Redesigning Data Breach Notifications for Consumer Comprehension and Actionability

Jamie Lai
University of Michigan
Ann Arbor, MI, USA
jllai@umich.edu

Michael Ni
University of Michigan
Ann Arbor, MI, USA
nimic@umich.edu

Yixin Zou
University of Michigan
Ann Arbor, MI 48105, USA
yixinz@umich.edu

Florian Schaub
University of Michigan
Ann Arbor, MI, USA
fschaub@umich.edu

CHI'20,, April 25–30, 2020, Honolulu, HI, USA
ACM 978-1-4503-6819-3/20/04.
https://doi.org/10.1145/3334480.XXXXXXX

Abstract
Data breach notifications are letters that companies are required to sent to affected individuals after a data breach. However, these notifications are often ineffective in motivating affected individuals to take appropriate reactive and protective actions. We present an enhanced data breach letter design that aims to improve comprehension and actionability of included information. We conducted a small-scale, between-subjects experiment comparing our design to a current breach letter. Our preliminary findings indicate that our design increases comprehensions and actionability and further provides insights for further design improvements to make data breach notifications useful and usable consumer protection tools.

Author Keywords
Privacy, security, data breach, notice design, usability.

CCS Concepts
•Security and privacy → **Usability in security and privacy; •Human-centered computing** → *Interaction design;*

Introduction
Data breaches are security incidents in which personal information is exposed or accessed without authorization. Data breaches can lead to identity theft, phishing attacks, and unwanted behavior manipulation on affected

Figure 1: Redesigned data breach notification letter: front page (*top*) and back page with recommended actions (*bottom*).

consumers, producing consequences such as financial loss and psychological trauma [4]. As a result, many countries have passed laws requiring companies affected by a data breach to send breach notification letters to potentially affected consumers. Consumers, however, tend to ignore these letters [7] and fail to adopt effective security practices [1]. Poor design of data breach notifications, including poor structure, lengthy paragraphs, incomprehensible text, and vague recommendations, likely factors into these inadequate responses by consumers [9].

We developed a new data breach notification design that aims to improve comprehension and actionability. Results from a preliminary evaluation study indicate that our new design outperforms current notices designs.

Related Work

Consumers learn about data breaches through various channels: news articles, television, social media, personal contacts, and the affected company [2]. However, data breach notifications sent by affected companies are problematic. They are lengthy and require advanced reading skills [9]. Visual emphasis (e.g., lists, tables, text markup) to help identify key information is rarely used [6, 9] and the use of hedge terms (e.g., "might" or "likely") downplay the risks of the breach and obscure whether the recipient was personally affected [8, 9]. While most breach notices recommend certain protective actions, their effectiveness or urgency is rarely communicated, leaving consumers overwhelmed by choices and them missing important measures that are hidden in unnoticeable places such as an appendix [9]. These issues cast doubt on whether such notices help consumers form accurate risk assessments of a breach and motivate them to initiate protective actions. Our work builds on the findings and recommendations by Zou et al. [9, 10] for improving the readability and actionability of breach notifications. Specifically, we designed a breach notification template that uses clear and concise language, explicitly prioritizes actions, and makes key aspects visually distinct.

Breach Notification Design

We developed our design based on representative examples of existing breach notification letters [9]. The design instantiation shown in Figure 1 is based on a breach notification letter sent by Rail Europe North America Inc. on April 30th, 2018. Our design makes improvements in the following four areas:

Structure/overview: We increased the font size difference between headers and paragraphs to create more information hierarchy, allowing the reader to more effortlessly follow the information flow. Headers (e.g "What Happened?") and recommended steps are highlighted in blue to mark the topic of each section and catch the reader's attention.

Conciseness: Current breach notifications are dense, which may intimidate and deter the reader from parsing through the information. On the front page of our design, information is condensed to a few lines under each header; on the back, a few sentences were used to describe each recommended action with checklisted steps beside it. Compared to the Rail Europe letter, we condensed the amount of text from four to two pages while retaining all key information.

Prioritization: Presenting choices in dense paragraphs can overwhelm the reader. We remedy this by numerically ordering the recommended steps from most to least urgent/effective. We list provided compensation (a free credit monitoring service for one year) first, followed by credit freeze, fraud alert, self-monitoring on credit reports, and obtaining additional information. We further used stylized arrows to guide the reader through the letter and the steps.

The reader would read the large, blue headers first, then read left to right, starting with “Why is this important?” and moving to the “What can I do?”

Actionability: Dense text and jargon can result in recommendations being inactionable for affected individuals. Our redesign removes unnecessary jargon and explicitly lays out each recommended step in a checklist form. We also bulleted and highlighted the breached information in gray to increase the urgency of the situation.

To instill credibility [3], we designed the front of our notification to appear formal (letterhead, formal address of recipient) while maintaining consistent formatting throughout (blue headers, bubbled icons, sans serif font).

Study Protocol

We conducted a preliminary between-subjects lab study comparing our improved design (treatment) to the original letter by Rail Europe North America Inc. (control). We made slight modifications to the original notification to ensure comparability: removing company name and logo to eliminate brand effects; including social security number as compromised information to justify the need for strong protective measures such as a credit freeze; adjusting the order of recommendations to make it consistent with the treatment condition.

We recruited 12 participants through online forums (e.g., Reddit, Craigslist) and university email lists. We used a screening survey to balance participants’ income, age, prior experience with data breaches – all of which might affect their reactions to breach notification letters. Participants were alternately assigned to the treatment or control group based on the order in which they were interviewed. 5 participants identified as men, 6 as women, and 1 as non-binary/gender fluid. The majority of participants were in their 20s and 30s with most in the 25–34 years range. Most of them studied or worked in a university setting with 10 having received a Bachelor’s degree or higher. 5 of them had prior experience with a data breach, and 5 had received a breach notification directly from an affected company.

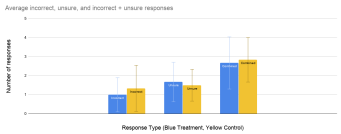

Figure 2: Average incorrect, unsure, and incorrect + unsure responses

Participants were asked to read the breach notification letter corresponding to their condition (control or treatment) at their own speed. Afterwards, participants completed a short questionnaire that assessed their comprehension of the letter’s content (e.g., date of the breach; what credit bureau to contact for credit freeze). Then, we interviewed participants regarding their intended reactions to the letter if they were the recipient, as well as their opinions of certain design features. Each session lasted 45-60 minutes.

Preliminary Findings

We next discuss our findings in terms of notice comprehension, attitudes toward the breach, intended reactions to the breach notification, and perceptions of certain design features.

Notice Comprehension

After scoring each participant’s answers to the comprehension questionnaire, we calculated the mean, median and mode for each group. The control group answered more questions inaccurately on average (1.33) than the treatment group (1). The median and the mode for the incorrect answers were higher for the control group as well (1.5, 1 and 2, 1 respectively). If we included the “I am not sure” response option, which the control group selected less often (1.5) than the treatment group (1.67), the control group still had more incorrect and unsure responses on average than the treatment group (2.83 > 2.67). In general, the median and mode of unsure and incorrect responses for the

treatment group are less than or equal to those of the control group. The data for incorrect responses for the control group is more varied than that of the treatment group (standard deviation: 1.21 vs. 0.89); however, the control group's data was less varied for unsure responses (0.83, 1.03) and for incorrect and unsure responses (1.16, 1.36).

Overall, the treatment group performed slightly better on the comprehension questions than the control group. All participants were unsure on at least one question, but when combining the incorrect and unsure responses, participants seemed to struggle on up to half of the comprehension questions. This general incomprehension resurfaced during interviews, with some participants misunderstanding how an action can be beneficial and with most participants feeling overwhelmed. The control and treatment letters were indeed informative in that regard, but may have tested participants' reading skills.

Several confounding variables may also be at play, including the participants' prior exposure to data breaches, level of education, time of day, test-taking ability, and pressure management ability (questionnaires were completed before an interviewer). In the future, we hope that a broader and more numerous pool of participants will allow us to draw more definite conclusions.

Attitudes Toward the Breach

Participants in both treatment and control conditions were confused about the difference between fraud alert and credit freeze. They believed that the chance of their information actually being compromised was low, and felt most worried about Social Security number (SSN) being involved. Some participants felt more alarmed and were more proactive about their data, and other participants were less sensitive about the breach in both groups. Most participants, except for P1 and P12, believed that their data were unlikely to be compromised in a data breach. P4 mentioned that the number of people affected impacts how likely their data will be misused. These participants (all except P1 and P12), however, asserted that they'd still take protective measures to ensure nothing went wrong. Nine participants acknowledged that the exposure of their SSN was the most alarming motivating factor to enact the recommended protective actions. Interestingly, all noted that if the SSN remained secure, they would simply cancel the card breached, void any inaccurate transaction, or take other less precautionary measures.

In particular, more participants in the control condition felt overwhelmed by the sheer amount of information they needed to read compared to the treatment condition. Four noted that they mostly skimmed through the letter after reading the type of information compromised in the front and the bolded words on the back. Only two participants in the treatment group expressed similar feelings.

We also asked to what extent participants felt the notification was personalized to them, and how the breach might impact their relationship with the company. The two groups shared similar thoughts; both believed that the notification was fairly impersonal. 5 participants mentioned wanting a more user-centered letter, featuring a more apologetic tone and explicit assurances that a breach will never happen again, which was absent in the original notification and therefore not included in the treatment. Because of this broken trust, these participants said they would rather look elsewhere for guidance, like the Internet or over the phone. Other participants noted the lack of personalization, but did not view it as a negative; they understood that the notification is meant to be mass-produced, thus limiting the need for personalization.

Intended Reactions to the Breach Notification
Five participants from both groups, when asked what recommended steps they would take, admitted that they could not distinguish between a credit freeze and a fraud alert. This left them frustrated and uncertain on which recommendations to take. Six participants were skeptical of a credit freeze, worrying that it would be overly burdensome to enact. P1 noted that they are currently completing a major financial transaction, and believes that a freeze may complicate it. Conversely, P8 mentioned that since they were not taking loans, they would enact a credit freeze. Because of the perception that placing and maintaining a credit freeze was too overwhelming and time-consuming, these six participants believed that the hassle of the freeze outweighed the potential benefits. The greatest factor that influenced our participants' behavior was the time required to initiate the protective actions. Six participants mentioned that they have busy lives, and a letter like this would easily be ignored; the actions might require significant time and effort, especially when dealing with bureaucracy, and they would rather delay taking action.

The complaints about "compliance budget" [5] were particularly salient in the control group. Three mentioned that, after seeing long paragraphs of text, they would immediately save the letter for later. P4 mentioned that they would have "ambient anxiety" – still worrying about the breach, but being unwilling to take action. P1 and P9 asserted that they would refer back to the treatment condition for future use, with P1 mentioning that "if [they] put [it] down in a pile of mail, [it] would stand out."

Three participants in the control group stated that they would probably call the company and speak to an individual to get more "layman terms" on what happened. This implies that they did not fully understand the contents of the letter, and felt much more at ease speaking to a human correspondent.

Opinions Toward Design Features
Participants in the treatment group emphasized design features that aided them with comprehension more frequently than the control group. All participants mentioned color, checkboxes, and headers as key features supporting comprehension. The blue coloring was appreciated by three participants, with P1 mentioning that anything brighter or warmer would "look like a weird ad." P5, however, believed that the notification needed brighter colors to convey urgency to readers. All treatment participants mentioned that the grey on the front page highlighting the compromised information drew their attention, effectively giving more weight to the subject matter.

Participants approved the use of headers and checkboxes. All treatment participants said the headers helped chunk the letter and more clearly partitioned the different sections. However, P7 mentioned that the headers seemed too large and distracting, diverting focus from the important information underneath.

All treatment participants, excluding P7, found the checkboxes appealing and understood its intent to promote productivity. P3 and P9 noted that, with the checkboxes, they would be more likely to follow the instructions because they were laid out clearly. The arrows and icons, however, did little to improve readability. P11 noted that the icons were distracting and diverted their attention away from the content. In many cases, the arrows did little to assist information flow; three participants described their reading order, which contradicted with how the arrows were supposed to work.

By contrast, little was said about the control notification beyond its front page headers and its use of bolding.

Limitations

Despite wide-ranging recruitment efforts, our sample consisted mostly of young and educated adults. As for next steps, we aim to recruit more participants, especially more older adults and/or individuals with lower levels of education and income, which will shed light on accessibility issues of breach notifications. We will keep refining our notification design, narrowing down to a smaller set of design features and compare the differences they make on participants' comprehension, attitude and intended behavior quantitatively, empowered by larger sample size.

In our lab setting, participants may have over-claimed their security concerns and intended actions due to social desirability bias. Likelihood of understating also exists, given that they were not the actual recipient, and were only reporting what they thought they might do hypothetically.

Future Design Improvements

Based on our findings, we recommend the following suggestions to increase comprehension and actionability:

Comprehension

Explain the difference between credit freeze and fraud alert. There was already a blurb distinguishing between freeze and alert in the treatment notification, but many participants were nevertheless unable to discern the difference. Many participants also wanted to receive a follow-up letter with updates and results regarding the breach investigation. This information seemed more useful for psychological ease than actionability, but might still increase customer trust. Use more concise language and chunk information using color, headers, and different font sizes. Section each key piece of information off into 1-3 sentences with large, colored headers. Different font sizes should also be used to increase information hierarchy, as well as highlighting and bulleting the affected information in the letter.

Actionability

Add a summary of the recommendations on the front of the page. This will give busy and impatient readers a preview of the back, so they know what to expect and do. Write in a more apologetic tone, since consumers' trust in the company has been compromised along with their information in the breach. A candid and explicit apology is likely to remedy the damage. List possible repercussions of the data breach. P3 mentioned that they knew SSN was important, but could not pinpoint what risks would be associated with it. Several other participants had the same sentiment, showing that they do not have a clear understanding of the possible repercussions of a stolen identity. By explicitly stating these risks, consumers may feel a greater urgency to take action. Increase actionability with the use of checklists. A checkbox is a simple motivator to do each step and gives consumers the ability to gratifyingly check off steps when completed.

Conclusion

Data breach notifications can be a useful tool for consumers in the event of a breach, but the notifications themselves need to be engaging and informative enough to motivate affected individuals to take action. Our research shows promising avenues for increasing consumer comprehension and actionability of data breach notifications.

REFERENCES

[1] Lauren Cole. 2017. After the Equifax breach, consumers were advised to freeze their credit — but almost no one did it. https://www.businessinsider.com/equifax-credit-freeze-2017-9. (Sep 2017).

Last accessed on: 01.01.2020.

[2] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 1.

[3] BJ Fogg and Hsiang Tseng. 1999. The elements of computer credibility. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*. ACM, 80–87.

[4] Simon Frankel, Robert Fram, and Amanda Lynch. 2015. *Standing in Data Breach Cases: A Review of Recent Trends*. Technical Report. Last accessed on: 03.17.2019.

[5] Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*. ACM, 133–144.

[6] Alexander Jenkins, Murugan Anandarajan, and Rob D'Ovidio. 2014. 'All that glitters is not gold': The role of impression management in data breach notification. *Western Journal of Communication* 78, 3 (2014), 337–357.

[7] Ponemon Institute. 2014. *The Aftermath of a Data Breach: Consumer Sentiment*. Technical Report. Ponemon Institute LLC.

[8] Jennifer Veltsos. 2012. An analysis of data breach notifications as negative news. *Business Communication Quarterly* 75, 2 (2012), 192–207.

[9] Yixin Zou, Shawn Danino, Kaiwen Sun, and Florian Schaub. 2019. You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 194.

[10] Yixin Zou and Florian Schaub. 2019. Beyond Mandatory: Making Data Breach Notifications Useful for Consumers. *IEEE Security & Privacy* 17, 2 (March 2019), 67–72. DOI: http://dx.doi.org/10.1109/MSEC.2019.2897834