Editors: Heather Richter Lipford, richter@uncc.edu | Jessica Staddon, jessica.staddon@gmail.com

Beyond Mandatory: Making Data Breach Notifications Useful for Consumers

Yixin Zou and Florian Schaub | University of Michigan School of Information

Data breaches pose significant security and privacy risks to affected consumers. However, it is doubtful whether data breach notifications mandated by respective laws effectively inform consumers of risks stemming from a data breach and motivate them to take protective actions.[5,8,12] We analyze potential reasons for consumers' inaction after a data breach and discuss how data breach notifications and respective requirements should be improved.

Consumer Inaction After Data Breaches

A range of measures can help consumers limit harm from data exposed in a breach. Consumers can accept free identity protection services offered by the breached company, place a credit freeze or fraud alert on their credit report, change compromised passwords, closely monitor their credit reports and financial accounts, and adopt security best practices, such as strong passwords and two-factor authentication.

Yet empirical evidence suggests consumers do not take adequate protective actions when affected by a data breach. In a 2014 U.S. national survey, the concern for being an identity theft victim increased by 21% following a breach, yet 32% of respondents reported their reaction to a data breach notification is to "ignore it and do nothing."[8] Two thirds of respondents in a 2017 worldwide survey reported similar identity theft concerns;[5] nevertheless, 56% continued using the same password for multiple accounts, and 41% did not adopt two-factor authentication when offered.[5] A positive exception is RAND's 2016 U.S. national survey, in which 62% reported accepting offers of free credit monitoring, a higher but still not satisfactory number.[1] Together, these studies suggest a dissonance between attitudes and behaviors around data breaches: awareness and concerns about privacy and security risks are not reflected in consumers' behavior.

Using Equifax's 2017 data breach as a case study, a breach that exposed sensitive personal information of almost half the U.S. population (145 million), we studied reasons behind people's inaction after a data breach through semistructured interviews.[12] Most participants were aware of the breach and associated risks, such as identity theft and privacy invasion. Nevertheless, only 10 of 24 participants had checked whether they were affected on Equifax's website, and only four took protective measures, such as freezing their credit reports and using identity theft protection.

Their inaction was not driven by a lack of risk awareness but rather

Digital Object Identifier 10.1109/MSEC.2019.2897834
Date of publication: 2 April 2019

by cognitive and behavioral biases. For instance, many participants exhibited optimism bias, assuming that identity thieves would choose and target data breach victims who are more affluent or have a better credit history than themselves. Some participants described a retroactive approach to dealing with risks: they saw nothing unusual happening to them after the breach as reassurance that no action was needed. Moreover, taking one action, such as freezing one's credit, can lead to a false sense of security, making it less likely to engage in additional protective actions, such as monitoring one's credit report or bank accounts, even though those participants were aware that a credit freeze could not eliminate all risks.

Additionally, participants' actions were heavily influenced by extrinsic factors, such as cost of protective measures. Actions with no cost, like checking Equifax's website and self-monitoring one's credit reports and accounts, were favored. Conversely, some participants refrained from freezing their credit report due to associated fees (US$3–10 by the time we conducted the study). It also matters how participants were made aware of the breach and available measures. Participants who took actions primarily followed advice from family members, colleagues, and trusted experts. News media helped enhance the awareness of the breach but did not necessarily prompt actions.

Furthermore, many participants struggled with the specialized terms used to describe protective measures and therefore discounted their applicability. For example, participants misconceptualized a credit freeze as "freezing credit cards" (12 out of 24) and a fraud alert as an "alert sent by banks and credit card companies when fraudulent activities occur" (21 out of 24). This begs the question: are current data breach notifications presenting protective measures in ways that are understandable and actionable?

Issues With Data Breach Notifications

Bisogni[3] found a lack of clarity in data breach notifications regarding the incident description, the types of information exposed, and the number of affected consumers; moreover, some companies use a reassuring tone to depict the consequences of a breach to limit the effects on their reputation. Building on this prior work, we conducted a content analysis of 161 data breach notifications to consumers[11] retrieved from the Maryland attorney general,[13] most of which (154) were letters. We identified several issues that may contribute to consumer inaction by hampering comprehension, risk perception, and intention to take action.

- *Poor readability*: The median of our sample's Flesch–Kincaid grade level was 10 (minimum 6.4, maximum 16), meaning that the text requires the reading abilities of a 10th grader. This is higher than what is recommended for materials addressed to the general public (i.e., seven to nine).[6]
- *Prevalent yet inconsistent headings*: 67% of the analyzed notifications (106) used headings to structure text into sections. However, the use of headings did not necessarily support readability, as they were often printed at the beginning of paragraphs or with little white space separating them from text.
- *Scarcity of visual emphasis*: When presenting recommended actions, list formats were common in sublevel text (e.g., details of a specific action) but not at the top level (e.g., different actions), hampering the reader's ability to gain an overview of available actions. Additionally, duration of benefits and enrollment deadlines of free identity protection, if provided, were often not highlighted by text formatting (e.g., bolding) despite their significance.
- *Many recommendations without priorities*: Multiple recommendations are usually described in long paragraphs, with little to no guidance on prioritization. Comparisons between different actions are rarely provided, leaving consumers overloaded with choices, even though some recommendations are more effective than others (e.g., credit freeze versus fraud alert; see Figure 1).
- *Downplaying risks*: Some companies claimed that there was "no evidence" that breached data had been misused, providing potentially false assurance regarding the likelihood of harm occurring. Moreover, hedge terms such as "probably," "might," and "likely" are frequently used when describing whether the consumer was affected, for example, "the information potentially involved in the incident may have included your name, credit or debit card number, and card expiration date."

Making Data Breach Notices More Effective

Our research indicates that how consumers are informed about a data breach and what actions they should take are likely to have substantial impacts on consumers' propensity to act. We argue that more emphasis should be placed on supporting consumers in protecting themselves after a data breach rather than merely informing them about the breach. We discuss opportunities for improving the utility and usability of data breach notifications to make them an effective mechanism for helping consumers mitigate potential risks.

Readability Expectations Beyond "Plain Language"

Current data breach notifications fail to comply with the "plain

language" requirement established in the General Data Protection Regulation and California's breach notification law. A potential reason may be that these laws do not clearly define how to assess whether something is written in plain language. Regulators should provide specific guidance on how this plain language requirement can be achieved, including recommended actions such as using short sentences, common words, and active voice. Furthermore, lessons can be borrowed from the insurance industry, where the Flesch reading ease score test is required as a readability assessment of insurance policies in some U.S. states.[6]

Delivering Notices Through Multiple Channels

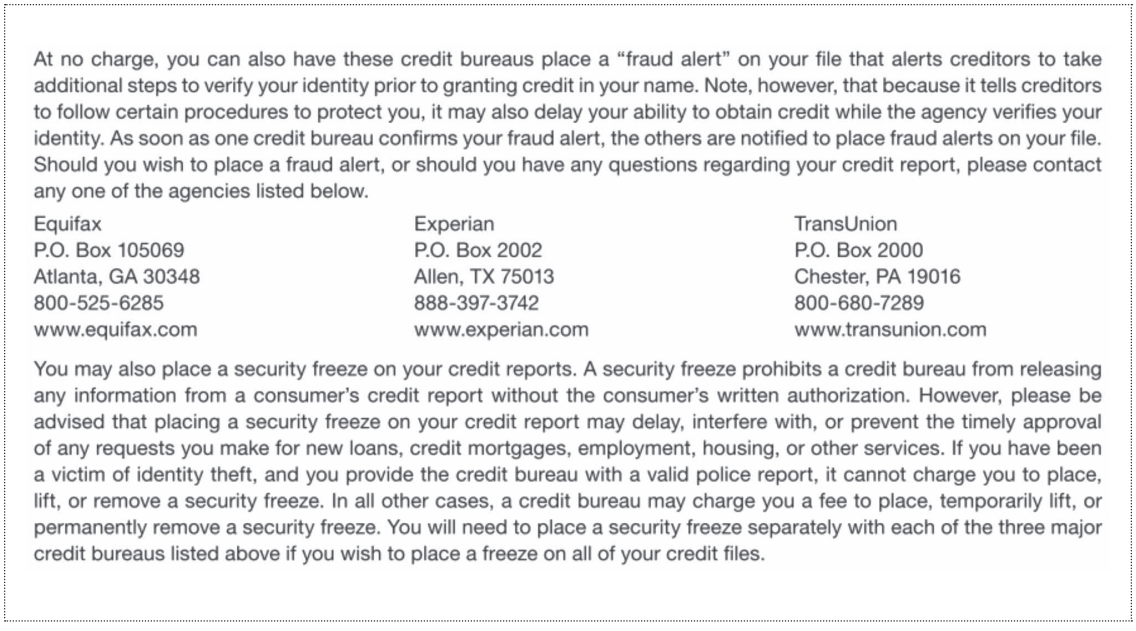
Currently, most U.S. state laws require written notices sent to affected consumers after a data breach; 96% of the data breach notifications we analyzed were mailed letters. Electronic notices (e.g., emails, website announcements, and notices to statewide media) are treated as substitutes when the cost of delivering mail is too expensive or the physical addresses of affected individuals are unavailable. However, the slow speed of mailed letters might increase the uninformed exposure time to potential risks for consumers.[3] This might explain why many consumers learn about a data breach even before receiving direct notifications from companies.[1] Conversely, electronic notices not only are faster but also have the advantage of providing consumers with direct links to action, thus reducing barriers in moving from intention to taking an action. The nature of electronic methods (a small screen if displayed on a mobile device, allowing less text) may also incentivize companies to shorten the text and increase aesthetics. This, of course, needs to be compounded with clear readability requirements to prevent companies from sending lengthy and unreadable electronic notices.

Consistent Standards for Style and Format

Even though our primary data source pertained to Maryland, most analyzed notifications with section headings adhered to wording required by California's breach notification law (California Civil Code section 1798.82). This indicates a promising avenue for standardizing style and format expectations for data breach notifications. Legislators and regulators should provide specific content and style requirements, potentially templates that have been validated in terms of readability and usability based on rigorous user testing. The requirements of California's data breach notification law and the Gramm–Leach–Bliley Act model privacy notice[4] demonstrate the reach and influence of official templates—but it has to be ensured that they are usable and actionable.

Using Visual Emphasis to Enhance User Experience

Formatting makes information visually accessible and enhances the



At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
800-680-7289
www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files.

Figure 1. An example of recommendations with poor actionability. The introduced measures (fraud alert and security freeze) are hidden in lengthy paragraphs without headings or highlighting or any indication of which one to prioritize. This image is obtained from a data breach notification in the breach notice database[14] on the Maryland Attorney General website.

overall user experience. We suggest text formatting should be effectively used to highlight crucial information along with a consistent use of list formats to lay out major actions. When lists are used, each point should be followed by short and succinct sentences, instead of long paragraphs, to keep the cognitive burden low for readers. Furthermore, it is important to consider the needs of special groups,[10] such as visually impaired people, which means the content should be displayed in a sufficiently large font size, be accessible to screen reader devices, and contain required metadata and text descriptions.

Communicating Risks Clearly and Concisely

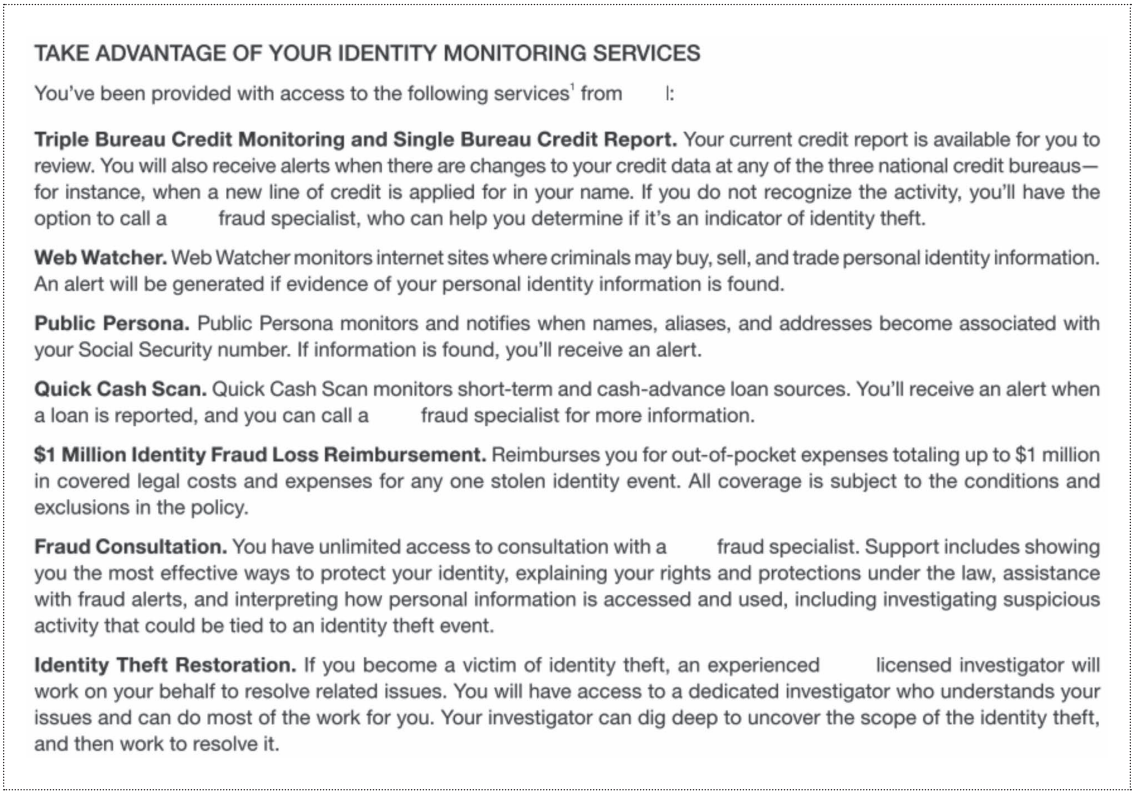
Risk communication is critical to data breach notifications because risk perception is the precursor for forming the intention to take action. Risk communication is also challenging because companies need to help consumers correctly assess risks and determine the necessity to take action while avoiding overstating of risks, which might harm their business interests. Privacy and security nudging literature[2] provides valuable insights for improving risk communication in data breach notifications. For instance, optimism bias could be addressed by removing hedge terms to make it clearer that the reader is personally affected by the breach. Loss aversion theory (i.e., people hate loss more than liking the equivalent gain) can be leveraged when framing the outcome of recommended actions by emphasizing negative consequences of inaction. We also found that people with low socioeconomic status, due to their limited money or assets, may subscribe to an "I've got nothing to lose" attitude, lacking motivation to react.[12] This fallacy could be addressed by describing how people the reader relates to have been affected by the consequences of data breaches, such as showing evidence of their susceptibility to identity theft and scams. Essentially, companies should be as clear as possible about whether the recipient has been affected and avoid "no evidence of data misuse" claims or at least combine them with clear warnings of potential future misuse.

Supporting Consumers in Prioritizing and Executing Actions

Jargon in naming as well as lengthy yet confusing descriptions of protective actions likely hamper consumers' ability to act, as they struggle to understand the functions and importance of recommended actions. When making recommendations, companies should identify and highlight those most relevant to the specific breach. Leveraging the anchoring effect,[2] actions of high priority should be listed first so they receive the most attention from readers. Moreover, companies should provide a clear rationale for why a certain action is important rather than merely listing out what is included in a recommended service (see Figure 2 for a counterexample). To deal with the choice overload problem, companies need to adjust their recommendations rather than blindly adopting a given template. For instance, in analyzing notifications to Maryland consumers, we often observed long lists of contact information for other state attorney general offices, which are unnecessary details, at least for Maryland residents, that should be removed.

Research on privacy policies has identified their deficiencies in communicating privacy risks: most are written in lengthy paragraphs filled with jargon and ambiguity, leading readers to struggle with comprehending the content and forming accurate mental models.[9] Our research reveals that data breach notifications, unfortunately, suffer from similar issues, yet we have a limited understanding of how these issues may impact users' comprehension and reactions in a moment when they are most vulnerable—after their information has been exposed in a data breach. Although data breaches are recognized as severe threats, the design of corresponding mandatory notifications has received little attention. Poor readability and actionability, compounded by ambiguous risk communication, are possible explanations for data breach fatigue, when consumers take little to no action after receiving a data breach notification. We outline directions for more effective data breach notifications that can help consumers overcome hurdles in dealing with risk and take action to adequately protect themselves. More research is needed to develop and validate best practices for successfully guiding consumers toward safety after a data breach.

Companies that suffer a data breach could leverage actionable data breach notifications to maintain or restore consumer trust. For them, the intuition to hedge about the consequences of a breach to prevent eroding consumer trust is understandable but misguided. In fact, in RAND's survey, consumers were generally satisfied with companies' postbreach handling, whereas only 11% terminated the business relationship.[1] Research has shown that making apologies and using visual elements in data breach notifications can enhance a company's perceived reputation.[7] Building on this, we argue for acknowledging risk openly and providing clear and actionable recommendations as indicators for a company's sincerity in protecting their customers' security and privacy. Although data breaches are irreversible and an unfortunate reality, providing consumers with understandable and actionable notifications, which clearly communicate associated



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from I:

Triple Bureau Credit Monitoring and Single Bureau Credit Report. Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher. Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona. Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan. Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement. Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation. You have unlimited access to consultation with a fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

Figure 2. The description of credit monitoring and identity restoration services, which was provided free to affected consumers by several companies. The description only states what is included but not why it matters to enroll and receive the benefits. This image is obtained from a data breach notification in the breach notice database[14] on the Maryland Attorney General website.

risks and available measures, offers mutual benefits for both companies and consumers. ■

References

1. L. Ablon, P. Heaton, D. C. Lavery, and S. Romanosky, "Consumer attitudes toward data breach notifications and loss of personal information," Rand Corporation. Santa Monica, CA, 2016. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf
2. A. Acquisti et al., "Nudges for privacy and security: Understanding and assisting users' choices online," *ACM Comput. Surv.*, vol. 50, no. 3, pp. 1–41, 2017.
3. F. Bisogni, "Proving limits of state data breach notification laws: Is a federal law the most adequate solution?" *J. Inform. Policy*, vol. 6, no. 1, pp. 154–205, 2016.
4. Federal Trade Commission, "Final model privacy form under the Gramm–Leach–Bliley Act: A small entity compliance guide," FTC. Washington, DC, 2009. [Online]. Available: https://www.ftc.gov/sites/default/files/documents/rules/privacy-consumer-financial-information-financial-privacy-rule/model_form_rule_a_small_entity_compliance_guide.pdf
5. Gemalto, "Databreachesand customer loyalty 2017," Gemalto. Belcamp, MD, 2017. [Online]. Available: https://safenet.gemalto.com/resources/data-protection/data-breaches-customer-loyalty-report-2017/
6. M. Hochhauser, "Lost in the fine print: Readability of financial privacy notices," Privacy Rights Clearinghouse, 2001. [Online]. Available: https://www.privacyrights.org/blog/lost-fine-print-readability-financial-privacy-notices-hochhauser
7. A. Jenkins, M. Anandarajan, and R. D'Ovidio, "'All that glitters is not gold': The role of impression management in data breach notification," *Western J. Commun.*, vol. 78, no. 3, pp. 337–357, 2014.
8. Ponemon Institute, "The aftermath of a data breach: Consumer sentiment technical report," Ponemon Institute. Traverse City, MI, 2014. [Online]. Available: https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf
9. A. Rao, F. Schaub, N. Sadeh, A. Acquisti, and R. Kang, "Expecting the unexpected: Understanding mismatched privacy expectations online," presented at the Symp. Usable Privacy and Security (SOUPS) 2016. [Online]. Available: https://www

.usenix.org/conference/soups2016/technical-sessions/presentation/rao
10. Y. Wang, "Inclusive security and privacy," *IEEE Security Privacy*, vol. 16, no. 4, pp. 82–87, 2018.
11. Y. Zou, S. Danino, K. Sun, and F. Schaub. "You 'might' be affected: An empirical analysis of readability and usability issues in data breach notifications," in *Proc. 2019 CHI Conf. Human Factors Computer Systems*, to be published.
12. Y. Zou, A. H. Mhaidli, A. McCall, and F. Schaub. "'I've got nothing to lose': Consumers' risk perceptions and protective actions after the Equifax data breach." *Proc. 14th Symp. Usable Privacy and Security (SOUPS)*, 2018, pp. 197–216. [Online]. Available: https://www.usenix.org/system/files/conference/soups2018/soups2018-zou.pdf
13. Office of the Attorney General, Maryland, "Maryland information security breach notices," 2019. [Online]. Available: http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx
14. Office of the Attorney General, "Maryland information security breach notices," Maryland Government. Accessed on: Feb. 20, 2019. [Online]. Available: http://www.marylandattorneygeneral.gov/pages/identitytheft/breachnotices.aspx

Yixin Zou is a Ph.D. student at the University of Michigan School of Information. Her research interests include usable privacy and security, particularly designing interventions that motivate users to take action in the face of privacy and security threats. Zou received a B.S. in advertising from the University of Illinois at Urbana–Champaign. Contact her at yixinz@umich.edu.

Florian Schaub is an assistant professor at the University of Michigan School of Information. His research interests include privacy, security, and human–computer interaction research to understand privacy and security behaviors and empower individuals to effectively manage their privacy and security in complex sociotechnical systems. Schaub received a doctoral degree in computer science from the University of Ulm. He is a Member of the IEEE, Association for Computing Machinery, and International Association of Privacy Professionals. Contact him at fschaub@umich.edu.

Digital Object Identifier 10.1109/MSEC.2019.2903677