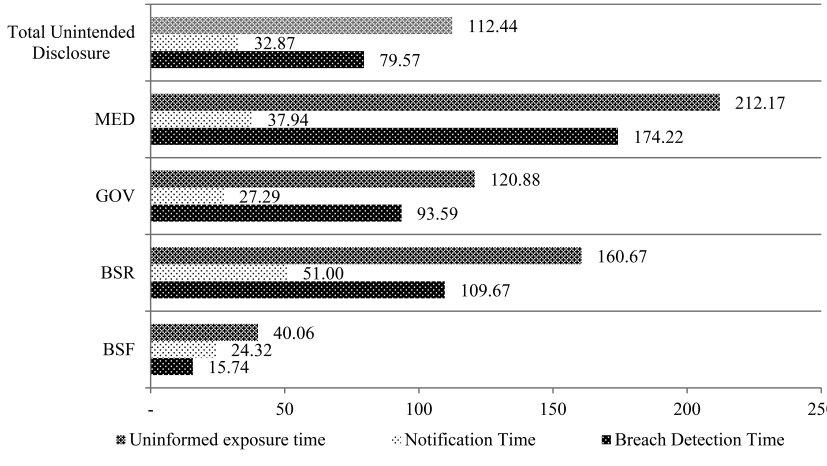


FIGURE 4 Unintended disclosure.

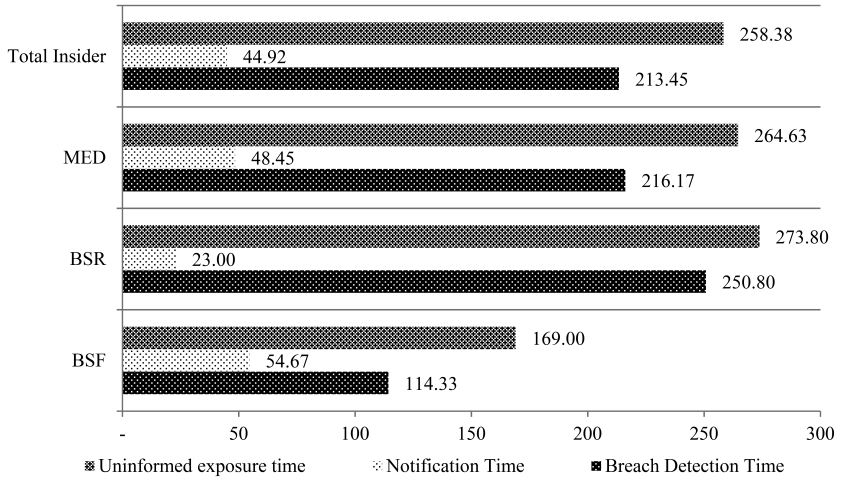


FIGURE 5 Insider.

retail sector is the most reactive once the breach is detected in cases of hacking or malware and in cases of insiders.

The Personal Data Notification & Protection Act, announced by President Obama, does not foresee the mandatory inclusion of any date in the content of the notice to individuals. The consequences could be very relevant, limiting the citizen risk awareness when receiving such a notification.

Looking at the Letter Style

Clearly, the predefined letter elements should make the public notices useful and easy to understand if they aim to be effective, meaning that they should contribute to mitigating the risks driven by an unauthorized and uncontrolled access of customer personal information. In fact, a prompt notification to customers in case of data breaches can help them mitigate the damage caused by information thefts[49] and specifically provide them with the opportunity to take steps to protect themselves from possible identity theft, suggesting placing fraud alerts and activating credit monitoring services.

The form is therefore important to ensure that the right message is sent, sufficient information is provided, and motivational incentives for precautionary actions are given. And the fact that many state statutes do not provide minimum mandatory information to be included in the letter highlights the

49. "Data Breaches and Identity Theft."

poor regulation in place in the different states to guarantee the quality and the appropriateness of the means—the notification—compared to the goal of timely alerting consumers to trigger a prompt reaction against identity thefts and other negative consequences of data breaches.

In the few cases where content is specified by law, some of the mandatory elements cannot be modulated, as they are objective details such as the date or contact information. However, the majority of the components can be calibrated and then resulting in messages with various tones, alarming or reassuring, clarifying or confusing, about the event and its consequences. We now concentrate on those elements and their chosen sequence.

According to Bisogni,[50] the key features that can be identified are four:

1. *Clarity*: Clarity of the incident description and of the PII involved
2. *Tone*: Communication tone on the possible consequences given the organization reaction
3. *Action*: Approach to actions to be taken by the affected customers
4. *Interaction*: Interaction with affected customers

We benefit, therefore, from this previous work that has analyzed in depth how main "conventional" components according to business communication textbooks (such as bad news, explanation, apology, prefatory, and closing buffers) are embedded in these four elements. Therefore, by using this classification we can also take advantage indirectly from the analysis performed by Veltsos on the bad-news traditional components applied to data breach notifications. Specifically on the advice from literature regarding negative messages that tend to focus on low risk, routine situations such as refusing claims or credit, rejecting requests, and making collections.[51] But also on the approaches used when negative news is not about refusals or rejections. In recent years, variations on negative messages have appeared, such as notices of cancelled flights,[52] product recalls,[53] negative policies or organizational news,[54] rate increases and price hikes,[55] and constructive criticism such

50. Bisogni.
51. Carter; Lehman and DuFrene; Oliu, Brusaw, and Alred; Shwom and Snyder.
52. Jansen and Janssen.
53. Shwom and Snyder.
54. Alred, Brusaw, and Oliu; Bovée and Thill; Shwom and Snyder.
55. Guffey and Lowey.

as employee evaluations.[56] Bisogni's and Veltos's research benefits from these previous works in order to investigate the intersection of business communication and information security in the form of breach notification messages.

We applied Bisogni's classification to the letters belonging to the sample providing definitions based on the outcomes of the analysis of a full year of notifications, enabling an analysis that will look at the traditional bad-news literature elements under the perspective of a better communication toward consumers affected by data breaches. Sentences extracted from letters belonging to the sample are provided to support a better understanding of those definitions.

(1) Clarity of the incident description and of breached PII involved (opaque vs. transparent). The decision on how detailed the event description should be and whether to acknowledge therefore organizational or procedural weaknesses of the company depends on the management's evaluation of the legal framework, customer relationships, potential additional harm for the affected customers, and/or the company. Sometimes organizations withhold information out of fear, or to save face. While this may be a natural reaction, withholding information can cause a wrong diagnosis of the actual problem or an underestimation of its extent. When the hidden facts become public, organizations are viewed in a worse light than if all the facts had initially been disclosed.

In order to determine the missive's clarity, there are three levels that can be identified related to the transparency in the event description. The three possible options for transparency are: transparent, transparent no dates, and opaque. In case of the event description, the notification is classified as transparent when it meets at least two out of the following three requirements (the type of event is specified, the generating causes are described, and the organization reaction is indicated) and opaque if it meets only one of the requirements listed above. In case of full transparency, we also look at the presence of the two above mentioned dates (breach discovery date and breach date) labeling as transparent no dates in case none of the dates is indicated.

Here, we present the text of three data breach notifications belonging to the analyzed sample highlighting the possible scenarios to represent the data breach generating event, that is, opaque, transparent, and transparent no dates.

56. Lehman and DuFrene; Locker and Kienzler.

In the letter sent by Experian on July 21, reporting unauthorized access of consumer information, we can recognize an *opaque* description of the event:

> This letter is to inform you that your personal information may have been accessed without proper authorization. This unauthorized access took place sometime between April 15, 2014 and June 27, 2014.
>
> Experian, one of the nationwide credit reporting agencies, identified that its client, NRG Assets LLC, had certain Experian consumer information accessed without proper authorization. The consumer information consists of information typically found in a consumer report. Such information includes your name and address and one or more of the following: Social Security number, date of birth, or account number. Experian is actively working with NRG Assets LLC to investigate this matter. (238)

A *transparent* approach is used by SIMMS in their letter dated November 25, 2014:

> I am writing to inform you of an incident discovered November 6, 2014, involving the theft of personal information from our online store. An unknown criminal installed malware in our online check out system that appears to have intercepted customer purchase information for purchases between September 1 and November 6, 2014. Your name, address, and credit card information, including the credit card number, expiration date, and CVV2 code (Card Verification Value on the back of the card), may have been among the information accessed.
>
> Our website hosting and support vendor has taken the necessary steps to remove the malware and prevent it from being reinstalled. We have reported the incident to and are cooperating with law enforcement. We have also informed the credit reporting agencies and payment card networks about this incident so that they may take appropriate action regarding your credit card account. (398)

Finally, it is possible to be transparent, avoiding giving visibility on the relevant dates (discovery of the breach and start date of potential harm), as Ameriprise financial did in September 2014:

> I am writing to make you aware of an incident that occurred involving your personal information. Recently, my office was broken into

> and the building set on fire. Many client files were damaged due to smoke and water, and the room where kept client files was accessed. It is not known if your information was taken, but your client file would contain your name, address, date of birth, Social Security and account numbers. Due to the sensitive nature of the information, I wanted to notify you of this incident.
>
> We have taken steps to protect your accounts from unauthorized activity, which includes instructing our services associates to use extra caution when verifying caller and to confirm the signature on written requests related to you accounts. (304)

(2) Communication tone in depicting the possible consequences of the data breach (reassuring/neutral/alarming). Options such as downplaying the effects of the data breach may mollify readers' anxiety, but also may discourage them from taking action to protect themselves.[57] According to the type and dimension of the breach, affected organizations have different options when communicating the event to consumers. Some tend to be reassuring about the consequences of the data breach in order to mitigate the short-term reputational effects on customers, particularly on those who ignore the existence of the data breach regulation in place. The reassuring communication tone is driven by expressions that stress the absence of actual harm for customers: *we have no reason to believe, we have no indication, we have no evidence*. The objective of this kind of notification in almost all cases is to underline no current damage and to belittle the potential future harm. In the letter sent by Thomson Reuter on July 7 notifying customers about a security incident involving the misuse of credit card information by an independent contractor, we can identify such a *reassuring tone*:

> Although we have no reason to believe that your personal information was misused by this independent contractor or that any fraudulent activity occurred on your credit card account, your EndNote order was one that this temporary contract processed. Nevertheless, as a precautionary measure, we have arranged to have AllClear ID, an identity theft and credit monitoring company, help protect your identity for 12 months at no cost to you. AllClear maintains an A+ rating at the Better Business Bureau. (215)

57. Veltsos.

The opposite tone could be to *alarm* the customers to foster them to take all the necessary steps to avoid additional negative consequences. The customer will bear part of the cost of the mitigation, but will perceive the company as trustworthy. One example of such approach is the letter sent by UPS dated August 20 informing customers of malware intrusion and highlighting the following:

> Based on the investigation, we feel it is critical to notify our customers of the potential data compromise. (279)

Others use a more *neutral* tone, stressing the uncertainty of current damage (*"we are uncertain," "we do not know"*) while explaining the steps to mitigate any potential consequences. We can find such tone in the notification sent on September 5 by Cedar-Sinai to consumers due to a data breach involving their health information.

> Cedar-Sinai is unaware of any attempted or actual unauthorized access to or misuse of your health information, but has provided information in this letter on additional steps you can take to protect your identity should you feel it appropriate to do so. (305)

(3) Approach to actions to be taken by the affected customers (neutral vs. encouraging). Another decision tree node for the organization is to choose between listing all the possible actions a customer could perform or taking a position and recommending selected actions to individuals. In the latter case the letter could act as an alarm bell for customers, encouraging them to take seriously the content of the notification. The actions that are usually suggested are to report to credit reporting agencies that one may have been a victim of an identity theft, to ask the credit reporting agencies to put a fraud alert on the credit file (also, though rarely, to put a credit freeze on the credit file), to check credit activity regularly with each credit issuer, and to activate a service of credit monitoring at no cost for the individual. In some cases, it is also specified why the organization is not performing those actions itself (*credit agencies will not permit our firm to act on your behalf regarding your credit data*).

When following a *neutral* approach, messages highlight that the company is not in the position (or does not want) to give advice on what to do, or they clearly encourage the individuals to evaluate the situation themselves. In December 2014, Allianz used this approach:

> At this time, we have no reason to believe that your personal information has been or will be misused. However, for your own peace of mind, you may wish to monitor your financial accounts, such as banking, brokerage and insurance statements, for any unusual activity. (439)

The opposite approach is to *encourage* the customer to act to reduce risks with determined expressions as *we would like to urge you to . . ., we believe you should . . ., we encourage you to. . . .* Such expressions were used by Home Depot for the data breach suffered in May 2014:

> We encourage you to review your account to check for any transactions that might reflect improper use of your information. You should immediately report any indication of inappropriate use of your information to your credit card company. Even if you do not see signs of misuse, to be cautious you may want to ask your credit card company to cancel your current card and issue you a new one. (167)

(4) Interaction with affected customers (neutral/available/fostering). Activating communication channels and managing those increases company costs, for support services as call centers, but also for additional costs generated by a higher rate of activated credit monitoring. On the other hand, fostering such contact may limit reputational effects, showing strong willingness in cooperating to avoid negative consequences. While in almost all letters contacts of the breached companies are given in order to provide additional information or help, the style used in offering this opportunity differs from case to case.

When classifying the notifications' tone for interaction we used the following requirements: in the case of the fostering tone there is a strong invitation for action supported with expressions as *we are eager to help* or with contact details in bold letters; availability tone is identified with a standard sentence *please do not hesitate to contact us*; finally, neutral interaction is considered when no contact number is explicitly provided. Here, there are three examples, respectively, of a fostered interaction, of availability, and of a neutral communication of a contact number.

State Industrial Product Corp. *foster* interaction in their communication sent on January 27 by the use of capital letters.

> We take this matter very seriously. We set up a dedicated call center if you have any questions, or you need further assistance. **Please call the**

> **dedicated (not the HR department) at 1.877.218.2561 and enter this reference number: 2702012514.** The call center will be open Monday through Friday, 9:00 AM until 7:00 PM, Eastern Time. (32)

Catamaran highlight *availability* toward interaction in their communication dated February 7, 2014:

> If you notice activity that may be of concern, or if you have any questions or need additional information, please do not hesitate to contact us toll-free at 855-577-6522, 24 hours per day, seven days per week. (47)

Finally, Tinyprints decided to be *neutral* in their data breach notification sent in November 2014:

> For more information and updates, please go to http://www.tinyprints.com/security.htm by typing this address into your browser. (380)

The existence of these elements, more specifically of the options at disposal of the breached organization, shows that companies have specific opportunity to belittle the event and to be law compliant. These elements were analyzed per each of the 445 letters sent in 2014.

Additionally, it is also relevant to look into the sequence used to communicate bad messages. How to interpret such sequences can be studied with the support of the existing research in the field of communicating negative messages. In the field of bad news, the lines of research inquiry and points of contention have centered on arrangement as key aspects of composing and teaching negative news messages.

The order or *arrangement* of components within a negative message has gathered much critical attention and experimentation. The patterns used by organizations in such communications are two, specifically indirect and direct. The first presents an explanation, delivers the bad news, and then closes with an expression of goodwill. The latter opens with the bad news, provides an explanation, and also closes with a statement of goodwill. The indirect or inductive pattern is strongly recommended by most of the authors,[58] who suggest to avoid negative words altogether, highlight how diplomacy and "reader psychology" are fundamental elements in corporate

58. Hynes; Kolin; Alred, Brusaw, and Oliu.

correspondence, and present it as more effective especially if stakes are high.[59] We find the consensus of the textbook authors upon the indirect pattern to be used when the problem is significant or when the reader is likely to be shocked or upset.[60] On the other hand, the fact that the stakes are high may be precisely the driver for using a direct pattern in data breach notifications.[61] Readers must be aware that their PII has been breached and their privacy may be threatened. Placing the bad news in the opening paragraph allows writers to capture the readers' attention immediately and "shake" them into action.[62] The direct pattern clearly provides stronger incentive to continue reading about protective measures. Locker and Kienzler[63] consider this type of directness to be "good ethics and good business."

Here, an example of the two typologies of opening (direct and indirect, respectively), the first one sent by Dreslyn and the latter sent by Liberty Tax.

> Dear [INDIVIDUAL NAME]:
>
> We deeply value your business. Your security is our top priority, which is why, as a precautionary measure, we are writing to inform you of a data security incident that involves your personal information. (250)

> Dear Liberty Tax Customer:
>
> Liberty Tax makes every effort to protect the confidentiality and integrity of our customer's confidential information. The state of Maryland requires that if a business experiences a security breach where personal information that, combined, may pose a threat to a consumer if misused, that business must notify any affected consumers residing in Maryland. Once a security breach is detected, a business must also conduct in good-faith a reasonable and prompt investigation to determine whether the information that has been compromised has been or is likely to be misused, i.e. for identity theft. If the investigation shows that there is a reasonable chance that the data will be misused, that business must notify the affected consumers.

59. Alred, Brusaw, and Oliu.
60. Bovée and Thill; Shwom and Snyder.
61. Veltsos.
62. Lehman and DuFrene, 105.
63. Locker and Kienzler, 437.

> Unfortunately, our office has discovered some tax returns that may have been filed with the IRS and respective states without the consent of the taxpayers. (282)

The combination of the four-letter elements defines the ultimate form of communication toward consumers and the type of message that is received. The decision on the arrangement may provide relevant indication on the willingness to capture the attention of the consumer on the negative event and its consequences.

Observation 3: Data Breach Notification Laws require that organizations contact customers after the discovery of a breach affecting PII; however, they offer poor indications on the style and content of the notification. Even in states where some letter elements are mandatory, companies have a relevant room for maneuver in delivering bad news related to the breach. This opens the possibility to belittle the actual risk and the possible consequences.

Table 6 shows how the previously listed missive components characteristics are represented in the analyzed sample. In most of the cases letters are transparent in describing data breach events and accessed PII, even if, as already reported, in some cases relevant dates are not specified. The performed analysis reveals that most of the organizations decide to describe the event in a very transparent manner. However, it is worth noting that in none of the analyzed letters the number of the breached records is provided: information that could reveal in a very direct way the extent of the breach and therefore the dimension of the company failure in ensuring data security. A neutral tone about the possible consequences of the breach is used in the majority of the cases (60%), and 30% of letters tend to reassure individuals. Organizations do usually show availability toward customers in terms of supporting them in the post-event processes (85.45%), but only a few are really fostering them in making contact with the breached organization (8.54%).

Starting from this sample, it can be observed that the combination of the letter elements defines the ultimate form of communication. We identified the clarity of the event, the tone on the consequences, the action suggested to the reader, and the interaction fostered by the writer as drivers for the letter type identification. Bisogni[64] proposes six letter types according to the combination of these elements that represent different strategies the organization can opt for when drafting the notification letter. Specifically, letter types are classified as follows: (1) Cold, the style is

64. Bisogni.

TABLE 6 Data Breach Notification Main Components

Clarity - Event	Notifications	%	Junk	No worries
Opaque	36	8.09%	√	√
Transparent	354	79.55%		√
Transparent no dates	55	12.36%	√	√
Total	**445**	**100%**		

Tone	Notifications	%		
Alarming	46	10.34%		
Neutral	267	60.00%	√	
Reassuring	132	29.66%		√
Total	**445**	**100%**		

Action	Notifications	%		
Encouraging	219	49.21%		
Neutral	226	50.79%	√	√
Total	**445**	**100%**		

Interaction	Notifications	%		
Available	382	85.84%	√	√
Fostering	38	8.54%		
Neutral	25	5.62%	√	√
Total	**445**	**100%**	**29**	**74**

detached, explaining in a cold and transparent way the facts; (2) Routine, presenting the event as a consequence of an unavoidable and rather common risk; (3) Cooperative, giving emphasis to the actions taken by the organization, while highlighting what actions need to be taken by individuals for their own safeguard; (4) Supportive, even if the tone of the possible consequences of the data breach is reassuring or neutral and the approach to actions to be taken by individuals is neutral, the company prefers anyway to foster the contact with customers; (5) No worries; and (6) Junk.

From the analysis of the sample, we must stress that companies decide to belittle the event in 23.15% of the cases by sending one of the following two letter types:

- No worries letter: This letter emphasizes the minor risk generated by the event, reassuring the affected customer, listing options for the customer's possible actions, but not recommending them. The interaction with

the company is not fostered, given the reassuring tone of the missive about the consequences. Seventy-four letters belong to this group, which includes notifications with the following characteristics: opaque or transparent no dates clarity of the event, neutral tone, neutral action, available, or neutral interaction.

- Junk letter: This letter can be easily exchanged for a junk message and therefore discarded from the moment the envelope is opened. The description of the incident is not clear, or transparent if no dates about the occurrence of the incident and about the discovery date is provided. The communication tone about the possible consequences and the approach to actions to be taken by affected customers is neutral. Twenty-nine letters of the sample belong to this group, which includes notifications with the following characteristics: opaque or transparent or transparent no dates clarity of the event, reassuring tone, neutral action, available or neutral interaction.

Another element of discretion that provides a clear indication on the type on the type of message the company wants to deliver to customers is represented by the use of the Tone element itself and therefore by the decision to reassure consumers on the consequence of the breach. To better analyze this element, we can classify the typology of data breaches according to the assumed decreasing company responsibility for the event.[65] To enable such an exercise, the role of apology was investigated in order to better understand the different options available. We can assume that at its core, an apology is marked by the organization accepting responsibility for the crisis and asking for forgiveness.[66] Consequently, we assume that if a company decides to apologize, then it has admitted its responsibility for the event. We analyzed this aspect at sentence level. Use of expressions such as "we apologize" and "accept our apologies" are coded as Apology, while sentences such as "we are sorry," "we regret," and similar are classified as Regrets. In a few cases, neither apologies nor regrets are offered (labeled as none in Table 7).

The results shown in Table 7 have been translated into three levels of responsibility: *** high level of responsibility with over 50% of use of apologies, ** medium with over 33% of use of apologies, and * low with less

65. Ibid.

66. Benoit and Drew; Fuchs-Burnett.

TABLE 7 Use of Apologies

Type of event	Apology	Regret	None	Total	% Apologies
Payment Card Fraud	8	0	0	***8***	100.00%
Unintended Disclosure	53	37	11	***101***	52.48%
Insider	24	15	7	***46***	52.17%
Physical Loss, Portable and Stationary Device	34	31	9	***74***	45.95%
Hacking or Malware	63	96	51	***210***	30.00%
Unknown or Other	3	3	0	***6***	50.00%
Total	**185**	**182**	**78**	***445***	**41.57%**

than 33%. We can therefore list the data breach causes according to these levels of responsibilities. The results are the following:

1. Payment card fraud: Fraud involving debit and credit cards that is not accomplished via hacking, mostly for mishandling of the information by the personnel of the organization involved.***
2. Unintended disclosure: Sensitive information posted publicly on a website, mishandled, or sent to the wrong party via e-mail, fax, or mail. The human resources' lack of attention and poor process control play often a decisive role.***
3. Insider: Someone with legitimate access intentionally breaches information—such as an employee or a contractor. Lack of control and screening in the recruiting/partnership phase can be seen as one of the reason behind the data breach.***
4. Physical loss: Lost, discarded, or stolen nonelectronic records, portable or stationary device. The security of premises or lack of personnel's attention may facilitate such events.**
5. Hacking and malware: Electronic entry by an outside party, malware, and spyware. Easier to be presented as unavoidable.*

It is worth noticing that in the cases where a company could be more easily identified as ultimately responsible for the data breach, and therefore possibly subject to legal actions, the use of a reassuring tone in letters in order to minimize the problem is present in a high percentage. Specifically, as per Table 8, in 100% of the cases of payment card fraud, 44.55% of the cases for

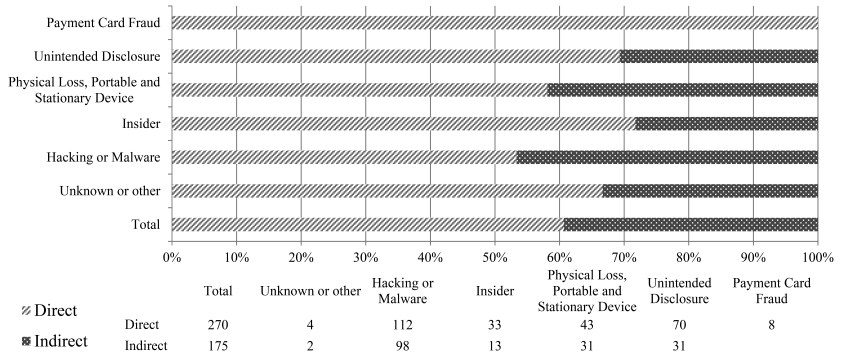
TABLE 8 Tone and Events

Tone vs. Event	Alarming	Neutral	Reassuring	Total	% Reassuring
Payment Card Fraud	0	0	8	***8***	100.00%
Unintended Disclosure	6	50	45	***101***	44.55%
Physical Loss, Portable and Stationary Device	8	36	30	***74***	40.54%
Insider	5	31	10	***46***	21.74%
Hacking or Malware	26	146	38	***210***	18.10%
Unknown or Other	1	4	1	***6***	16.67%
Total	**46**	**267**	**132**	***445***	**29.66%**

unintended disclosure, 40.54% in case of physical loss, 21.74% when the breach is generated by an insider, and 18.10% when hacking or malware.

Finally, we looked into the arrangements, coding the use of direct and indirect patterns in the analyzed sample. We compared the use of the pattern with the outcomes of the related debate in the communications textbooks. The analysis shows (Figure 6) that the need to capture immediately the attention of the readers to foster their action is not in line with the suggestion given by the business communication authors to use indirect pattern in case of quite high stakes, for both the writer and the reader. The rationale behind this is that the stakes may become even higher if the reader is not "shaken" into action. Of the letters, 60.67% show the use of the direct pattern as instrument to overcome optimism bias and rational ignorance. In other words, writers must convince readers that a potential problem exists and encourage them to act, particularly when their action could be useful.

In line with the findings about timing, that highlight how in cases of hacking or malware the time span between the data breach and the notification shows a conspicuous delay, the direct approach is used in the lowest percentage (53.33% vs. 47.67% indirect) in cases of hacking or malware. There is probably no urgency to capture the attention of the reader in order to foster his/her reaction if the event has happened more than three months before the notification. In case of payment card fraud or unintended disclosure, the percentages indicating the use of the direct approach are consistently higher (100% and 69.31%, respectively). This let



	Total	Unknown or other	Hacking or Malware	Insider	Physical Loss, Portable and Stationary Device	Unintended Disclosure	Payment Card Fraud
Direct	270	4	112	33	43	70	8
Indirect	175	2	98	13	31	31	

FIGURE 6 Direct and indirect patterns.

us reflect about the fact that companies may consciously decide to use the direct approach when they feel it is useful given the short detection time, while they may opt more frequently for the indirect approach when they are aware it is already too late for consumers to protect themselves against the consequences of data breaches.

To sum up, clearly, organizations exploit the fact that many state statutes do not yet provide minimum mandatory information in terms of the content of the notification, providing them with elements of discretion. Companies often use such elements in order to limit eventual reputational damage or short-term additional costs given by the activation and management of communication channels (e.g., call centers, but also possible higher rate of activated credit monitoring). Organization's discretion may not always support customers' conscious reactions to the breach. And the results of such "flexibility" can produce non-optimal effects for the society.

For sure the notice-based approach of the state breach notification statutes in the United States represents an important step toward increasing a widespread corporate culture toward data security. The fear of reputational sanction is in fact an important motivator, and recognizing its value, it is important to limit any easy "way out" for companies. But consumers may not open notification letters or act on their information because they are already overwhelmed by communications from commercial entities and the letters themselves do not convey their content effectively. As such, the letters as currently constituted may not provide particularly useful information about a company's security practices, or about the steps customers should take to protect themselves from harm.

A federal law represents a unique opportunity to regulate the content and way letters may convey the content properly, and we would therefore

recommend the following use of the above mentioned notification elements for the interest of consumers:

- *Full transparency* on the clarity of the incident description and of breached PII involved indicating also the number of consumers affected by the breach to allow consumers to self-evaluate the size of the breach.[67]
- *Avoidance of a reassuring tone* in depicting the possible consequences of the data breach, not attempting to sugar coat the consequence, which could represent an incentive for consumers not to act in any way.
- *Clear recommendation* to the affected customers to perform necessary actions to belittle breach-related risks. This may include encouraging them to carefully review bank and credit card statements, activate credit monitoring and credit freeze services, and so on.
- To *foster interaction* with affected consumers by highlighting full company availability in supporting involved individuals and in clarifying possible unclear aspects of the notification and of the breach.

By ensuring or fostering such options related to the four letter elements, companies will have less room for maneuver in drafting notifications and will support consumers in better engaging themselves in post-breach self-protection.

Conclusions

If it is true that the Data Breach Notification laws generally serve two purposes: (1) to enable individuals to mitigate against the risks arising from a data breach particularly in relation to identity theft crimes promoting an individual's *right to know*,[68] and (2) to provide a market-based incentive for the enhancement of organizational information security measures in relation to the protection of personal information, "disinfecting" organizations of shoddy security practices.[69] The data presented above provide insights on the actual achievement of these objectives contributing to the ongoing discussion on the federal law on data breach notifications, highlighting limitations and effects of the already implemented state laws.

---

67. Based on the letter sample analyzed, this information is never reported in the notification letters to consumers but is often present in the notification letter to the attorney general sent in the same time frame, indicating a clear intention of the firms not to disclose such element.

68. Schwartz and Janger.

69. Ranger.

The analysis presented was performed following an innovative approach not based on the traditional investigation about data breach trends or evaluation of data breach costs, but it leveraged the vast dataset represented by the data breach notifications themselves. The research was feasible thanks to the letters made available by four attorneys general offices out of forty-seven. In order to reinforce the role of information disclosure against misaligned incentives and information asymmetries, such visibility should not only be limited to California, Maryland, New Hampshire, and Vermont. In case of implementation of the federal data breach law, we could expect a much higher number of notifications made public, fostering the emergence of "hidden" notifications. This would also support a more precise estimation of the number of breaches. Awaiting the developments related to the federal law, those states in which attorneys general already are in the communication loop when notifications are issued could greatly contribute by making these notifications available. This would also support the second goal of the data breach notification laws, to act as sunlight as disinfectant. Additionally, this could produce not only better analysis of the phenomenon, but also help to investigate more deeply the different causes for the statistical mismatch between data breach and cybercrime trends and magnitude.

Concerning the timing of breach detection, notification drafting, and therefore of uninformed exposure, it is first of all essential to have the knowledge of their actual magnitude. In order to do so, we suggest that in the notifications made by breached organizations toward consumers and relevant authorities the specification of both dates would be mandatory. The analysis of such information makes it possible to study sectoral dynamics, which are generated by the different typologies of events, aiming at a better prevention and response in case of a data breach. In fact, we noticed that organizations belonging to certain sectors are significantly slower in reacting after the breach discovery. Relevant differences in the breach detection capability in various industries should be taken into consideration.

Regarding the content of the missive, the number of states that have law provisions requiring a minimum set of elements to be specified in the notifications is low. The consequence is that consumers must fully rely on the letter style of the breached organizations to understand the seriousness of the situation and to be adequately alerted about the breach. But organizations might rather prefer to focus on profit margins instead of security of personal data, using the given room of maneuver in order to belittle the event or to reassure consumers, safeguarding their breach ex post costs in the short term. For sure, extensive mandatory elements regarding the content of notice to individuals should be dictated by the data breach

notification laws. If we look at the pending Personal Data Notification & Protection Act, a foundation of the possible forthcoming federal law, we notice that only three elements are mandatory, that is, a description of the categories of sensitive personally identifiable information accessed or acquired, a toll-free number to contact the business entity or the agent of the business entity from which the individual may learn what types of sensitive personally identifiable information the business entity maintained about that individual, and the toll-free contact telephone numbers and addresses for the major credit reporting agencies. Such light restrictions in communicating the breach will enable companies to manage almost independently the level of alert communicated to the consumer, not safeguarding the latter.

Given the current framework, it seems that data breach notification laws serve more as sunlight as disinfectant in the medium to long run than as effective and prompt response for identity thefts. The reassuring tone, underreporting, and time spans analysis demonstrate that businesses cannot work without strict supervision in this arena. Mandatory data breach notifications, control on their content and timing, together with associated penalties for non-compliance, are fundamental pillars for more responsible data management practices, responding to the right to know and sunlight as disinfectant principles. The implementation of a federal law or ad hoc reviews of state laws that can define stricter rules and better control on the described elements, particularly on the date of notification and on mandatory elements, represent two clear options to reinforce the effects of the current legislative framework toward a better safeguard against identity theft. Apart from specific features that a state or a federal data breach notification law can present, the relevant added value of the federal solution can be derived from the illustrated analysis. A federal law would provide uniform indications to consumers and companies, helping to solve the issues related to the current patchwork of data breach notification laws. In fact, in case of breaches affecting different states' residents, the current patchwork results in a notification system that is challenging for companies to navigate. This increases the consumer risk of remaining unprotected. Federal data breach notification legislation would represent an opportunity to provide standardization. Replacing the current mix of state laws with a single comprehensive federal law would enhance response time of firms by having equal and clear steps to follow after a breach. Time consuming cross state analysis to answer questions regarding what information is covered and when

and how notification must be provided would not be necessary anymore. Finally, a federal approach would allow centralizing data collection, enabling to develop and maintain accurate national data breach statistics to monitor the dynamics of the phenomenon and to promptly react by means of audit, penalties, or legislative revisions.

BIBLIOGRAPHY

Acquisti, Alessandro, Allan Friedman, and Rahul Telang. "Is There a Cost to Privacy Breaches? An Event Study." Paper presented at the fifth workshop on the Economics of Information Security, University of Cambridge, England, June 2016.

Alred, Gerald J., Charles. T. Brusaw, and Walter E. Oliu. *The Business Writer's Handbook*. Boston: Bedford/St. Martin's, 2011.

BakerHostetler. "State Data Breach Statute Form." 2014. http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf.

Benoit, William L., and Shirley Drew. "Appropriateness and Effectiveness of Image Repair Strategies." *Communication Reports* 10 (1997): 153–63.

Bisogni, Fabio. "Data Breaches and the Dilemmas in Notifying Customers." WEIS 2015: 14th Workshop on the Economics of Information Security, June 2015.

Bovée, Courtland L., and John V. Thill. "Writing Negative Messages." In *Business Communication Today*. 11th ed., 180–208. Upper Saddle River, NJ: Prentice Hall, 2012.

California Civil Code § 1729.98(a).

Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb., and Lei Zhou. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market." *Journal of Computer Security* 11 (2003): 431–48.

Carter, Carol. "Negative Messages." In *Keys to Business Communication: Success in College, Career, and Life*, 208–35. Upper Saddle River, NJ: Prentice Hall, 2012.

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers." *International Journal of Electronic Commerce* 9 (2004): 70–104.

Census Brief. "Population Distribution and Change: 2000 to 2010." 2010.

Claburn, Thomas. "Most Security Breaches Go Unreported." *Dark Reading*. 2008. http://www.darkreading.com/attacks-and-breaches/most-security-breaches-go-unreported/d/d-id/1070576.

CLLA. "Data Breach Notification Laws by State." 2012. http://www.clla.org/documents/breach.xls.

"Data Breaches and Identity Theft." Prepared statement of the Federal Trade Commission before the Committee on Commerce, Science and Transportation. US Senate 109th Congress, 2005.

Economic Census. 2012. http://www.census.gov/econ/census/.

Edwards, Benjamin, Steven Hofmeyr, and Stephanie Forrest. "Hype and Heavy Tails: A Closer Look at Data Breaches." WEIS 2015: 14th Workshop on the Economics of Information Security, June 2015.

Fuchs-Burnett, Taryn. "Mass Public Corporate Apology." *Dispute Resolution Journal* 57, no. 3 (2002): 26–32.

Guffey, Mary Ellen, and Dana Lowey. *Business Communication: Process and Product*. 7th ed. Mason, OH: South-Western/Cengage Learning, 2011.

Hynes, Geraldine E. "Routine Messages." In *Managerial Communication: Strategies and Applications*. 4th ed., 99–125. Columbus, OH: McGraw-Hill, 2008.

Identity Theft Resource. "2014 Data Breach Reports." 2014.

Identity Theft Resource Center (ITRC). "Data Breaches." 2016. http://www.idtheftcenter.org/id-theft/data-breaches.html.

Jansen, Frank, and Daniel Janssen. "Explanations First: A Case for Presenting Explanations Before the Decision in Dutch Bad-News Messages." *Journal of Business and Technical Communication* 25, no. 1 (2011): 36–67.

Joerling, Jill. *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data, 32 Wash*. U. J. L. & Pol'y 467. 2010, http://openscholarship.wustl.edu/law_journal_law_policy/vol32/iss1/14.

Ko, Myung, and Carlos Dorantes. "The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation." *Journal of Information Technology Management* 17 (2006): 13–22.

Kolin, Philip C. *Successful Writing at Work*. Boston: Houghton Mifflin, 2007.

Kwon, Juhee, and Eric Johnson. "The Market Effect of Healthcare Security: Do Patients Care about Data Breaches?" WEIS 2015: 14th Workshop on the Economics of Information Security, June 2015.

Laube, Stefan, and Rainer Böhme. "The Economics of Mandatory Security Breach Reporting to Authorities." WEIS 2015: 14th Workshop on the Economics of Information Security, June 2015.

Lehman, Carol M., and Debbie M. DuFrene. "Delivering Bad-News Messages." In *BCOM*. 3rd ed., 110–29. Mason, OH: South-Western/Cengage Learning, 2012.

Locker, Kitty O., and Donna S. Kienzler. "Delivering Negative Messages." In *Business and Administrative Communication.* 9th ed., 286–321. New York: McGraw-Hill/Irwin, 2010.

Mintz Levin. State Data Security Breach Notification Laws. 2012. http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf.

Oliu, Walter E., Charles T. Brusaw, and Gerald J. Alred. "Writing Business Correspondence." In *Writing that Works: Communicating Effectively on the Job.* 9th ed., 320–52. Boston: Bedford/St. Martins, 2009.

Perkins. Security Breach Notification Chart. 2013, http://www.perkinscoie.com/files/upload/LIT_09_07_SecurityBreachExhibits2.pdf.

Personal Data Notification & Protection Act. http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf.

Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (Sen. Leahy).

Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (Sen. Blumenthal).

Pike, George H. "Legal Issues: Data Breaches Top the Agenda at RSA Conference." *Information Today* 25, no. 6 (2008): 19.

Ponemon Institute, LLC. "2014 Cost of Data Breach Study: Global Analysis." 2014.

Ranger, Steve. "Data Breach Laws Make Companies Serious about Security." September 3, 2007. Silicon.com. http://management.silicon.com/itdirector/0,39024673,39168303,00.htm?r=1.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. "Do Data Breach Disclosure Laws Reduce Identity Theft?." *Journal of Policy Analysis and Management* 30, no. 2 (2011): 256–86.

Sasso, Brendan. "Why Businesses Love Obama's Push for Security Regulation." *National Journal* (January 2015). http://www.nationaljournal.com/tech/why-businesses-love-obama-s-push-for-security-regulation-20150112.

Schwartz, Paul, and Edward Janger. "Notification of Data Security Breaches." *Michigan Law Review* 105, no. 913 (2007).

Shwom, Barbara G., and Lisa G. Snyder. "Communicating Bad-News Messages." In *Business Communication: Polishing Your Professional Presence*, 212–45. Upper Saddle River, NJ: Prentice Hall, 2012.

Steptoe. Data Breach Notification Chart 2015. Comparison of US State and Federal Security Breach Notification Laws—Current through May 26, 2015.

Telang, Rahul, and Sunil Wattal. "An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price." *IEEE Transactions on Software Engineering* 33 (2007): 544–57.

ThreatTrack Security. "Malware Analysts Have the Tools to Defend Against Cyber-Attacks, But Challenges Remain." White Paper. November 2013.

Veltsos, Jennifer R. "An Analysis of Data Breach Notifications as Negative News." *Business Communication Quarterly* 75, no. 2 (2012): 192–207.

Verizon. "2014 Data Breach Investigations Report." 2014.

ATTORNEY GENERAL WEBSITES ACCESSED FOR NOTIFICATION DOWNLOADS

https://oag.ca.gov/ecrime/databreach/list
http://www.oag.state.md.us/idtheft/businessGL.htm
http://doj.nh.gov/consumer/security-breaches/
http://www.atg.state.vt.us/issues/consumer-protection/privacy-and-data-security/vermont-security-breaches.php
http://www.maine.gov/ag/consumer/identity_theft/

LETTERS DOWNLOADED FOR STATISTICS

1. East West Bank—02 January 2014
2. Erie Insurance—02 January 2014
3. T-Mobile—02 January 2014
4. Unicef letter to Consumers re Security Breach—06 January 2014
5. Customer Notice Final Generic version—06 January 2014
6. AHS letter to Consumers re Security Breach—06 January 2014
7. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—07 January 2014
8. Experian—07 January 2014
9. Lafarge West, Inc.—07 January 2014
10. Straight Dope LLC—09 January 2014
11. Barry University letter to Consumers re Security Breach—10 January 2014
12. Edgepark letter to Consumers re Security Breach—13 January 2014
13. Update Legal—13 January 2014
14. Apex Systems, Inc.—14 January 2014
15. Genworth—15 January 2014
16. Easton Bell Sports letter to Consumers re Security Breach—16 January 2014
17. Burlington letter to Consumers re Security Breach—16 January 2014

18. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—16 January 2014
19. TD Bank—16 January 2014
20. Vermont Health Connect—17 January 2014
21. Neiman Marcus letter to Consumers re Security Breach—17 January 2014
22. Dartmouth Hitchcock letter to Consumers re Security Breach—20 January 2014
23. Complete Medical Homecare—21 January 2014
24. PCC Structurals—21 January 2014
25. Discover letter to Consumers re Security Breach—22 January 2014
26. Sidney Regional Medical Center—22 January 2014
27. MilCo Enterprises, Inc. DBA EasyDraft—22 January 2014
28. Focus on Surety LLC DBA Suretegrity—22 January 2014
29. Coca Cola letter to Consumers re Security Breach—23 January 2014
30. W. J. Bradley Mortgage Capital, LLC—23 January 2014
31. TD Bank letter to Consumers re Security Breach—24 January 2014
32. State Industrial letter to Consumers re Security Breach—27 January 2014
33. Michaels letter to Customers re Security Breach—27 January 2014
34. Bring it To Me, LLC—29 January 2014
35. Tribeca Film Institute—30 January 2014
36. Intuit—30 January 2014
37. Beebe Healthcare—31 January 2014
38. Neilsen letter to Consumers re Security Breach—03 February 2014
39. University of California Davis Medical Center—03 February 2014
40. Greenleaf Book Group, LLC—03 February 2014
41. Bank of the West—05 February 2014
42. K. Min Yi, M.D. General Surgery—05 February 2014
43. St. Joseph Health System—05 February 2014
44. Mimeo.com—05 February 2014
45. San Francisco Airport letter to Consumers re Security Breach 1—07 February 2014
46. Easter Seal Society of Superior California—07 February 2014
47. Catamaran—07 February 2014
48. Farmers and Merchants Trust Company of Chambersburg—07 February 2014
49. Mymatrixx—07 February 2014
50. Home Depot letter to Consumers re Security Breach—10 February 2014
51. The Freeman Company—10 February 2014
52. 80s Tees letter to Consumer re Security Breach—11 February 2014
53. Embassy suites—11 February 2014
54. Fresenius Medical Care—11 February 2014
55. TD Bank—11 February 2014
56. Zevin Asset Mgmt letter to Consumer re Security Breach—13 February 2014
57. MSPCC letter to Consumers re Security Breach—13 February 2014
58. Carmike Cinemas, Inc.—13 February 2014
59. Experian letter to Consumers re Security Breach—14 February 2014
60. Rubin Lublin, LLC—14 February 2014
61. TD Bank Security Breach Notice—18 February 2014
62. Blue Shield of California—18 February 2014
63. John Hancock Life & Health Insurance Company—18 February 2014
64. Department of Resources Recycling and Recovery—20 February 2014
65. Discover Financial Services—21 February 2014
66. Alaska Communications letter to Consumer re Security Breach—24 February 2014

67. Merrill Lynch Wealth Management—24 February 2014
68. DST Systems, Inc.—24 February 2014
69. eScreen, Inc.—25 February 2014
70. The Variable Annuity Life Insurance Company—26 February 2014
71. Mkenna Long & Aldridge—26 February 2014
72. Smucker letter to Consumers re Security Breach—27 February 2014
73. L.A. Care Health Plan—27 February 2014
74. ProAssurance Mid-Continent Underwriters, Inc.—27 February 2014
75. Sands Casino letter to Consumers re Security Breach—28 February 2014
76. AppleCare Insurance Services, Inc.—28 February 2014
77. Digia USA, Inc.—28 February 2014
78. ThermoFisher—28 February 2014
79. Capital One letter to Consumers re Security Breach—03 March 2014
80. Timken Co letter to Consumers re Security Breach—03 March 2014
81. Assisted Living Concepts LLC Security Breach Notice—03 March 2014
82. St. Joseph Health—03 March 2014
83. Equifax—03 March 2014
84. EMC—03 March 2014
85. Eureka Internal Medicine—04 March 2014
86. Assisted Living Concepts Notice—05 March 2014
87. Oak letter to Consumers re Security Breach—06 March 2014
88. OANDA letter to Consumers re Security Breach—12 March 2014
89. UCSF Family Medicine Center at Lakeshore—12 March 2014
90. Silversage Advisors—13 March 2014
91. USAA letter to Consumers re Security Breach—17 March 2014
92. Arcadia Health Services, Inc. d/b/a Arcadia Home Care & Staffing—17 March 2014
93. Shelburne Country Store Notice to Consumers—18 March 2014
94. Auburn University letter to Consumers re Security Breach—19 March 2014
95. Discover letter to Consumers re Security Breach—20 March 2014
96. Marian Regional Medical Center—20 March 2014
97. Sorenson letter to Consumers re Security Breach—21 March 2014
98. Castle Creek Properties, Inc., dba Rosenthal the Malibu Estates—21 March 2014
99. Human Resource Advantage—21 March 2014
100. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—25 March 2014
101. RBS—25 March 2014
102. Palomar Health—28 March 2014
103. ITHAKA—31 March 2014
104. RK Internet—31 March 2014
105. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—01 April 2014
106. Susquehanna Health—01 April 2014
107. Kaiser Permanente Northern CA Department of Research—02 April 2014
108. California Department of Corrections and Rehabilitation—02 April 2014
109. American Health Information Management Association (AHIMA)—02 April 2014
110. Citibank, N.A.—02 April 2014
111. Cole Taylor Bank—03 April 2014
112. Sutherland Healthcare Solutions—03 April 2014
113. Logos Management Software, LLC—03 April 2014
114. Parallon—03 April 2014

115. Deltek letter to Consumer re Security Breach—07 April 2014
116. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—07 April 2014
117. City of Crossville, Tennessee—07 April 2014
118. FujiFilm—07 April 2014
119. CRL letter to Consumer re Security Breach—08 April 2014
120. StumbleUpon, Inc.—08 April 2014
121. LaCie USA—11 April 2014
122. Society for Science & the Public—11 April 2014
123. Wilshire Mutual Funds letter to Consumers re Security Breach—14 April 2014
124. Mid Atlantic Professionals, Inc. DBA SSI—14 April 2014
125. Blue Cross and Blue Shield of Kansas City, Inc.—16 April 2014
126. Discover letter to Consumers re Security Breach—17 April 2014
127. Michaels press release re Security Breach—17 April 2014
128. VFW letter to Consumers re Security Breach—21 April 2014
129. NCO FinancialRevSpring, Inc. letter to Consumers re Security Breach—22 April 2014
130. Snelling letter to Consumers re Security Breach—22 April 2014
131. Johns Hopkins University (Identity Theft)—22 April 2014
132. Seattle University—22 April 2014
133. Larsen Dental Care—22 April 2014
134. L Brands, Inc.—23 April 2014
135. JCM Partners letter to Consumer re Security Breach—24 April 2014
136. Westlife Distribution USA, LLC—24 April 2014
137. CCC letter to Consumer re Security Breach—25 April 2014
138. Willis North America letter to Consumers re Security Breach—25 April 2014
139. Central City Concern—25 April 2014
140. Federal Home Loan Mortgage Corporation (Freddie Mac)—25 April 2014
141. Seterus—29 April 2014
142. Boomerang Tags—30 April 2014
143. UMass Memorial MC ltrt Consumer (Redacted) re Security Breach—05 May 2014
144. ground(ctrl)—05 May 2014
145. Maschino, Hudelson & Associates—05 May 2014
146. Department of Child Support Services—06 May 2014
147. 2014 Gingerbread Shed letter to Consumer re Security Breach—07 May 2014
148. Green's Accounting—07 May 2014
149. Mercer HR Services, LLC—07 May 2014
150. Entercom Portland, LLC—07 May 2014
151. PREIT—08 May 2014
152. Lowes letter to Consumer re Security Breach—12 May 2014
153. Santander Bank, N. A.—12 May 2014
154. Hubbard-Bert, Inc.—13 May 2014
155. University of California Irvine—14 May 2014
156. Precision Planting LLC—14 May 2014
157. Discover letter to Consumers re Security Breach—16 May 2014
158. Affinity Gaming—19 May 2014
159. Paytime Harrisburg, Inc. d/b/a Paytime, Inc.—21 May 2014
160. Hanover Foods Corporation—21 May 2014
161. CoreLogic Saferent—21 May 2014
162. Experian letter to Consumer re Security Breach—22 May 2014
163. San Diego State University—22 May 2014

164. CenturyLink—22 May 2014
165. Ebay—22 May 2014
166. Power Equipment Direct Security Breach Notice to Consumers—23 May 2014
167. The Home Depot, Inc.—23 May 2014
168. AutoNation (Ford White Bear Lake) letter to Consumers re Security Breach—26 May 2014
169. Placemark Investments, Inc.—27 May 2014
170. Walgreen Co.—27 May 2014
171. Service Alternatives, Inc.—27 May 2014
172. SHARPER FUTURE—28 May 2014
173. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—29 May 2014
174. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—02 June 2014
175. Kimpton—02 June 2014
176. Gordon Feinblatt LLC—02 June 2014
177. Rowan Companies, Inc.—02 June 2014
178. Craftsman Book Company—03 June 2014
179. National Credit Adjusters letter to Consumers re Security Breach—05 June 2014
180. College of the Desert—09 June 2014
181. AT&T Mobility, LLC—10 June 2014
182. Stanford Federal Credit Union—11 June 2014
183. Santa Rosa Memorial Hospital—12 June 2014
184. The Union Labor Life Insurance Company—12 June 2014
185. Ullico, Inc.—12 June 2014
186. AirBorn letter to Consumers (Redacted) re Security Breach—13 June 2014
187. Riverside Community College District—13 June 2014
188. Fidelity National Financial, Inc.—13 June 2014
189. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—16 June 2014
190. David Stanley Dodge—16 June 2014
191. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—17 June 2014
192. Specialized Eye Care—17 June 2014
193. The Metropolitan Companies, Inc. letter to Consumers re Security Breach—18 June 2014
194. Bell Nursery USA, LLC—18 June 2014
195. Papa John's USA, Inc.—19 June 2014
196. Excelitas—19 June 2014
197. Rady Children's Hospital-San Diego—20 June 2014
198. University of California, Washington Center (UCDC)—20 June 2014
199. Primerica—20 June 2014
200. Montana Department of Public Health Human Services letter to Consumers re Security Breach—23 June 2014
201. Safety First—Non MA Notice Template with data elements—23 June 2014
202. MileOne letter to Consumers re Security Breach—23 June 2014
203. Giant Eagle letter to Consumer re Security Breach—23 June 2014
204. Riverside County Regional Medical Center—24 June 2014
205. Butler University letter to Consumers re Security Breach—26 June 2014
206. Sterne, Agee & Leach, Inc.—26 June 2014
207. Legal Sea Foods letter to Consumers re Security Breach—27 June 2014
208. Benjamin F Edwards letter to Consumer re Security Breach—27 June 2014

209. Record Assist letter to Consumers—27 June 2014
210. Invest Financial Corporation—27 June 2014
211. Baltimore School of Massage Therapy—27 June 2014
212. Seterus—27 June 2014
213. Dennis East International, LLC—30 June 2014
214. P.F. Chang's—01 July 2014
215. Thomson Reuters—01 July 2014
216. Wayneburg University—02 July 2014
217. Black Mountain Software—03 July 2014
218. Montana Department of Public Health and Human Services—03 July 2014
219. Watermark Retirement Communities, Inc.—03 July 2014
220. Jiffy Lube—07 July 2014
221. ABM Parking Services, Inc.—08 July 2014
222. AECOM Technology Corporation—08 July 2014
223. Heartland Automotive Services Inc.—08 July 2014
224. TotalBank letter to Consumer re Security Breach—09 July 2014
225. Park Hill School District—10 July 2014
226. Department of Managed Health Care—11 July 2014
227. Davidson Hotel Company LLC d/b/a Davidson Hotels & Resorts—14 July 2014
228. City of Encinitas 7 San Dieguito Water District—15 July 2014
229. Freshology, Inc.—15 July 2014
230. Bank of the West—16 July 2014
231. Bay Area Pain Medical Associates—16 July 2014
232. United Air Temp Conditioning & Heating, Inc.—16 July 2014
233. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—17 July 2014
234. Bank of America—17 July 2014
235. Seattle University—17 July 2014
236. Archdiocese of Portland Ltrt Consumer re Security Breach—18 July 2014
237. Blue Cross Blue Shield of Michigan—18 July 2014
238. Experian letter to Consumer re Security Breach—21 July 2014
239. NRG Assets LLC—21 July 2014
240. Vermont Office of Professional Responsibility Ltrt Consumer—22 July 2014
241. Discover letter One to Consumers re Security Breach—23 July 2014
242. Washington National Insurance Company—23 July 2014
243. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—25 July 2014
244. Managed Med, A Psychological Corporation—25 July 2014
245. NorthShore University Healthsystem—25 July 2014
246. Self Regional Healthcare—25 July 2014
247. Backcountry Gear—28 July 2014
248. Seattle University—28 July 2014
249. Northern Trust—29 July 2014
250. Dreslyn—30 July 2014
251. Lasko Group, Inc.—30 July 2014
252. Oppenheimer Funds letter to Consumers re Security Breach—30 July 2014
253. Reading Partners—30 July 2014
254. The Houstonian Hotel, Club, and Spa—30 July 2014
255. Chicago Yacht Club—31 July 2014
256. Recreational Equipment, Inc.—31 July 2014

257. Signal Outdoor Advertising, LLC—01 August 2014
258. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—04 August 2014
259. Crothall Services Group—04 August 2014
260. Test Effects, LLC—04 August 2014
261. Vibram USA, Inc.—05 August 2014
262. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—06 August 2014
263. Jersey City Medical Center letter to Consumer re Security Breach—06 August 2014
264. Polish Falcons of America—06 August 2014
265. The Dreslyn letter to Consumer re Security Breach—06 August 2014
266. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—07 August 2014
267. Anderson & Murison—07 August 2014
268. Harry Barker letter to Consumers re Security Breach—07 August 2014
269. San Mateo Medical Center—07 August 2014
270. Diatherix Laboratories—08 August 2014
271. St. Francis College letter to Consumers re Security Breach—08 August 2014
272. Freedom Management Group, LLC dba The Natural—12 August 2014
273. Kleiner Perkins Caufield & Byers—12 August 2014
274. The Natural letter to Consumers re Security Breach—14 August 2014
275. Hatchwise.com or eLogoContest.com letter to Consumer re Security Breach—18 August 2014
276. MeeTMe, Inc.—18 August 2014
277. Community Health Systems Professional Services Corporation—20 August 2014
278. M&T Bank—20 August 2014
279. The UPS Store, Inc. on behalf of 51 franchised center locations—20 August 2014
280. Ascensus, Inc.—21 August 2014
281. George Mason letter to Consumer (Redacted) re Security Breach—22 August 2014
282. Liberty Tax—22 August 2014
283. Bimbo Bakeries USA letter to Consumers re Security Breach—26 August 2014
284. Geekface LLC—26 August 2014
285. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—27 August 2014
286. ClamCase LLC letter to Consumer re Security Breach—28 August 2014
287. Xerox State Healthcare, LLC—28 August 2014
288. AB Acquisition LLC (Shaw's)—29 August 2014
289. AltaMed Health Services Corporation—29 August 2014
290. Bartell Hotels—29 August 2014
291. Department of Social Services—29 August 2014
292. LPL Financial LLC—29 August 2014
293. Goodwill Industries International—02 September 2014
294. Goodwill Industries of Sacramento Valley and Northern Nevada, Inc.—02 September 2014
295. LPL Financial LLC—02 September 2014
296. Nationstar Mortgage LLC—02 September 2014
297. Aventura Hospital and Valesco Ventures letter to Consumer re Security Breach—05 September 2014
298. California State University East Bay letter to Consumers re Security Breach—05 September 2014
299. J.P. Morgan Corporate Challenge—05 September 2014

300. Republic Bank & Trust Company—05 September 2014
301. Intuit—06 September 2014
302. Holy Cross Hospital—08 September 2014
303. Yandy.com—08 September 2014
304. Ameriprise Financial Services, Inc.—09 September 2014
305. Cedars-Sinai Health System—10 September 2014
306. County of Napa, Health and Human Services Agency, Comprehensive Services for Older Adults—12 September 2014
307. Tim McCoy & Associates (DBA NEAT Management Group)—15 September 2014
308. CareCentrix, Inc.—18 September 2014
309. Discover letter 1 to Consumers re Security Breach—19 September 2014
310. SELF Loan—19 September 2014
311. Viator letter to Consumer re Security Breach—19 September 2014
312. North American Title Company—22 September 2014
313. Rentrak Corporation—23 September 2014
314. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—24 September 2014
315. Jimmy John's Franchises LLC—24 September 2014
316. Pacific Biosciences of California, Inc.—25 September 2014
317. Advantage Funding Company—26 September 2014
318. Bay Area Bioscience Association—26 September 2014
319. Experian—26 September 2014
320. Fidelity Investments—26 September 2014
321. USAA letter to Consumers re UPS Security Breach—26 September 2014
322. Albertson's LLC—29 September 2014
323. Imhoff and Associates, P.C.—29 September 2014
324. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—01 October 2014
325. AT&T letter to Consumers re Security Breach—01 October 2014
326. DHLS letter to Consumers re Security Breach—01 October 2014
327. Flinn Scientific, Inc.—01 October 2014
328. Community Technology Alliance—02 October 2014
329. East West Bank—02 October 2014
330. East West Bank—02 October 2014
331. Touchstone Medical Imaging LLC letter to Consumers 2 re Security Breach—03 October 2014
332. Advanced Data Processing, Inc.—08 October 2014
333. International Dairy Queen, Inc. ("IDQ") on behalf of 9 Dairy Queen franchise locations in California listed in the attached addendum—09 October 2014
334. Penn Highlands Brookville—09 October 2014
335. National Domestic Workers—10 October 2014
336. SAUSALITO YACHT CLUB—10 October 2014
337. University of California Davis Medical Center—13 October 2014
338. GovMint Com letter to Consumers re Security Breach—14 October 2014
339. Pulte Mortgage LLC—14 October 2014
340. Gold's Gym—15 October 2014
341. National Domestic Workers Alliance letter to Consumers re Security Breach—16 October 2014
342. Primerica—16 October 2014
343. Backcountry Gear—17 October 2014

344. Sourcebooks letter to Consumers re Security Breach—17 October 2014
345. Columbia Southern University—20 October 2014
346. Experian—20 October 2014
347. Experian letter To Consumers re Security Breach—22 October 2014
348. The Sinclair Institute letter to Consumers re Security Breach—22 October 2014
349. Alliance Workplace Solutions, LLC—23 October 2014
350. American Soccer Company, Inc.—23 October 2014
351. Reeves International, Inc.—23 October 2014
352. Benefit Express Services—24 October 2014
353. c3controls—24 October 2014
354. Duluth Pack—24 October 2014
355. Fidelity National Financial, Inc.—24 October 2014
356. Capital One letter to Consumers re Security Breach—27 October 2014
357. Direct Learning Systems, Inc., d/b/a 123ce.com—27 October 2014
358. East West Bank-CA Impacted Customers-Kmart Data Breach—27 October 2014
359. Green Energy Training Academy—27 October 2014
360. Modern Gun School—27 October 2014
361. Modern Gun School—27 October 2014
362. The Evolution Store letter to Consumers re Security Breach—27 October 2014
363. Arizona State Retirement System—28 October 2014
364. Cape May-Lewes Ferry—30 October 2014
365. Delaware River & Bay Authority—30 October 2014
366. US Investigations Services, LLC letter Consumer re Security Breach—30 October 2014
367. Anderson & Murison, Inc.—31 October 2014
368. Nationstar Mortgage, LLC d/b/a Champion Mortgage—31 October 2014
369. M&T Bank (Identity Theft)—02 November 2014
370. Camp Bow Wow Franchising, Inc.—03 November 2014
371. Experian—03 November 2014
372. One Love Organics, Inc.—03 November 2014
373. Palm Springs Federal Credit Union—03 November 2014
374. West Publishing Corporation—03 November 2014
375. Nova Southeastern University—06 November 2014
376. Nova Southeastern University—06 November 2014
377. Aarow Equipment & Services, Inc.—07 November 2014
378. Evolution Nature Corp. d/b/a The Evolution Store—07 November 2014
379. Weill Cornell Medical College—07 November 2014
380. EZ Prints, Inc. letter to Consumer re Security Breach—10 November 2014
381. Easter Seals New Hampshire, Inc.—12 November 2014
382. Citibank, N.A.—13 November 2014
383. Visionworks 1st letter to Consumer re Security Breach—13 November 2014
384. REEVE-WOODS EYE CENTER—14 November 2014
385. AHS letter to Consumer re Security Breach—18 November 2014
386. MemberClicks, Inc. d/b/a Moolah Payments—18 November 2014
387. Amgen, Inc. letter to Consumer re Security Breach—19 November 2014
388. Discover letter to Consumers re Security Breach—19 November 2014
389. AlliedBarton Security Services LLC—21 November 2014
390. APi Group, Inc.—21 November 2014
391. Experian—21 November 2014
392. Blue Zebra Sports—24 November 2014
393. Cultivian Ventures, LLC—24 November 2014

394. Fairway Independent Mortgage Corporation—24 November 2014
395. Visionworks 2nd letter to Consumer re Security Breach—24 November 2014
396. Form—25 November 2014
397. New Hampshire Employment Security—25 November 2014
398. Simms Fishing Products letter to Consumers re Security Breach—25 November 2014
399. State Compensation Insurance Fund—25 November 2014
400. Calypso St. Barth letter to Consumer re Security Breach—26 November 2014
401. Highlands-Cashiers Hospital—26 November 2014
402. Shutterfly, Inc.—26 November 2014
403. Holiday Motel letter to Consumer re Security Breach—28 November 2014
404. American Residuals and Talent, Inc. (ART) letter to Consumer re Security Breach—01 December 2014
405. Big East Conference—01 December 2014
406. Blue Mountain Community Foundation—01 December 2014
407. Godiva Chocolatier, Inc.—01 December 2014
408. Highlands-Cashiers Hospital—01 December 2014
409. Bebe Stores, Inc.—05 December 2014
410. Econolight501 General Proofs—05 December 2014
411. Sands Casino Resort Bethlehem—05 December 2014
412. AHS letter to Consumers re Security Breach—09 December 2014
413. Seterus—09 December 2014
414. EMCOR Services Mesa Energy Systems—11 December 2014
415. ABM Parking Services—12 December 2014
416. Acosta, Inc. and its subsidiaries, including Mosaic Sales Solutions US Operating Co. LLC—12 December 2014
417. Clay County Hospital—12 December 2014
418. University of California, Berkeley—12 December 2014
419. Apple Leisure Group and AMResorts—15 December 2014
420. Point Loma Nazarene University—15 December 2014
421. Valplast Supply Services, Inc. letter to Consumer re Security Breach—16 December 2014
422. Ascena Retail Group, Inc.—17 December 2014
423. Harmonic Inc.—18 December 2014
424. American Express Travel Related Services Company, Inc. and/or its Affiliates ("AXP")—19 December 2014
425. Mercy Medical Center Redding Oncology Clinic—19 December 2014
426. Presidian Hotels & Resorts—19 December 2014
427. Quest Diagnostics—19 December 2014
428. Staples, Inc.—19 December 2014
429. BolderImage SBN to Consumers—20 December 2014
430. Azusa Pacific University—22 December 2014
431. ID Parts LLC letter to Consumers—22 December 2014
432. Nvidia Corporation—22 December 2014
433. DutchWear—23 December 2014
434. Public Architecture—23 December 2014
435. Rob Kirby, CPA—23 December 2014
436. Transamerica Premier Life Insurance Company—23 December 2014
437. Corday Productions, Inc.—24 December 2014
438. Lokai Holdings LLC—24 December 2014
439. Allianz Life Insurance Company of North America—26 December 2014

440. Empi, Inc./DJO, LLC—26 December 2014
441. Physicians Skin and Weight Centers, Inc.—26 December 2014
442. Six Red Marbles—26 December 2014
443. Stagecoach Transportation, Inc. SBN to Consumer—December 26, 2014
444. Fast Forward Academy, LLC—30 December 2014
445. La Jolla Group—31 December 2014