WEIS 2015 – Paper submission

Author: Fabio Bisogni

Affiliations: Delft University of Technology - Faculty of Technology, Policy and Management / Formit Foundation

Key words: data breach notification laws, data breach disclosure, data breach notification federal law, security breach notification effects, bad-news messages

Date: May 15th 2015

Data Breaches and the dilemmas in notifying customers

While the discussion about a federal law on data breach notification is ongoing and a rash of large, costly data breaches has galvanized public interest in the issue, this paper investigates on the phenomenon of data breach notification letters. In case of any data breach a company faces a number of dilemmas on how to inform the customers. The choices that a company makes on the missive content result decisive in having a prompt customers' reaction against identity theft and eventually in shaping the relations between customers and the organization itself.

Starting from the various regulations in place in US, the analysis has been performed focusing on the content of over 210 letters sent in US in the first semester of 2014. In particular letters are classified based on elements that can be isolated and analysed, e.g. the level of transparency used in communicating the event causing the breach or the time span between data breach identification and its notification to customers. In the end we labeled the data breach notifications according to the message customers might perceive when reading them. As a result six message types have been identified. This investigation contributes to the ongoing debate on the federal law on data breach notifications, highlighting limitations and effects of the already implemented State laws.

1. Introduction

Nowadays data breaches have become a very complex phenomenon to be handled with multifaceted competencies, not only technical. The identification, in a company, of a breach that generates an access or acquisition of customer personal information by third parties triggers a decision making process that includes also an important aspect, i.e. communication towards customers. This communication is represented by data breach notification letters, one of the elements covered by the data breach notification laws enacted in the US.

The choice on the content of these missives provides an opportunity to communicate, not only to customers, but more in general to stakeholders, the importance for the organisation of values such as security, law compliance and law enforcement cooperation. Such a communication has therefore an important impact on the organisation's reputation. Moreover, if duly analysed, those letters can support the detection of the organisational risk propensity towards potential losses due to customer churn, fines and class actions.

While the discussion about a federal law on data breach notifications is ongoing and a rash of large, costly data breaches has galvanized public interest in the issue, this paper investigates on the phenomenon of data breach notification letters

- highlighting different regulations in place in the US;
- presenting concrete examples of various communication styles used to inform customers about breaches;
- proposing specific evaluation metrics that allow a classification of letter types;
- calculating average time span between data breach, data breach identification, data breach notification to customers.

To perform each of the listed objectives it is important to consider each notification as a set of elements that can be isolated and analysed. Each of these elements poses the letter signatory in front of a dilemma of how to inform about the breach. This research can be useful to take more conscious decisions when choosing among the options at stake and to contribute to the ongoing discussion on the federal law on data breach notifications, highlighting limitations and effects of the already implemented state laws.

The main sources of information used for the investigation are 1) 47[1] state data breach notification laws and selected extensive reports issued by law firms and available on line[2], thoroughly examined to identify - where available - mandatory elements of the notification letters; 2) thirty-two letters sent to customers by organisations based in California and Florida and downloaded from dataloss.org used to identify the different dilemmas; 3) the Ponemon study[3] used to cross the letters with the consumers' perceptions recorded by the study results about the importance and value of receiving a notification when their sensitive personal information has been lost or stolen; 4) 213 data breach notification letters sent in the first semester of 2014, downloaded from the attorney general websites of 4 different States used to verify the choices made by the affected companies.

2. Defining the context

Data breach notification laws are promulgated under the theory that the customer has the right to know when their personal information has been stolen or compromised. Additionally, data breach notification laws provide an incentive for organizations to take adequate steps to secure personal information held by them (sunlight as disinfectant[4]). The notification itself represents the core element of these laws.

Issuing data breach notification letters is just one of the challenging tasks an organisation needs to accomplish after a leak of secure information to an un-trusted environment has been discovered. More specifically, a company that identified a data breach has to face a series of challenges in order to be certain to be law compliant.
Firstly, customers whose data may be breached need to be identified. In fact organisations, such as merchants, that have breached credit card numbers not always do themselves possess the mailing addresses associated with those numbers (GAO-07-737, 2007).
Secondly, it is necessary to deal with the compliance with multiple state laws. In fact the applicability of the US notification laws relates not to the residence of the breached organisation 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 must be notified apart from the customer, the level of risk that triggers a notice, the nature of the notification, and exceptions to the requirement. Therefore, one must perform an analysis of all applicable state regulations, in order to be sure that each resident's state law has been fully followed in all its provisions.
Finally, the data breach notification letters need to be prepared and sent to customers. This is often a trigger of potential harm for the company and for sure an additional cost to be incurred.

While this paper investigates on the second challenge, it is worth mentioning a few interesting findings developed by other researchers on impacts breach notifications for breached organizations in terms of their performance. These findings provide a relevant context for our study:
Romanosky, Telang and Acquisti (2011) 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 (2007) highlights how software vendors' stock prices suffer if information about their products' vulnerability is announced. Acquisti, Friedman, and Telang (2006) 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

---

[1] Alabama, New Mexico and South Dakota are now the only U.S. states that have not yet enacted a data breach notification law.

[2] Data Breach Notification Laws by State' (CLLA, 2012) http://www.clla.org/documents/breach.xls
State Data Security Breach Notification Laws' (Mintz Levin, 2012)
http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf
State Data Breach Stature Form' (Baker Hostetler, 2013)
http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf
Security Breach Notification Chart (Perkins, 2013)
http://www.perkinscoie.com/files/upload/LIT_09_07_SecurityBreachExhibits2.pdf

[3] 2012 Consumer Study on Data Breach Notification, Ponemon Institute LLC, June 2012

[4] Phrase attributable to Justice Louis Brandeis, 1933

et al. (2003) 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 (2004) 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 (2006) 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). Bisogni (2013) investigated the possibility to assess the severity of the different data breach notification laws in place in US to support a fine-tuned impact evaluation.

Focusing now on the second challenge, notifications are issued in the 47 US States that have enacted data breach notification laws requiring businesses and other entities to notify affected individuals when a data breach involving their personally-identifiable information (also referred to as PII or personal information) occurs.

The first US DBNL, enacted in California, requires any business that has suffered a data breach, or believes to have suffered a data breach that entails an unauthorized acquisition of unencrypted and computerized personal information, to notify California residents about the incident.[5] Also the Attorney General needs to be notified if more than five hundred residents’ data are involved in the security breach. A law enforcement agency can request a delay if the notification would impede a criminal investigation. The concerned individuals are to be notified within a timeframe that is expedient and without reasonable 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 DBNL 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 (Faulkner, 2007).

The requirements of the laws in the other 46 States differ from the Californian model and also vary from one State to another. These differences generate a significant complexity for organisations 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.[6]

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 State legislations out of forty-seven. From the analysis of these legislations, notifications can contain a certain number of mandatory requirements, listed by State in Table1.

[5] California Civil Code § 1729.98

[6] Some organizations opt for filling the gap with an annex which fulfils case by case each state legislation

	California	Hawaii	Illinois	Iowa	Maryland	Massachusetts	Michigan	Missouri	New Hampshire	New York	North Carolina	Oregon	Vermont	Virginia	West Virginia	Number of States with feature availability	% on 15 States
Type of PI subject ti the unauthorized acces or acquisition	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	13	87%
The reporting entity's name and contact information so that affected individuals can obtain additional assistance or information. (in some case toll free required, in some case if one exist specified)	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	12	80%
A general description of the breach incident, if that informatino is possible to determine at the time notice is provided	✓	✓		✓			✓	✓	✓		✓		✓	✓		9	60%
Contact information for national consumer reporting agencies			✓	✓	✓			✓			✓	✓			✓	7	47%
A brief description of the actions taken by the business to contain the breach and protect data from further unauthorized access or use.	✓*	✓					✓				✓		✓	✓		6	40%
A statement that the individual can obtain information from these sources about fraud alerts and security freezes			✓		✓	✓					✓				✓	5	33%
The date of the breach, or if unknown, the approximate date or date range of the breach.	✓								✓			✓	✓			4	27%
Remind notice recipients of the need to remain vigilant for incidents of fraud and identity thefts							✓	✓			✓			✓		4	27%
Contact information for law enforcement and other government authorities, including the Federal Trade Commission (FTC).			✓		✓						✓					3	20%
Advice on actions affected individuals should take (In Iowa and Oregon only specified advice to report suspected incidents of indentity thefts to local law inforcement or the attorney general)	✓*	✓		✓								✓				4	27%
Advice to the consumer to report suspected incidents of indentity thefts to local law inforcement or the attorney general				✓								✓				2	13%
Frequency by State	7	5	3	4	5	2	5	5	4	2	8	6	5	5	4		

* at discretion

Table 1 – Mandatory elements of data breach notification by State

Almost all fifteen States require the letters to include the type of personal information subject to an unauthorized access or acquisition (87%) as well as the reporting entity's name and contact information so that affected individuals can obtain additional information (80%). A general description of the breach incident is required in nine States out of fifteen. General advice on actions that affected individuals should take has to be included in four States. Other state legislations have opted for more explicit requirements. Specifically, a statement indicating that individuals can obtain information from specific sources such as Federal Trade commission and consumer reporting agencies and a remind notice of the need to remain vigilant for incident of fraud and identity theft, are mandatory respectively in five and four States.[7]

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 identity thefts (Data breaches and identity theft, 2005 p.10) and specifically provide them with the opportunity to take steps to protect themselves from a possible identity theft, suggesting to place fraud alert 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 is at least peculiar, increasing the number of consumers who received a notification letter and found it not easy to understand (52% according to Ponemon study), and generating potential confusion with other mail solicitations that may resemble notification letters.[8]

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.

[7] 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.

[8] For example, officials at one large national bank noted that marketing solicitations for credit monitoring services often are made to resemble breach notification letters, potentially desensitizing or confusing consumers when a true notification letter arrives.

These laws create an intersection between business communication and information security (Veltsos, 2012), that we will investigate by proposing an ad hoc evaluation framework. We will observe if and how companies leverage on the consumer inaction, resulting from their behavioural decision biases such as optimism bias (consumers perceiving their chances of suffering identity theft to be very low), rational ignorance (consumers believing the cost of taking precautions outweighs any benefits they may receive), and status quo bias (consumers' own inertia inhibiting them from anticipating the consequences of identity theft and responding) (Romanosky, Telang, and Acquisti, 2011, Loewenstein, John, & Volpp, 2012).

3. Building up the DBNL evaluation framework

We have discussed how Data Breach Notification Laws dispose that organisations contact customers after the discovery of a breach affecting PII, offering poor indications on the style and content of the notification. We will now investigate how companies use such given room for manoeuvre in delivering bad news related to the breach. To perform such investigation we will build up an evaluation framework starting with a review of the existing research in the field of communicating negative messages.

A rich source of information is represented by business communication textbooks, with their limitations related to the fact that they provide advice for low risk and routine situations, such as denial of credit, collection requests, rejections for employment, inability to meet deadline, and similar occurrences that have occupied attention in the business communication classrooms since the 1930s (DeKay 2012). Even if growing in number, data breach notifications need to be seen rather as high risk and non-routine situations: "specific unexpected and non-routine events or series of events that create high level of uncertainty and threaten an organisation's high priority goals" (Seeger, Sellnow, & Ulmer, 1998, p. 233).

In the field of bad-news the lines of research inquiry and points of contention have centered on three key aspects of composing and teaching negative news messages: (a) arrangements (b) components, and (c) pedagogical techniques (Creelman 2012). We will focus on arrangements and components for our evaluation framework. The framework will be built up on concrete examples from authentic letters sent in the past in two States: California and Florida. The sample of data breach notification letters was collected through dataloss.org for companies based in these two States.

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 (Hynes, 2008 and Kolin, 2007 and Alred et al., 2011) who suggest to avoid negative words altogether, highlight how diplomacy and "reader psychology" are fundamental elements in corporate correspondence, and present it as more effective especially if stakes are high (Alred et al., 2011). 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 (Bovée & Thill, 2012, Shwom & Snyder, 2012). On the other side, the fact that the stakes are high may be precisely the driver for using a direct pattern in data breach notifications (Veltsos, 2012). 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 (Lehman & DuFrene, 2012, p. 105). The direct pattern clearly provides stronger incentive to continue reading about protective measures. Locker and Kienzler (2010) consider this type of directness to be "good ethics and good business" (p. 437).

Here below an example of the two typologies of opening (direct and indirect respectively).

> *Dear customer,*
> *We are writing to inform you of a recent incident involving the unauthorized disclosure of your name and Social Security Number. [11FL]*

Dear Sir or Madam:
We are writing to you because of a recent security incident at the Department of Consumer Affair (Department). A document containing the names and Social Security Number of Department employees was inappropriately sent outside the Department. We are notifying you of this incident because your name and Social Security number were included in the document.[11 FL]

In addition to placing an explanation before the bad news, a key element in the indirect pattern is an opening buffer, that occasionally can also be found in the direct pattern. Although most textbooks endorse the use of buffers to open negative messages, Locker (1999) argues that buffers are not always appropriate, explaining that "Good buffers are hard to write. If buffers do not make readers respond more positively, then we have little reason for mandating buffers as the standard opener for negative messages" (p. 21). Here below an example of the two typologies of opening (direct and indirect respectively) with a buffer.

Dear customer,
XY's commitments to customer privacy and data privacy are top priorities, and we take those commitments very seriously. We recently determined that employees of one of our service providers violated our strict privacy and security guidelines by accessing your account without authorization... would have been able to view you social security number...

Dear customer,
At ..., we pride ourselves on creating a positive environment for all of our customers. We wanted to be proactive in bringing a recent incident at our Sacrament division office to your attention and we hope to address any concern you may have. [1CA]
Follows explanation..

Beyond arrangements, researchers have also questioned the use and effectiveness of the conventional **components** or parts of bad-news messages prescribed by business communication textbooks as an effective means of presenting the unfortunate event. Textbook authors agree that an (1) **explanation** is a crucial aspect of negative messages. The explanation should describe the problem clearly and unemotionally while not placing blame (Carter, 2012), as well as protect the organization's reputation reducing follow-up correspondence (Bovée & Thill, 2012). In the analysed breach notifications we can identify the explanation component in two recurring elements: incident description and reaction of the organisation.
(2) **Bad news** is the next component that contains information resulting in a perceived loss by the receiver, and it creates cognitive, emotional or behavioural deficits in the receiver after receiving the news (Bies, 2013). In case of data breach notifications we find a specification that PII has been accessed/acquired and possible negative consequences might be generated by this access/acquisition. When possible, bad news is followed by an ***alternative*** solution or action**,** in line with a traditional advice in the bad-news research to "offer an alternative or a compromise if one exists" (Locker, 1999, p.31). In the analyzed notifications we can identify the alternative element in the suggestions for customer reactions to be vigilant, check credit reports, file a complaint with the FTC, and activate eventual security freezes.
Components include also (3) **prefatory and closing buffers** that provide background information, good news, thanks and compliments, general accepted truths, or express empathy with the audience (Shwom & Snyder, 2012). In the investigated notifications, buffers are mostly represented by statements on importance of security within the organisation and by reassurance on an enhanced level of protection. Closing buffers usually offer support for clarifications by providing company contact information.

After a careful analysis of the notifications we propose a new approach to pinpoint and evaluate the decisions taken by companies when writing a data breach notification. The main "conventional" components are embedded in the proposed framework that in this new form describes better the dilemmas faced by organisations when writing data breach notification letters.

In particular, given their frequency in the letters, six elements are worth an isolated analysis:

1) **Clarity:** Clarity of the incident description and of the PII involved. (Explanation and bad news)
2) **Tone:** Communication tone on the possible consequences given the organisation reaction (Explanation and bad news)
3) **Action:** Approach to actions to be taken by the affected customers (Alternative)

4) **Interaction:** Interaction with affected customers (Closing buffer)
5) Stated **relevance of security and** of the **steps to reinforce it** (Prefatory and closing buffers)
6) **Style** in addressing customers

For each one a description will be given, followed by extracts of sentences from the collected letters as well as comments on different styles, and finally the link with the results recorded in the Ponemon study.

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 if to acknowledge therefore organisational or procedural weaknesses of the company depends on the management evaluation of the legal framework, customer relationships, potential additional harm for the affected customers and/or the company. Sometimes organisations 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 organisations are viewed in a worse light than if all the facts had initially been disclosed. This scenario is confirmed by the customers according to the Ponemon Study on Data Breach Notification 2012. The study says that they were dissatisfied with the communication and often felt the need for more information. In particular 61% of customers believed notifications were not easy to understand (mostly because of a too long and poorly written letter and too much legal language). Many customers did not believe that notifications increased their understanding of the event, in particular 37% of the customers said they had no idea what the data breach was about. Additionally 45% of the customers suggested to disclose all the facts in order to improve the communication of the notification.

In order to determine the level of clarity we defined a simple tool that crosses the level of transparency in the event description with the one of the PII details. To simplify the analysis we assumed there are only two possible options for transparency: transparent and opaque. In case of the event description the notification is classified as transparent when it meets at least 2 out of the following 3 requirements (the type of event is specified, the generating causes are described, the organisation reaction is indicated) and opaque if it meets only 1 of the requirements listed above. In case of the PII details the letter is considered transparent if the personal identifiable information accessed/acquired by third party are clearly specified and opaque if not. The "crossing" tool provides basically 4 areas of clarity as shown in Figure 1. Clearly within each area we may find many shades of clarity, to be noted particularly in the letters where either the event or the PII lack some transparency (see boxes b and c in the figure below).

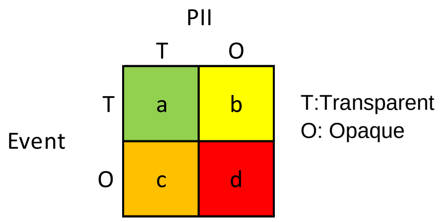


Figure 1 – Clarity options

In case of box b, the description of the event can be very detailed and clear, but opacity can be found in the description of the accessed/acquired PII, not specifying clearly which ones were breached.

> *...in late February our archive services vendor notified us that they could not account for one of several boxes of data backup tapes being transported to an off-site storage facility. The missing tapes held certain personal information, such as your name, address, social security number and/or shareowner account information. [2CA and 4FL[9]]*

The opacity can also be generated by providing an extensive list of PII potentially accessed/acquired, expressing however uncertainty that such information was contained.

[9] The code indicates the letter the sentence was taken from. See list in reference for more details (Letters downloaded for framework setup)

We sincerely regret to tell you that a laptop computer belonging to an employee of xyz was lost on May 11 and may have contained certain personal information regarding you and your account.. your name and social security number, and potentially other information about you, including date of birth, home address and telephone number, net worth, annual income and your xy account number [3CA and 6FL]

Box c refers to those examples of an opaque description, where no details are given about the specific circumstances that led to the necessity of sending the data breach notification letter and only essential information is provided on the PII involved. The description is therefore brought to the bare minimum.

The xy recently discovered that some internal documents that contained personal information about you were lost. This information included your name and full social security number. [7CA]

Finally, statements that may increase the event transparency but also the likelihood of misunderstanding by the reader, are also an option, stating both what was not contained in the accessed database and what was indeed contained.

Our investigation has concluded that the computer did not contain your social security number, address, or any other financial information, such as a credit card number. However, we do believe it may have contained some additional information such as your alternate plan ID number, prescription numbers and names, and date of birth. [10CA]

In order to reduce the analytical complexity we decided not to take into consideration the PII input and work only on the event description. In order to determine the level of clarity, we focused on the details provided in the event explanation. If no indication of the type of the event that generated the breach and of the circumstances related to the presumed cause of the event is provided we classified the clarity as opaque.

The performed analysis reveals that most of the organisations decide to describe the event in a very transparent manner. However it is worth noting that in none of the analysed 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.

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 (Veltsos 2012). Organisations are torn between a range of possibilities. 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. In this way unfortunately the risk of legal actions could be higher in case the data breach would result in serious tangible consequences such as identity thefts.

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. The study conducted by the Ponemon Institute underlines that customers (56%) suggest to improve notifications by explaining the risk of harms that will most likely be experienced as a result of the breach.

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 notifications in almost all cases is to underline no current damage and to belittle the potential future harm.

In particular, a message can be reassuring about consequences, when:

- stressing that the notice is due mostly to legal compliance, even if the risk is very low:

Florida law requires us to notify you that this loss of personal identifiable information has occurred so that you may take some protective steps if you desire. We believe the risk for anyone using the information for identity theft or other unlawful proposes is extremely low. [2FL]

- highlighting that the law compliance obligation for the current event is even questionable:

While we do not believe that we are obligated to provide notice of this data breach to you, we are doing so as a precautionary measure. [13FL]

- stressing the low risk of the specific breach but also naming potential risk of such an event:

> *While we have no reason to believe that your information has been accessed for any unlawful purpose, and believe the risk to you is limited, we feel important to inform you of the potential risk of identity thefts resulting from this mistake. [16FL]*

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.

> *While we are uncertain whether your personal information was actually obtained, I want to bring this situation to your attention and urge you to take action to minimize your risk of identity theft.[1FL]*
>
> *Even though we do not know whether your personal information has been improperly accessed or misused, we want to make you aware of the incident and the steps that have been taken to prevent a reoccurrence. [14CA]*

In this case the company was very direct describing truly what the situation was, while in fact in most cases organisations do not have thorough knowledge on the incident consequences however they are not explicit about it.

Finally an ***alarming*** tone can be used, focused on stressing the present and/or potential risks with straight-forward expressions as *we wanted to alert you, your personal information is at risk, due to the serious nature of this situation.*

> *We are actively investigating this incident to fully determine the extent to which credit card information for our customers may have been accessed, and wanted to alert you that your credit card may be at risk. You should therefore consider taking the following steps. [15FL]*

Another option to alert customers is to add an adverb of time before usual expressions such as "*we have no reason to believe, we have no indication, we have no evidence*". The time reference clearly points out the organization's limitations of control upon potential consequences.

> *We and the vendor are cooperating with law enforcement authorities on this matter and an investigation is under way. In addition, the vendor has adopted additionally security measures as its offices. We're also reviewing the facts and circumstances that led to this incident closely, and will take appropriate steps to help prevent something like this from happening again. At this time, we have no reason to believe the data contained on the computer was the target of the theft of that the personal information has been accessed or used improperly. [3FL]*

The decision on the communication tone is of course dependent on the event itself but also on the given legal framework. In case of the States without mandatory content of the missive, companies can more easily opt for reassuring instead of alarming customers about the event in comparison to fully regulated States. This can be a consequence of a larger room for manoeuvre when deciding which elements to include. California regulation does not make it possible to belittle the event considering that almost all the elements of Table 1 should be included in the letter.

3) Approach to actions to be taken by the affected customers (neutral vs. encouraging). Another decision tree node for the organisation 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 work as an alarm bell for customers, fostering them in taking seriously the content of the message 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 credit file (also, however rarely, to put a credit freeze on credit file), to check credit activity regularly with each credit issuer, to activate a service of credit monitoring at no cost for the individual. In some cases it is also specified why the organisation is not performing those actions itself (*credit agencies will not permit XY to act on your behalf regarding your credit data [1FL]*).

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.

Although we cannot provide advice, other than logistical information in this letter, for your convenience and information, following are two sources of information about precautions you can take to protect your personal information. [8CA]
Although we are employing measures to prevent unauthorized access to your records with us, we want to inform you about this incident so that you can determine whether you should take some additional steps to protect yourself from identity thefts. [5CA]

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…,.*

While we are uncertain whether your personal information was actually obtained, I want to bring this situation to your attention and urge you to take action to minimize your risk of identity thefts. [1FL]

We suggest you also contact all of your banks, credit cards companies, investor and financial institutions and all other creditors and ask what steps they deem appropriate as to the accounts you have with them. Although these are precautionary measures, we believe you should take very reasonable measure to protect your personal information. [6CA]
While there is no reason to believe your information has been accessed, we encourage you to the following steps to protect against the remote possibility your personal information is used for unlawful purposes.

4) Interaction with affected customers (neutral / available / fostering). Activating communication channels and managing them increases company costs not only for call centers, but also for a higher rate of activated credit monitoring. On the other side 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 can be different.
When classifying the notifications' tone for interaction we used the following requirements: in 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 below there are three examples respectively of a fostered interaction, of availability, and of a neutral communication of a contact number.

Fostering interaction

We're eager to help answer your questions and to explain how to activate the credit monitoring. You can contact us right now by.. [3FL]

Highlighting **availability**:

If you have other questions please do not hesitate to call me at.. [2FL]

Being **neutral**:

For additional information, please see the enclosed sheet titled "Information about Identity Theft Prevention" and the enclosed "Frequently Asked Questions" document, or call 1-866-979-2512.

5) Stated relevance of security for the affected organization and stated steps to reinforce security[10] (none/medium/high).
Highlighting the relevance of security can be on one hand reassuring for the customer, but on the other it could generate the sensation that even though security is a top priority for the organisation, it has failed in protecting key information. Moreover pompous statements on the high level of security in the organisations could also be seen as a tentative to minimize the event. According to the Ponemon study customers who had received notification letters in the past suggest not to "sugar coat" the message (28%) to improve such communication.

[10] In particular stated actions taken or planned to contain the breach and protect data from further unauthorized access or use

Typically such messages are either included in the letter intro or at the very end and they refer to data protection, data confidentiality and security as well as privacy as key priority in the organization (see the examples below).

> *Protecting the confidentiality of this information – and all of our clients' information – has long been a top priority at xyz. However.. [2CA]*
>
> *You can be assured that we take our obligation to protect data security of personal information very seriously. [3FL]*
>
> *The confidentiality and security of our business partners' and former and current customers' personal information is very important to xy. We maintain physical, electronic and procedural safeguards that meet state and federal regulations and we limit access to our customers' information. [5CA]*
>
> *You security and privacy are very important to us. [5FL]*
>
> *At ..., we pride ourselves on creating a positive environment for all of our customers. We wanted to be proactive in bringing a recent incident at our Sacrament division office to your attention and we hope to address any concern you may have. [1CA]*

This last example shows how law compliance can be communicated as pro-activity. This is a sentence that once again proves how companies may make use of the customers' informative gap in terms of legal framework in place, which enables them to present a particular action as proactive, when in most of the cases it is just mandatory.

As for the actions taken by the business to contain the breach and protect data from further unauthorized access or use, more than 50% of the organisations prefer to state that additional steps have been taken in order to reinforce the security to prevent from the same/similar events. This is a very critical point considering that 35% of the Ponemon study respondents say their relationship and loyalty is dependent upon the organisation not having another data breach.

> *We're also reviewing the facts and circumstances that led to this incident closely, and will take appropriate steps to help prevent something like this from happening again.[3FL]*
>
> *We have implemented additional measures that will help prevent a similar occurrence [4FL]*
>
> *While we have measures in place to help prevent this type of situation from happening, we are carefully reviewing our processes to minimize the chance that it could happen again, including issuing special advisories to store management. [5FL]*
>
> *We are taking immediate steps to minimize the likelihood of similar events in the future, including a top-to-bottom review of the company's information security policies, limiting the amount of personally identifiable information stored on devices, and increasing the use of encryption and other protective technologies [3CA, 6FL]*
>
> *In addition to terminating the unauthorized access, we revalidated our information security infrastructure to confirm that we maintain industry standard protections for customer data. [10FL]*
>
> *We have implemented additional control to avoid a similar future incident. These controls include enhanced security measures which limit use to select authorized personnel. [13FL]*

When classifying notifications, we consider **medium** the "stated relevance of security for the affected organization and of the steps to reinforce it", when only one of the two elements is included, **high** when both are stated and **none** when there is no mention on any of the two.

Finally, it is interesting to notice that some organisations anticipate the risk of an additional notification related to a new data breach, using expressions such as the one here below.

We have also taken additional proactive security measure to help prevent a similar incident from occurring in the future; however due to the nature of cybersecurity attacks, it is virtually impossible to entirely prevent these types of event from ever occurring.

6) *Style in addressing customers (form / personal).* Additionally, it is important to notice how the communication style plays an important role in influencing the customer perception in terms of the relevance of the news received.
Maintaining a cold profile, not even addressing the customer by name and surname, could be an option if the strategy behind it is not to alarm the customer or even not to let him take seriously the letter and rather confuse it with junk missive. On the other side if negative consequences will result and the customer is able to link such consequences to the data breach greater negative impacts are to be expected for the organisation.

The personal addressing uses always the following style:
Dear <<Title>> <<Last Name>>, [2FL] or
Dear <<First Name>> <<Last Name>>[1CA]

On the contrary the form option uses such expressions as:
Dear Applicant, [3FL]
Dear Cardholder, [8FL]
or there is no salutation at all.

The Ponemon study shows that in 62% of the cases the notification was a form letter and in only 19% it was a personal letter[11]. This generates the perception that such missive is junk mail or spam (49%) against the identification of such letters as important communications (34%). It is even more important to highlight that the same indicators measured in 2005 were respectively 23% and 51%, defining a clear growing trend in misunderstanding the true goal of the letter.

It is worth mentioning that in order to limit the reputational effects organisations may also apply solutions often used in case of product complaints such as coupons or inexpensive "goodies". Compensation may further symbolic goals, such as demonstrating the importance of the customer to the company and the sincerity of the remorse. (Conlon and Murray, 1996).

As a token of your appreciation for your continued patronage, we are also enclosing a 20% discount code that you may use on your next purchase from us at www… [7FL]

For a limited time, we are offering a Preferred Customer Rate discount program for our customers who may have been impacted by this incident. You will receive a 20% discount…[10FL]

4. Implementing the framework and shaping the letter types

After this initial overview of the core elements of the Data Breach Notification Laws and of the Notifications themselves, the methodological steps described below were followed in order to conduct a more in depth analysis and to enable the implementation of the framework:

1) Identify the States that make available the data breach notification letters issued by affected companies. From our desk research only 4 States out of 47 make this information easily available through the government website. In particular, California, Maryland, New Hampshire and Vermont.[12] It is maybe not a coincidence that the four States are within the

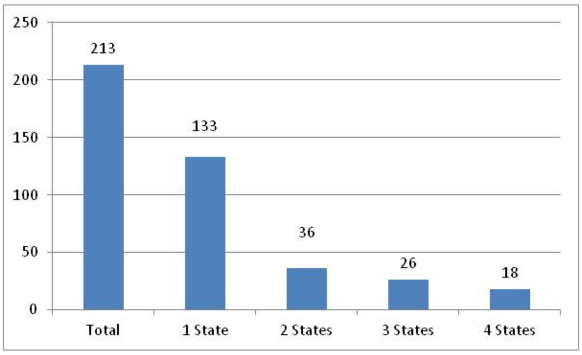


Figure 2 – Data breach sample 1/1/2014-30/6/2014

[11] The remaining cases (19%) refer to other options to communicate the breach, including telephone call and Posting in major newspaper
[12] https://oag.ca.gov/ecrime/databreach/list
http://www.oag.state.md.us/idtheft/businessGL.htm
http://doj.nh.gov/consumer/security-breaches/

group of 15, where the content of notifications is defined by law. Clearly setting mandatory requirements seems to produce also an incentive to give more visibility to such missives. Another State, Maine, makes available the list of data breaches relevant for the state residents, but does not provide the notifications sent.

2) Download all letters included in the list available in the timeframe 1/1/2014-30/6/2014, identifying the letters sent out in more than one of the four States. The number of analysed letters taking out the duplications (same letter sent to different States) is 213, with the following split of unique letters by State: 66 for Vermont, 84 for California, 122 for Maryland, 83 for New Hampshire. The overlapping between the four States can be seen in the Figure 2. 133 were the notifications sent only in one of the four States, 36 in two States, 26 in three States and finally 18 letters were sent to residents in all four States.
It is important to point out the relevance of the used sample. In fact, even if the number of the analysed letters can be perceived as low, taking into consideration the phenomenon of data breach, it is worth noticing that 213 letters represent 56,50% of the 377 cases collected totally in US in the same period by different sources, as the Data Breach Report 2014 (Identity Theft Resource Center, 2014) shows. Such high percentage can raise the question about under reporting. We will discuss about it in the conclusions.

3) Based on the content of the missive and on the characteristics isolated previously, create a database to code each letter characteristic, at paragraph level to understand the order of the letter contents, and at sentence level to identify the content and purpose. The database provides information on the following elements for each notification in the sample:

I) Type of Event: Definition of the event according to privacyrights.org that 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 email, fax or mail), physical loss (lost, discarded or stolen non electronic records, portable or stationary device), insider (someone with legitimate access intentionally breaches information - such as an employee or contractor), hacking and malware (electronic entry by an outside party, malware and spyware), payment card fraud (fraud involving debit and credit cards that is not accomplished via hacking), Unknown or other.
II) Type of PII: Identification of the kind of personal identifiable information accessed with a specification in the following categories: SSN, Financial information, Email / Password / User / ID card number, Personal Health Information.
III) Arrangement: Choice between direct and indirect patterns, indicating also the use of buffers.
IV) Components: Identification of each of the proposed components for evaluation, i.e.:
a) Clarity of the incident description and of the PII involved: **transparent** or **opaque** regarding both the description of the facts and the accessed PII. In case the date of the incident was not present in the description the terminology "**transparent no date**" was used.
b) Communication tone on the possible consequences: **alarming**, **neutral** and **reassuring** based on the sentences coding.
c) Approach to actions to be taken by the affected customers: encouraging or not (remaining **neutral**) customers' action to minimize their own harm, and subsequently the company's one.
d) Interaction with affected customer: encouraging contact with a contact person in the breached organisation (**fostering**), showing availability for contact (**available**) or being **neutral.**
These four elements define the prerequisites of the letter typologies and their various combinations by letter type will be illustrated below.

Additionally, information about further characteristics was collected to have a clearer picture of the phenomenon.
e) Stated relevance of security for the affected organization and stated steps to reinforce it: **medium** when only one of the two elements is included in the letter, **high** when both are stated and **none** if there is no mentioning at all about the importance of security for the organisation and about the steps taken or planned to reinforce it.
f) Style of addressing: use of the name and surname for a **personal** letter or initiating the notification with a general "dear customer" or no salutation at all for a **form** letter.

---

http://www.atg.state.vt.us/issues/consumer-protection/privacy-and-data-security/vermont-security-breaches.php

Also the presence of an **Annex** with additional information, the type of offered **apology**, any mentioning to **law enforcement** and **internal/forensic investigation** was recorded.

Finally, based on the specification, where present, of the dates respectively of the discovery of the data breach and of the (potential) access to Personal Information, the following time frames have been calculated per each notification letter:

- Time frame between data breach identification and data breach notification dates
- Time frame between data breach occurrence and data breach notification dates

4) Perform a data analysis aimed at investigating:

- possible schemes in the notifications sent
- the timing of such missive and their related usefulness to support a lower social harm

5. The dataset

The total number of 213 notifications has been analysed across all framework elements: each letter was classified in terms of type of event, type of PII, arrangement and options for components. The single notification elements were recorded using an inductive content analysis.

Type of event

Figure 3 shows the distribution of notifications based on the types of event that generated the data breach. As expected Hacking and Malware is ranked first. The second type of event, unintended disclosure, overwhelms with its magnitude accounting for ¼ of the total data breaches is. In the third and fourth place we find insiders and physical loss respectively, that have the same dimension. Finally payment card fraud not accomplished via hacking represents 2% of the sample.

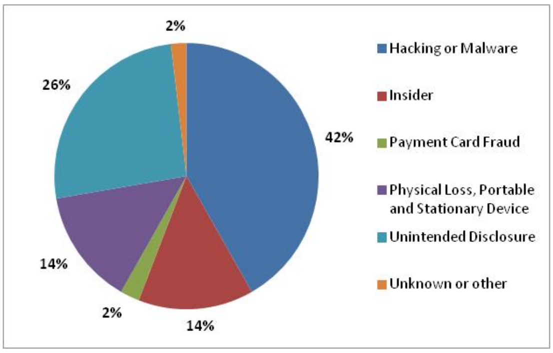


Figure 3 – Data sample by event

Type of PII

The dataset shows that the notified breach are related mostly to Social Security Number and financial information, including data/credit card details. In particular one letter out of two was related to breaches involving such data. Personal Health information and other Personal information were included in the 14% of the cases.

SSN	59,15%
Financial information	49,30%
Email / Password / User / ID	14,55%
Personal Health Information	13,62%

Table 2 – PII frequency

Arrangement

We look into the use of direct or indirect patterns and can compare it with the outcomes of the related debate in the communications textbooks. The analysis shows (Table 2) that the need to capture the attention of the reader immediately to foster its action prevailed in line with the suggestion given by the business communication authors to use indirect pattern in case of quite high stakes, for both writer and reader. The point here is that the stakes may become even higher if the reader is not "shaken" into action. 58% of the letters show the use of the direct pattern with opening buffers present in one notification out of three.

	Direct			Indirect			Total
Type of event	No Buffer	Buffer	Total	No Buffer	Buffer	Total	
Hacking or Malware	33	7	40	30	19	49	89
Insider	13	9	22	6	2	8	30
Payment Card Fraud	5	0	5	0	0		5
Physical Loss, Portable and Stationary Device	15	3	18	5	7	12	30
Unintended Disclosure	28	8	36	11	8	19	55
Unknown or other	3	0	3	1	0	1	4
Total	97	27	124	53	36	89	213
Total %	45,54%	12,68%	58,22%	24,88%	16,90%	41,78%	

Table 3 – Direct and indirect patterns

Components

Table 4 shows how the previously listed missive components characteristics are represented in the analysed sample. In most of the cases letters are transparent in describing data breach events and accessed PII. A neutral tone about the possible consequences of the breach is used in the majority of the cases (60,56%), even if one letter out of four tends to reassure individuals. Organisations do usually show availability towards 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 organisation (7,04%).

Characteristics	Options	Number of letters	%
Clarity of the incident description	Transparent	141	66,20%
	Transparent no date	56	26,29%
	Opaque	16	7,51%
Communication tone on the possible consequences	Alarming	27	12,68%
	Neutral	129	60,56%
	Reassuring	57	26,76%
Approach to actions to be taken by the effected customers	Encouraging action	79	37,09%
	Neutral	134	62,91%
Interaction with effected customers	Fostering	15	7,04%
	Available	182	85,45%
	Neutral	16	7,51%

Table 4 – Data breach notification characteristics – main components

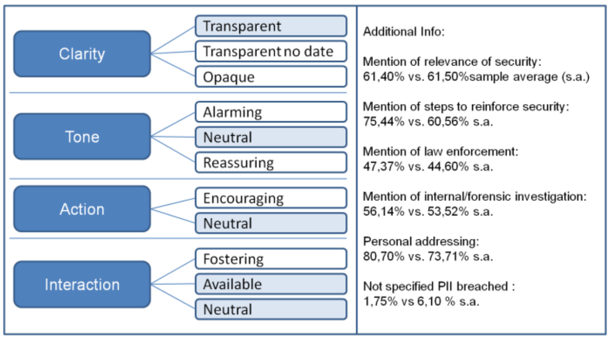
Table 5 indicates additional elements recorded and highlights how in the content of the letter, organisations prefer to stress both the importance of security (61,50%) and the steps taken to reinforce it after the breach (60,56%). In most of the cases the letters address the individuals by name and surname (73,71%) and not using a generic dear customer or similar. Annexes providing additional info are present in 109 letter out of 213, while law enforcement and internal investigation are mentioned respectively in 44,60% and 53,52% of the cases.

Characteristics	Options	Number of letters	%
Stated relevance of security	*Yes*	131	61,50%
	No	82	38,50%
Stated steps taken/planned to reinforce security	*Yes*	129	60,56%
	No	84	39,44%
Mention of law enforcemet	*Yes*	95	44,60%
	No	118	55,40%
Mention of internal investigation	*Yes*	114	53,52%
	No	99	46,48%
Clarity of the PII involved	*Transparent*	*200*	*93,90%*
	Opaque	*13*	*6,10%*
Style in addressing consumers	*Personal*	157	73,71%
	Form	56	26,29%
Presence of annexes	*Yes*	109	51,17%
	No	104	48,83%

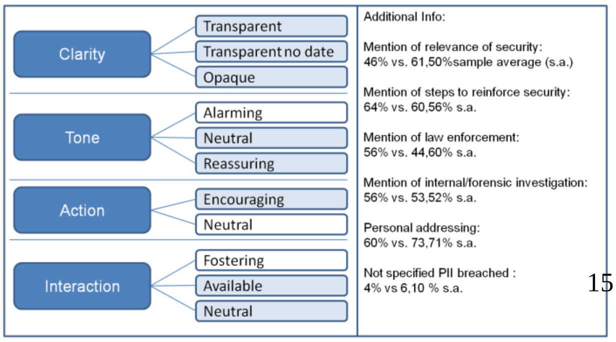
Table 5 – Data breach notification characteristics – additional components

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. In fact, the analysis of the available letters allows to determine the following 6 letter types, which cover almost 97% of the sample analysed as Table 6 shows.

1) Cold: The style is detached, explaining in a cold and transparent way the facts. It remains neutral in all elements of the missive, in particular when describing the consequences of the breach and the actions that might be initiated by the recipient of the letter. 24,41% of the letters belong to this group, where companies do not really take a position while communicating the data breach and do not strongly foster contact with customers.

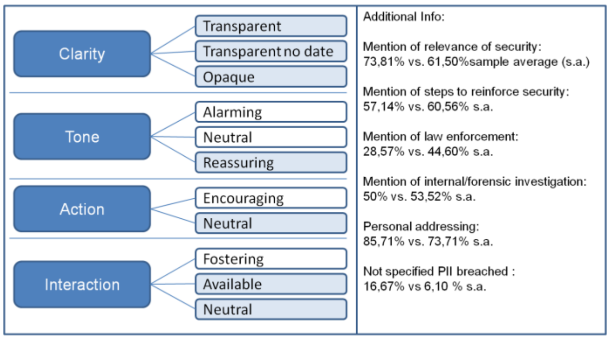


2) Routine: Companies present the event as a consequence of an unavoidable and rather common risk. The company stresses its actions, describing how all necessary steps after the event were duly performed. The consequences are represented with a neutral or reassuring tone, encouraging anyway a prompt action from customers. The company shows

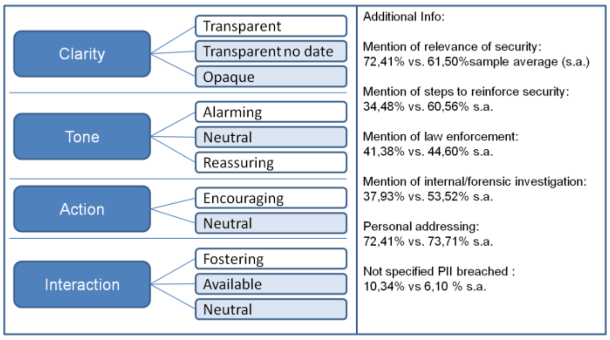


availability or neutrality towards the contact with customers. 23,47% of letters belong to this group.

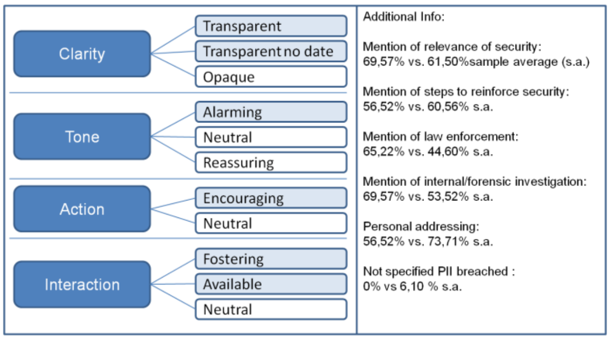
3) No worries: This letter gives emphasis on the minor risk generated by the event, reassuring the affected customer, listing options for possible customers action, but not recommending them. The interaction with the company is not fostered, given the reassuring tone of the missive about the consequences. 19,72% of letters belong to this group. The relevance of security for the company and the steps taken to reinforce are normally clearly stated in the letter.



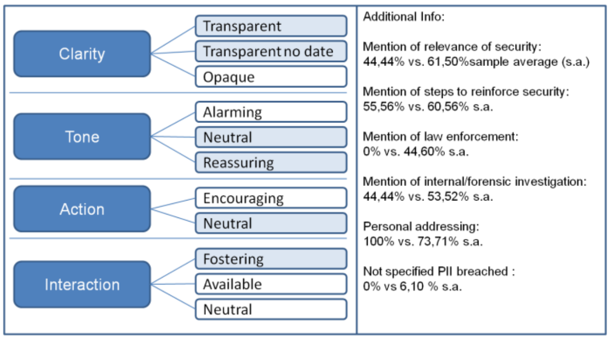
4) Junk: This letter can be easily exchanged for a junk message and therefore discarded from the moment the envelop is opened. The description of the incident is not clear, or if transparent no date about the occurrence of the incident is provided. The communication tone about the possible consequences and the approach to actions to be taken by affected customers is neutral. Those letters represent 13,62% of the sample.



5) Cooperation: The facts are clearly described. This letter gives emphasis to the actions taken by the organisation, while highlighting what actions need to be taken by individuals for their own safeguard. Usually a statement about the increase of security is included and the contact to the company is encouraged. One letter out of ten belongs to this group.



6) Supportive anyway: Even if the tone on 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, highlighting its supportive attitude (4,23%).



In the remaining 3,76% of the cases there is no evident red line among the different sections of the letter.

Type of event	**Cold**	**Routine**	**No worries**	**Junk**	**Cooperation**	**Supportive anyway**	**Other**	**Total**
Hacking or Malware	18	26	7	15	14	2	7	*89*
Unintended Disclosure	12	14	17	4	2	5	1	*55*
Physical Loss, Portable and Stationary Device	13	4	6	1	5	1		*30*
Insider	7	6	6	8	2	1		*30*
Payment Card Fraud			5					*5*
Unknown or other	2		1	1				*4*
Total	**52**	**50**	**42**	**29**	**23**	**9**	**8**	***213***
Total (%)	**24,41%**	**23,47%**	**19,72%**	**13,62%**	**10,80%**	**4,23%**	**3,76%**	**100%**

Table 6 – Data breach by event and letter type

6. Results

The decision about each single element and the resulting letter style represent the dilemmas that each breached organisation will have to face. While making their choices organizations have to take into consideration the clashing aspects of the breach notification: On one side to develop clear and effective notification letters in order to comply with the law informing the customer about the event, on the other side mitigating the potential harm to the company. Often the organization faces the supreme dilemma of minimizing concrete short term reputational effects or potential future damages due to customer churn and fines. There is no unique solution that can be adopted, but from the analysed data we can establish some preferred behavioural aspects on the side of the breached organisations. To better perform such a task we propose to classify the typology of data breaches according to the assumed decreasing company responsibility in the event. To enable such exercise we investigated the role of apology and its shades. We can in fact assume that at its core, an apology is marked by the organization accepting responsibility for the crisis and asking for forgiveness (Benoit & Drew, 1997; Fuchs-Burnett, 2002). A variety of additional components can be added to this definition including expression of remorse/sympathy, expression of regret, preventative measures, and reparation (Benoit & Drew, 1997; Cohen, 1999; Fuchs-Burnett, 2002; Patel & Reinsch, 2003). However clearly companies have at their disposal a wide range of communication strategies, starting from the apology strategy to those less accommodative ones such as giving no comment, denial, excuse, or justification (Bradford & Garrett, 1995; Dean, 2004; Lyon & Cameron, 1998). The less accommodative ones (partial apologies) are likely to resolve disputes in which the extent of each party's fault is unclear and would be difficult to establish. (Patel & Reinsch 2003). We will therefore assume that if a company decides to apologise, than it has admitted its responsibility for the event. We have investigated this aspect at sentence level. Use of sentences such as "we apologize", "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.

Type of event	Apology	Regret	none	Total	% of Apologies
Payment Card Fraud	5	0	0	5	100,00%
Unintended Disclosure	30	19	6	55	54,55%
Insider	16	9	5	30	53,33%
Physical Loss, Portable and Stationary Device	13	13	4	30	43,33%
Hacking or Malware	30	38	21	89	33,71%
Unknown or other	1	3		4	25,00%
Total	**95**	**82**	**36**	**213**	

Table 7 – Use of apologies

The results shown in Table 7 have been translated into 3 levels of responsibility: +++ high level of responsibility with over 50% of use of apologies, ++medium with over 40% of use of apologies, +low with less then 35%.

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 organisation involved. +++
2. Unintended disclosure: Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, 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 non electronic 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. +

Type of event	Cold	Routine	No worries	Junk	Cooperation	Supportive anyway	Other
Payment Card Fraud			100,00%				
Unintended Disclosure	21,82%	25,45%	30,91%	7,27%	3,64%	9,09%	1,82%
Insider	23,33%	20,00%	20,00%	26,67%	6,67%		
Physical Loss, Portable and Stationary Device	43,33%	13,33%	20,00%	3,33%	16,67%		
Hacking or Malware	20,22%	29,21%	7,87%	16,85%	15,73%	2,25%	7,87%
Unknown or other	50,00%		25,00%	25,00%			
Total	**24,41%**	**23,47%**	**19,72%**	**13,62%**	**10,80%**	**4,23%**	**3,76%**

Table 8 – Data breaches by event and letter type (%)

It is worth noticing that in the cases where a company could be more easily identified as ultimate responsible of the data breach, and therefore possibly subject to legal actions, the use of no worries letters in order to minimize the problem is present in high percentage. Specifically in 100% of the cases if payment card fraud, 30,91% of the cases for unintended disclosure, 20% if data breaches are generated by insiders and 20% if the physical loss was the origin of the potentially accessed PII. It is interesting that in case of junk letters the insider event shows a pretty high share of this letter type (26,67%). When the breach is generated by physical loss the cold letter type is used in the 43% of the cases.

	Clarity		Tone			Action		Interaction		
Type of event	Opaque	Transparent	Alarming	Neutral	Reassuring	Encouranging	Neutral	Available	Fostering	Neutral
Payment Card Fraud (5)	100%	0%	0%	0%	100%	0%	100%	100%	0%	0%
Unintended Disclosure (55)	2%	98%	5%	53%	42%	31%	69%	84%	9%	7%
Insider (30)	0%	100%	7%	67%	27%	27%	73%	97%	3%	0%
Physical Loss, Portable and Stationary Device (30)	0%	100%	17%	60%	23%	30%	70%	93%	3%	3%
Hacking or Malware (89)	9%	91%	19%	66%	15%	51%	49%	79%	9%	12%
Unknown or other (4)	50%	50%	0%	75%	25%	0%	100%	100%	0%	0%
Total	8%	92%	13%	61%	27%	37%	63%	85%	7%	8%

Table 9 - Data breaches by event and key elements (%)

Apart from the information that can be retrieved from Table 8, we believe that also looking at the core elements of the notifications as defined previously (clarity, tone, action, interaction), can add food for thought when investigating the choices made by organisation in case of data breach. In Table 9 we have an overview of these elements by type of event. Regarding **clarity** the great majority of missives show full transparency in describing the event. Only in case of Hacking or Malware we can recognise a significant percentage of opaque descriptions. Looking at the **tone**, the neutral option is adopted more frequently. The reassuring option is using in line with the company sense of responsibility (according to the previous proposed classification). Tthe more responsible it feels the more frequently it uses the reassung style. One third of the letters ecourage reader to take **action** to protect themselves. Only in case of Hacking or Malware costumers are encouraged to take action more frequently (50%). Finally, **Interaction** with costumers has a strong tendecy for availability. Only in case of Unintented disclosure and Hacking or Malware, a relevant percentage of the missives (9%) strongly push the customers to get in touch with the breached organisation.

A concluding aspect of the analysis is referred to the timing of the notification, the ultimate compliance dilemma for organisation.

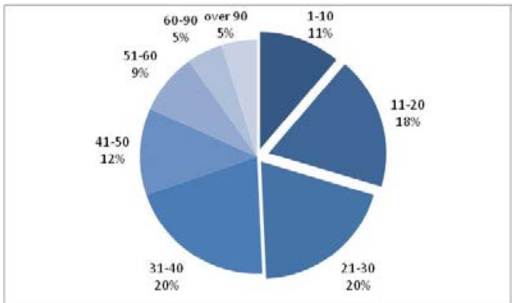


Figure 4 - Time span (days) between data breach discovery date and breach

Type of event	Date of DB discovery - date of DB notification	N. of notifications
Hacking or Malware	35,07	56
Insider	37,94	17
Payment Card Fraud	39,00	2
Physical Loss, Portable and Stationary Device	38,52	21
Unintended Disclosure	29,90	40
Unknown or other	41,67	3
	34,65	**139**

Table 10 – Average time span between data breach discovery date ad breach notification date

Only in 142 of the letters the time of the event identification is specified. This enables to calculate in days the average time from the discovery of the event to the moment of the communication to customers. The result[13] is 34,65 days (see Table 10), with 71[14] cases over one month.

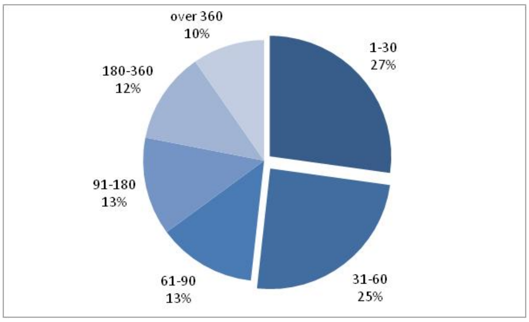


Figure 5 - Time span (days) between initial potential harm date and data breach notification date

Type of event	Date of DB notification - date of initial potential harm (days)	N. of notifications
Hacking or Malware	161,23	44
Insider	178,00	13
Physical Loss, Portable and Stationary Device	47,60	20
Unintended Disclosure	78,38	32
Unknown or other	60,00	1
	117,53	**110**

Table 11 – Average time span between initial potential harm date and data breach notification date

114 cases indicate also the date when the event 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 intentions. These data reveals an even more worrying situation. We identified in fact the average of 117 days[15] (see Table 11) between the communication and the day when the potential harm started, with 51[16] cases over 2 months.

Type of event	Date of DB discovery - date of initial potential harm (days)	N. of notifications
Hacking or Malware	131,45	29
Insider	133,17	6
Physical Loss, Portable and Stationary Device	1,85	13
Unintended Disclosure	22,24	25
Unknown or other	26,00	1
	70,50	**74**

Table 12 - Average time span between data breach discovery date and initial potential harm date

Finally, it is also important to point out the delay between the date of discovery and the begin of the potential harm, that can be calculated in 74 cases where both dates are available. The average amounts to 70,50 days while specific data breach types show great differences. Table 12 suggests to explore the opportunity to differentiate the approach by 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 4 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 rapidly.

7. 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 *right to know* (Schwartz & Janger, 2007), and 2) to provide a market based incentive for the enhancement of organisational information security measures in relation to the protection of personal information, "disinfecting" organisations of shoddy security practices (Ranger, 2007), the data presented above provide insights on the actual achievement of these objectives.

---

[13] once eliminated 3 outliers according to the z score rule

[14] Information extracted from the created database

[15] once eliminated 4 outliers represented by 4 insider cases, discovered more than 3 years after the potential data breach

[16] Information extracted from the created database

On the basis of the analysis performed it is still premature to indicate the most adequate letter type in response to these objectives, however we were able to picture interesting patterns related to the use of specific letters in response to specific events. These patterns suggest a tendency to belittle the event (no worries, junk) when the responsibility of the firm is unquestionable. In order to be able to complete the picture an investigation on actual customers' reactions and changes in companies' performance by letter type would be very relevant. This would confirm if different firm strategies – based on their decisions to the highlighted dilemmas – result in significantly different effects in terms of economic and financial impact on the customers' and firms' sides.

The conducted timing analysis alone shows that the first law purpose 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 towards customers, given the late notifying reaction by breached organisations. And the fact that many State statutes do not yet provide minimum mandatory information in terms of the content of the notification, provides organisations with elements of discretion that may not always support customers' conscious reactions to the breach.
Given the current framework it seems that data breach notification laws serve more as sunlight as disinfectant in the medium-long run than as effective and prompt contrast for identity thefts. 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, represent an opportunity to increase the support for contrasting the identity theft.

Another element worth to consider when evaluating control measures at central level is the limited number of publicly ascertained data breaches. Specifically, in the investigated timeframe (1.1.2014-30.6.2014) 377 data breaches were recorded in US[17] and 213 letters made publicly accessible through Attorney General websites. While this figure is comforting about the representativeness of the sample analyzed in this paper (also considering that the 213 letters were acquired for only four States which make them public) on the other hand this makes us reflect on the existence of a plausible high number of hidden data breaches, not disclosed by the companies towards customers.
In the past the topic of underreporting had been discussed and the inputs suggested that organizations might rather prefer to focus on profit margins instead of security of personal data. Therefore organizations underreport data breaches, mainly out of concern for the their business reputation.
Since 43 States are left out from the analysis (as they do not make notifications accessible), we would expect a much higher number than 377 as the total of data breaches in US in the analyzed six-month period. The organization that makes this data available, ITRC, states itself "we are certain that our ITRC Breach List underreports the problem"[18].

Additionally, considering the current statistics about cyber crime and cyber attacks[19] it is hardly conceivable that in a half year period less than 400 data breaches were registered across US.[20] According to a white paper[21] from ThreatTrack released in 2013, polling 200 security professionals in US enterprises, 57% had experienced a data breach that they did not disclose. According to the survey of about 300 attendees at RSA Conference, more than 89% of security incidents went unreported in 2007[22]. It is significant that also in dedicated reports such as the *2014* Data breach investigation report (Verizon, 2014), the dataset has been extended to all confirmed security incidents in 2013, over 63,000 globally, no longer restricting the analysis to confirmed data breaches only.

Junk styled letters, underreporting and the time spans analysis provided 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

---

17 http://www.idtheftcenter.org/

18 http://www.idtheftcenter.org/id-theft/data-breaches.html

19 In 2001, the annual total loss of complaints referred to the IC3 (Internet Crime Complaint Center) amounted to approximately 17.8 million U.S. dollars and grew to 781.84 million U.S. dollars in 2013. In 2012 the amount was 581,44 million U.S. dollars. Statista 2015

20 Note that Maine Attorney General only lists data breaches without providing letters for consultation. Maine was therefore not included in the analysis. This list allows us however to observe that adding a fifth state to the sample there would be additional 29 data breaches, bringing the total to 242 (64% of total data breaches then would be covered by 5 States out of 47)

21 Malware Analysts Have the Tools to Defend Against Cyber-Attacks, But Challenges Remain, Threattrack security, White Paper, November 2013

22 http://cybercrimeupdates.blogspot.it/2008/08/over-89-of-security-incidents-not.html /

practices, responding to the *right to know* and *sunlight as disinfectant* principles. As policy options to be implemented, with or without a federal data breach notification law, we would suggest the following:

- To act more firmly on the timing of communication establishing a proper system of control and sanctions. To date, the terminology used by the majority of State laws to set the timing of notification, i.e. *without unreasonable delay,* translate in a worrying 34 days after the discovery as the investigation shows;
- To motivate Authorities of the States that do not make data breaches public to do so, strengthening even more the second goal of the data breach notification laws, to act as sunlight as disinfectant. Additionally this would produce not only better analysis of the phenomenon, but also help to investigate more deeply on the different causes for the statistical mismatch between data breach and cybercrime trends and magnitude.
- To 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, in case of hacking or insiders, we estimated that organizations need 90 days more to identify a data breach in comparison to physical loss or unintended disclosure.

To conclude it is important to stress that there are additional opportunities for analysis of the collected data that might support further policy developments.

We could first focus on the reason why some data breach details are withhold by organisations. As an example we could start with 4 cases where even if the exact date of the data breach is known to the organisation (as it is present in the communication the company sent to the Attorney General on the same day) the organisation decided to omit this information in the notification to customers.

We could focus also on different reactions that specific events drive within organisations. As an example we could concentrate our attention on the accessed Personal Identifiable Information and investigate if the delay in notifying is driven by the type of PII present in the breached data. We would then discover that in the 66 cases where financial info is included in the accessed PII, the average time span from the discovery to the notification is 37,42 days, while in the remaining 68 cases the time span is 48,47 days. This would suggest that organisations are more reactive in notifying if customers' credit card or bank account details are accessed by third parties.

The scenarios of analysis are numerous and we suggest to investigate them in future works taking into account variables such as the number of affected individuals and the PII contained in the breached data. The value of such investigations is relevant not only for US, but also for other Regions facing the same problem, even if approached differently. One worth mentioning is Europe, currently dealing with important reforms regarding data privacy and security breaches. Despite the divergence between the concepts of personal data in the United States and the European Union (Schwartz and Solove, 2014), these analysis may add points for discussion in the light of the recent adopted European regulation[23] for providers of publicly available electronic communications services and its possible extension to other sectors. Art. 3 of this regulation states that when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall, in addition to the notification to the competent national authority, also notify the subscriber or individual of the breach. As the points highlighted in the annex II[24] (Content of the notification to the subscriber or individual) of the regulation cover the same elements described in the US Data Breach Notification Laws, we would take into great consideration the highlighted issues. One among all, we would like to underline the risk related to the timing of the notification as the term *undue delay* is also here present and not linked to the specified 24 hours-time set for the notification to a competent national authority "The notification to the subscriber or individual shall be made without undue delay after the detection of the personal data breach, as set out in the third subparagraph of

[23] COMMISSION REGULATION (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches. under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications

[24] 1. Name of the provider

2. Identity and contact details of the data protection officer or other contact point where more information can be obtained

3. Summary of the incident that caused the personal data breach

4. Estimated date of the incident

5. Nature and content of the personal data concerned as referred to in Article 3(2)

6. Likely consequences of the personal data breach for the subscriber or individual concerned as referred to in Article 3(2)

7. Circumstances of the personal data breach as referred to in Article 3(2)

8. Measures taken by the provider to address the personal data breach

9. Measures recommended by the provider to mitigate possible adverse effects

Article 2(2). That shall not be dependent on the notification of the personal data breach to the competent national authority, referred to in Article 2.“

References

Alred, G. J., Brusaw, C. T., & Oliu, W. E. (2011). The business writer’s handbook. Boston, MA: Bedford/St. Martin’s

Baker Hostetler (2014). State Data Breach Statute Form

Benoit, W. L., & Drew, S. (1997). Appropriateness and effectiveness of image repair strategies. Communication Reports, 10, 153–163

Bies, R. J. (2013). The Delivery of Bad News in Organizations: A Framework for Analysis. Journal of Management Vol. 39 No. 1, January 2013 136-162

Bies, R. J., & Shapiro, D. L. (1987). Interactional fairness judgments: The influence of causal accounts. Social Justice Research, 1: 199-218.

Bisogni, F. (2013). Evaluating Data Breach Notification Laws - What Do the Numbers Tell Us?. TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy, September 2013

Bovée, C. L., & Thill, J. V. (2012). Writing negative messages. In Business communication today (11th ed.). Upper Saddle River, NJ: Prentice Hall

Bradford, J. L., & Garrett, D. E. (1995). The effectiveness of corporate communicative responses to accusations of unethical behavior. Journal of Business Ethics, 14, 875–892

California Civil Code § 1729.98

Carter, C. (2012). Negative messages. In Keys to business communication: Success in college, career, and life. Upper Saddle River, NJ: Prentice Hall

Cohen, J. R. (1999). Advising clients to apologize. Southern California Law Review, 72, 1009–1073

Commercial Law League of America (2012). Data Breach Notification Laws by State

Conlon D. E., & Murray N. M. (1996). Customer perceptions of corporate response to product complains: the role of explanations, Academy of Management Journal, Vol.39, No. 4, 1040-1056

Creelman, V. (2012). The Case for “Living” Models. Business Communication Quarterly 75 (2) 192-207

Data breaches and identity theft (2005). Prepared statement of the Federal Trade Commission before the Committee on Commerce, Science and Transportation. US Senate 109th Congress.

Dean, D. W. (2004). Consumer reaction to negative publicity: Effects of corporate reputation, response, and responsibility for a crisis event. Journal of Business Communication, 41, 192–211

DeKay, S. H. (2012). Where is the research on Negative Messages. Business Communication Quarterly 75 (2) 173-175

EU Commission Regulation No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches. Under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications

Faulkner B. (2007). Hacking into Data Breach Notification Laws. 59 Florida Law Review

Fuchs-Burnett, T. (2002). Mass public corporate apology. Dispute Resolution Journal, 57(3), 26–32

GAO United States Government Accountability Office (2007). Personal Information. Data Breaches are frequent, but evidence of resulting Identity Theft is limited; however, the full extent is unknown. GAO Report to Congressional Requesters

Greenberg, J. (1990). Looking fair vs. being fair: Managing impressions of organizational justice. In B. M. Staw & L. L. Cummings (Eds.), Research in organizational behavior, vol. 12:111-157. Greenwich, CT: JAI Press

Hynes, G. E. (2008). Routine messages. In Managerial communication: Strategies and applications (4th ed.). Columbus, OH: McGraw-Hill

Identity Theft Resource (2014). 2014 Data Breach Reports

Javelin Strategy & Research (2011). Identity Fraud Survey Report: Consumer Version

Kolin, P. C. (2007). Successful writing at work. Boston, MA: Houghton Mifflin

Lehman, C. M., DuFrene, D. M. (2012). Delivering bad-news messages. In BCOM (3rd ed.). Mason, OH: South-Western/Cengage Learning

Lyon, L., & Cameron, G. T. (1998). Fess up or stonewall? An experimental test of prior reputation and response style in the face of negative news coverage. Web Journal of Mass Communication Research, 1(4). Retrieved May 1, 2015 from http://www.scripps.ohiou.edu/wjmcr/vol01/1-4a.htm

Loewenstein, G., John, L., & Volpp, K. (2012). Using decision errors to help people help themselves. In E. Shafir (Ed.), The behavioral foundations of policy. Princeton, NJ: Princeton University Press
Locker, K. O. (1999). Factors in reader responses to negative letters: Experimental evidence for changing what we teach. Journal of Business and Technical Communication, 13, 5-48
Locker, K. O., & Kienzler, D. S. (2010). Delivering negative messages. In Business and administrative communication (9th ed.). New York, NY: McGraw-Hill/Irwin
Mintz Levin (2012). State Data Security Breach Notification Laws
Patel, A., Reinsch, L. (2003). Companies Can Apologize: Corporate Apologies and Legal Liability. Business Communication Quarterly 66.1, 9-25
Perkins (2013). Security Breach Notification Chart
Pike, G. H. (2008). Legal Issues: Data Breaches Top the Agenda at RSA Conference
Ponemon Institute LLC (2012). 2012 Consumer Study on Data Breach Notification
Ranger, S. (2007, September 3). Data breach laws make companies serious about security.
Silicon.com. Available at http://management.silicon.com/itdirector/0,39024673,39168303,00.htm?r=1.
Romanosky, S., Telang R., & Acquisti, A. (2011). Do data breach Disclosure Laws Reduce Identity Theft?. Journal of Policy Analysis and Management, Vol. 30, No. 2, 256–286
Seeger, M. W., Sellnow, T. L., & Ulmer, R. R. (1998). Communication, organization, and crisis. In M. E. Roloff (Ed.), Communication yearbook (Vol. 21, pp.231-275). Thousand Oaks, CA:SAGE
Schwartz, P., & Janger, E. (2007). Notification of Data Security Breaches. 105 Michigan Law Review 913
Schwartz, P. M., & Solove, D. J. (2014). Reconciling Personal Information in the United States and European Union, 102 Cal. L. Rev. 877
Shwom, B. G., & Snyder, L. G. (2012). Communicating bad-news messages. In Business communication: Polishing your professional presence. Upper Saddle River, NJ: Prentice Hall
Threattrack security (2013) Malware Analysts Have the Tools to Defend Against Cyber-Attacks, But Challenges Remain. White Paper
Veltsos, J. R. (2012). An Analysis of Data Breach Notifications as Negative News. Business Communication Quarterly 75 (2) 192-207
Verizon (2014). 2014 Data breach investigations report

http://cybercrimeupdates.blogspot.it/2008/08/over-89-of-security-incidents-not.html /

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 framework setup
California
1 CA_pulte_homes.pdf
2 CA_BNY_Mellon.pdf
3 CA_sungard.pdf
4 CA_countrywide.pdf
5 CA_New_York_Life.pdf
6 CA_wells_fargo.pdf
7 CA_OSI.pdf
8 CA_modern_builders_supply.pdf
9 CA_Dept_general_services.pdf
10 CA_United_healthcare2.pdf
11 CA_DCA.pdf
12 CA_United_Healthcare.pdf
13 CA_Union_standard.pdf
14 CA_pillsbury.pdf

15 CA_dept_rehabilitation.pdf
16 CA_air_resources_board.pdf
Florida
1 FL_university_florida.pdf
2 FL_university_florida_2.pdf
3 FL_gap_inc.pdf
4 FL_lasalle_bank.pdf
5 FL_best_buy.pdf
6 FL_sungard_data_systems.pdf
7 FL_direct_marketing_services.pdf
8 FL_bank_atlantic.pdf
9 FL_certegy.pdf
10 FL_wyndham_hotels.pdf
11 FL_pfizer.pdf
12 FL_countrywide.pdf
13 FL_anheuser_busch.pdf
14 FL_lending_tree.pdf
15 FL_altman_weil.pdf
16 FL_florida_agency_workforce_innovation.pdf

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 Univeristy 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 Comsumers 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 Univ 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