Lengthy, Vague, and Inactionable: Issues with Data Breach Notifications and Implications for Public Policy

Yixin Zou, Shawn Danino, Kaiwen Sun, Abraham H. Mhaidli, Austin McCall, Florian Schaub

Jun. 27, 2019

The research presented was partially funded by the Mozilla Corporation.
Data Breach

Unauthorized access
Potential harms of data breaches

- Data leaked to the dark web
- Phishing attacks
- Identity theft
U.S. regulations for data breach notifications

Each state has their own law, with large inconsistencies in between.[1]

A few industry-specific laws (e.g., HIPPA).

Consumers’ inaction to data breaches

32% Ignored the notification(s) and did nothing.\[2\]

56% Used the same password for multiple online accounts.\[3\]

Data breaches pose significant security risks.

Data breach notifications DO NOT trigger consumer reactions effectively.
How to make data breach notifications useful?
Consumer Reactions to the **EQUIFAX** Data Breach
Research questions

1. How did consumers perceive the risks of the Equifax data breach?

2. What protective actions did consumers take in response, and what are the reasons behind (in)action?

Method


Use social media and email lists for recruitment.

Thematic coding for analysis (κ = 0.79).

"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach.
Little action despite high concern

20 out of 24 were aware of the breach.

Identity theft and privacy invasion were conceived as major risks.

14 participants DID NOT take any protective measures.
"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach.

Cognitive and behavioral biases behind inaction

Optimism bias

Tendency to delay

False sense of security

“Why would they go after me?”

“I haven’t done anything since the (credit) freeze.”

Extrinsic factors that motivate actions or inaction

Dear [Driver Name]:

Our security teams detected unusual activity on your account that looked like it might not be from you. We want to make you aware of this incident, what we have done in response, and steps that you can take to help protect your information.

What Happened
Specifically, we detected a login between approximately December 10, 2018 22:00 UTC and December 11, 2018 01:00 UTC that may not have been you. We further detected activity accessing the “Waybill” functionality on your account between the time of the unusual login and the point when your password was reset. For your account, we identified the following Waybill access(es):

Date and time (UTC): [Timestamp]  
IP Address: [IP Address]

What Information Was Involved
The Waybill functionality in your jurisdiction displays information about your current or most recent trip, as well as your name and driver’s license number.

What We Are Doing
We reset the password on your account to prevent additional unauthorized access. Furthermore, we have since removed the display of driver’s license from the Waybill in your jurisdiction.

What You Can Do
If you accessed a Waybill at the time(s) above, then no further action is necessary. If you believe someone else may have been responsible for this access, we recommend that you take the steps below. In addition, remember to practice good password hygiene, including using complex and unique passwords for each of your online accounts. If you used the same password on any other online accounts, you should change it on those accounts too. A password manager and this useful guide from the Electronic Frontier Foundation (https://sscl.eff.org/en/node/23/) can help you create and safely keep track of strong passwords for every account.

Activate Experian IdentityWorks
To help protect your identity, we are offering a complimentary one-year membership of Experian’s® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:
What are the potential issues with current data breach notification?

- Readability
- Risk communication techniques
- Structure and format
- How recommended actions are presented

You ‘Might’ Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Method

161 notifications during the first half of 2018, sampled from the website of Maryland Attorney General.

Quantitative metrics

<table>
<thead>
<tr>
<th>Readability Grade Levels</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Flesch–Kincaid Grade Level</td>
<td>9.8</td>
</tr>
<tr>
<td>Gunning Fog Index</td>
<td>13.2</td>
</tr>
</tbody>
</table>

Readability Scores

| Flesch Reading Ease | 47.5 |

Qualitative coding

<table>
<thead>
<tr>
<th>Code name</th>
<th>NVivo codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery method</td>
<td>Delivery method - mailed letter</td>
</tr>
<tr>
<td></td>
<td>Delivery method - email</td>
</tr>
<tr>
<td></td>
<td>Delivery method - website announcement</td>
</tr>
<tr>
<td></td>
<td>Delivery method - other</td>
</tr>
<tr>
<td>Use of structural headings</td>
<td>Use of structural headings - yes (in separate lines)</td>
</tr>
<tr>
<td></td>
<td>Use of structural headings - yes (in the same line as main text)</td>
</tr>
<tr>
<td></td>
<td>Use of structural headings - yes (as tables)</td>
</tr>
<tr>
<td></td>
<td>Use of structural headings - other</td>
</tr>
</tbody>
</table>

Data breach notifications are hard to read
Six minutes estimated reading time on average

Privacy policies, 10 mins

Data breach notifications, 6.3 mins

News articles, 2 mins

Emails, 20 secs

Techniques to downplay potential risks

70% used **hedge terms** when describing the likelihood of the recipient being affected.

employees and contractors. We are writing to inform you that we recently identified and addressed a security incident that may have involved your personal information. This notice explains the incident, measures we have taken, and some steps you can take in response.

40% used **“no evidence”** claim when describing the possibility of exposed data being misused.

of the school district’s internal computer systems or networks, or that any student information or any other employee information was affected. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.
8 as the median number of suggested actions.

73% mentioned credit freeze in the appendix.
Important actions buried in long paragraphs

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

Credit freeze
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.
Little guidance for comparison and prioritization

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.

You ‘Might’ Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
94% of notifications that used headings followed the exact wording suggestions in California’s breach notification law. [5]

Long list of state attorney general contact info

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

**Maryland Residents:** The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or http://www.oag.state.md.us.

**Massachusetts Residents:** Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**North Carolina Residents:** The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

**New Mexico Residents:** You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

**Rhode Island Residents:** The Attorney General can be contacted at (401) 274-4400 or http://www.riag.ri.gov/. You may also file a police report by contacting local or state law enforcement agencies.

Does a Maryland resident really need to see this?
Consumers **DO NOT** react to data breaches for various reasons, such as behavioral biases, source of advice, and jargon in notification.

In order to make data breach notifications **effective** at **motivating** consumers to take actions, we need to **fix these uncovered issues**.

Recommendations for data breach regulations

Incorporate **readability testing** based on standardized metrics.

What does “plain language” mean in California’s law? [5]

(1) The security breach notification shall be written in plain language, shall present the information described in paragraph (2) under the following Information Was Involved,” “What We Are Doing,” “What You Can Do,” information may be provided as a supplement to the notice.

Specific metric-based requirement for health insurance policies [6]

Effective August 31, 2010, the Rhode Island Office of the Health Insurance Commissioner (“OHIC”) will impose a readability requirement for all health insurance policies to be readable at the eighth grade level measured by the Flesch-Kincaide formula. The readability requirement comes in response to Rhode Island’s low adult literacy rate, and is designed to protect consumers by making health insurance policies, which are often complicated, easy to understand.


You ‘Might’ Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Recommendations for data breach regulations

Incorporate **readability testing** based on standardized metrics.

Provide concrete guidelines of how information should be presented.

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.
Recommendations for data breach regulations

1. Incorporate **readability testing** based on standardized metrics.
2. Provide concrete guidelines of **how** information should be presented.
3. Leverage the **influence** of **templates** to advocate positive changes.

The model privacy form for GLBA [7]


You ‘Might’ Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Consumers are **NOT reacting** to data breaches.

Data breach notifications are **NOT protecting** consumers.

Let’s have **stronger and more concrete** regulatory guidelines to affect changes.

Yixin Zou

yixinz@umich.edu

@yixinzou1124

The research presented was partially funded by the Mozilla Corporation.