You ‘Might’ Be Affected:

An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications

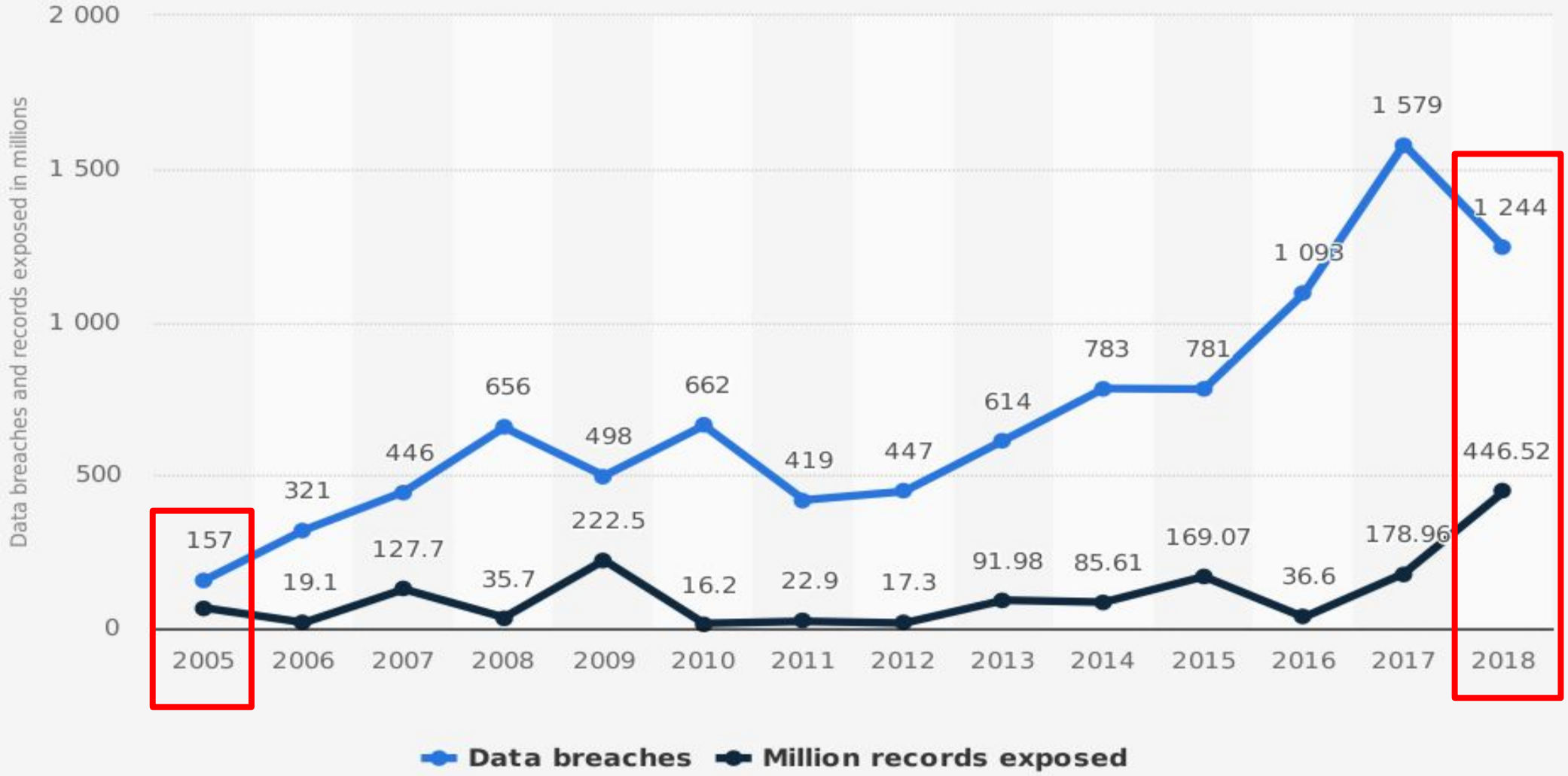
Yixin Zou, Shawn Danino, Kaiwen Sun, Florian Schaub

SCHOOL OF
INFORMATION
UNIVERSITY OF MICHIGAN

Who knows what a data breach is?

Do you know someone who has been affected by a data breach?

Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions)



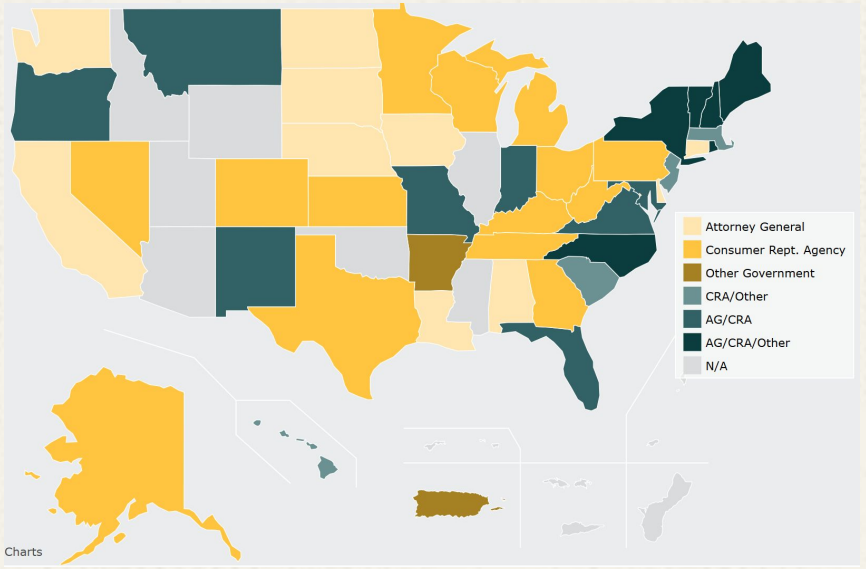
Source
Identity Theft Resource Center
© Statista 2019

Additional Information:
United States; Identity Theft Resource Center; 2005 to 2018

Background

Many laws require data breach notifications being sent to affected consumers.

EU: the General Data Protection Regulation, with unified requirements.



US: 50 state laws and a few sectoral laws (e.g., HIPAA), with large inconsistencies in between. [1]

[1] https://www.dwt.com/statedatabreachstatutes/

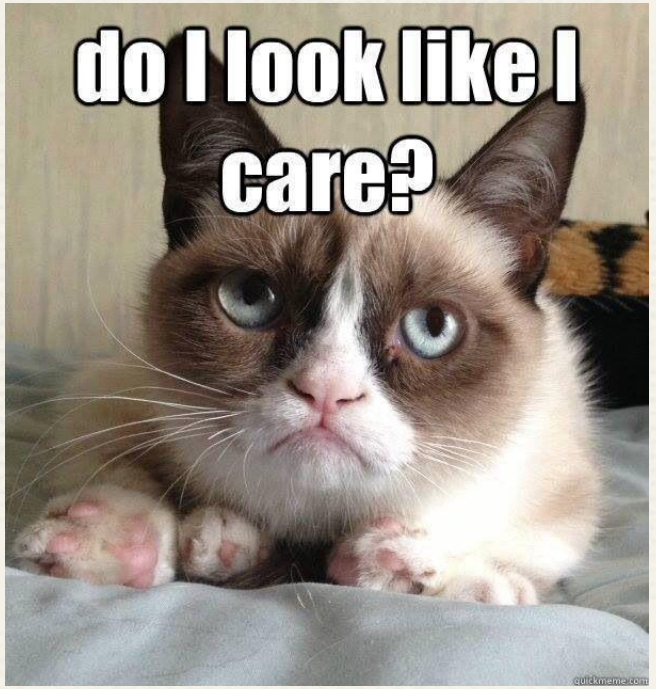
Background

However, consumers do not take sufficient protective actions when affected by a data breach...

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

41% Did not use two-factor authentication when provided.[3]

56% Continued using the same password for multiple accounts.[3]



[2] Ponemon Institute (2014). The Aftermath of A Data Breach: Consumer Sentiment.

[3] Gemalto (2017). Data Breaches and Customer Loyalty 2017.

Data breaches pose significant security risks.

Data breach notifications, while required by laws, do not trigger protective actions effectively.

What are potential issues with these notifications?

Motivation

Dear Sample A Sample:

Ventiv Technology, Inc. ("Ventiv") understands the importance of protecting personal information of its 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.

On December 5, 2017, our IT department received reports of suspicious activity regarding an employee email account hosted on Office365. We immediately changed the password for the account and began an investigation. Our investigation involved the assistance of a professional forensic firm to determine if any employee email accounts had been accessed without authorization. On January 4, 2018, the investigation determined that an unknown individual had accessed certain employees' email accounts hosted on Office365 without authorization between October 14, 2017 to December 8, 2017. The emails and attachments that were in the accounts include your name VARIABLE DATA.

Readability issues?

Usability issues?

Related Work

Rare use of visual elements (Jenkins et al., 2012)

“Lost data might not be used at all” appears in 2 out of 13 notification templates (Veltsos, 2014)

Large disparities among breach notifications in terms of timing and content (Bisogni, 2016)

Issues with content and visuals can impact users’ comprehension and reactions in other security and privacy domains (Bravo-Lillo et al., 2011; Gluck et al., 2016)

Maryland Information Security Breach Notices

As of January 2008, any business that retains consumer records is required by Maryland law to notify a consumer who is a resident of Maryland if his or her information is compromised. The "security breach law" also requires the business to notify the Office of the Attorney General. This webpage contains links to all notices sent to the OAG since the law took effect. Below is a chart containing the case number, date of the notice, business name, how many people are affected what information was compromised and how it was lost.

Find a file

Case Title	Case No.	Date Received	No of MD Residents	Information Breached	How Breach Occurred

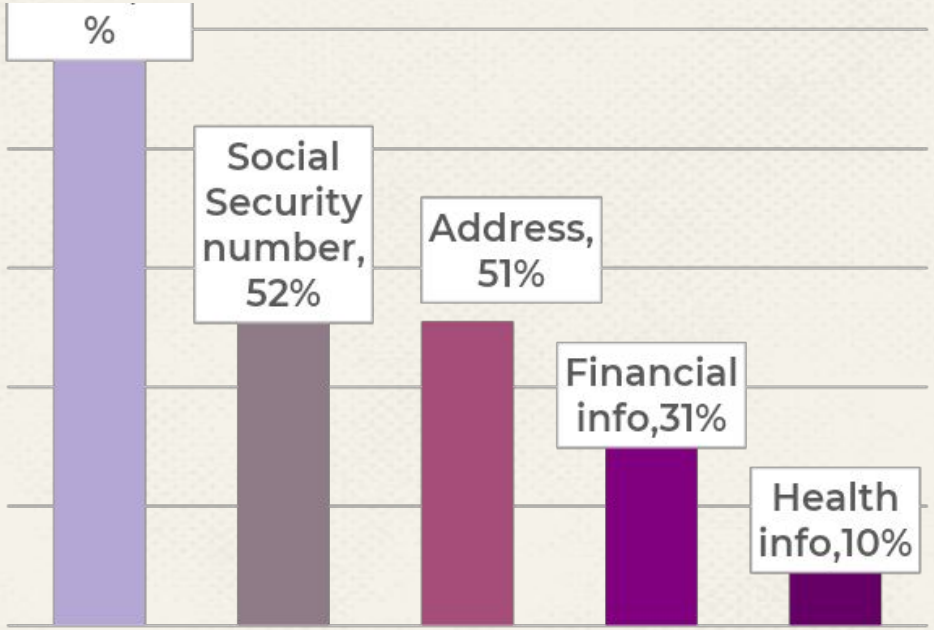
- **Year : 2019** (94)
- **Year : 2018** (1067)
- **Year : 2017** (1084)
- **Year : 2016** (792)
- **Year : 2015** (482)

Largest number of notifications compared to other states (California, Iowa, New Hampshire, and Vermont).

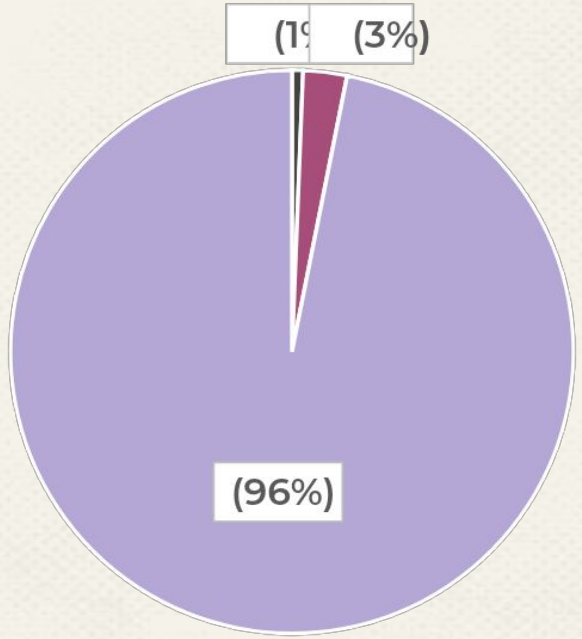
Method

161 notifications randomly sampled from January to June 2018.

Types of Exposed Data



Delivery Method



Method

Quantitative Analysis

Readability Grade Levels	
Flesch–Kincaid Grade Level	9.8
Gunning Fog Index	13.2
Readability Scores	
Flesch Reading Ease	47.5
Text Statistics	
Paragraph Count	14
Sentence Count	28
Word Count	354

Qualitative Analysis

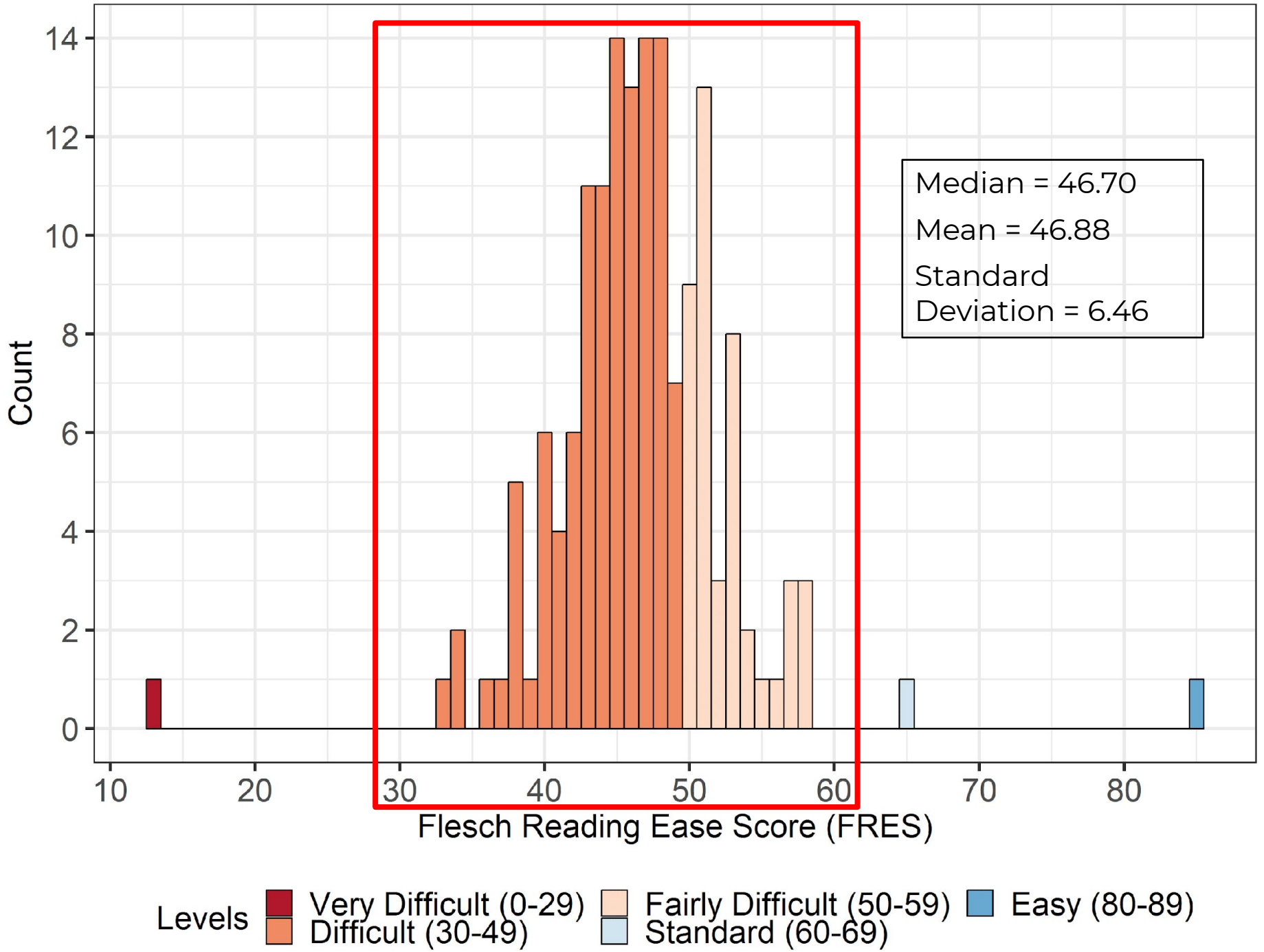
Code category	Code name	NVivo codes
Delivery	Delivery method	Delivery method - mailed letter
		Delivery method - email
		Delivery method - website announcement
		Delivery method - other
Structure	Use of structural headings	Use of structural headings - yes (in separate lines)
		Use of structural headings - yes (in the same line as main text)
		Use of structural headings - yes (as tables)
		Use of structural headings - other
Cross-case comparison	Multiple templates provided	Multiple templates provided - yes
		Multiple templates provided - other

Codebook developed using **thematic coding** and **affinity diagramming** (κ = 0.75).

Themes: structure and formatting; risk communication; presentation of recommended actions.

1. Data breach notifications are hard to read.

Key findings


Median = 46.70
Mean = 46.88
Standard Deviation = 6.46
Count
Flesch Reading Ease Score (FRES)
Levels
Very Difficult (0-29)
Difficult (30-49)
Fairly Difficult (50-59)
Standard (60-69)
Easy (80-89)

Findings

Estimating reading time based on word counts (McDonald and Cranor, 2008):

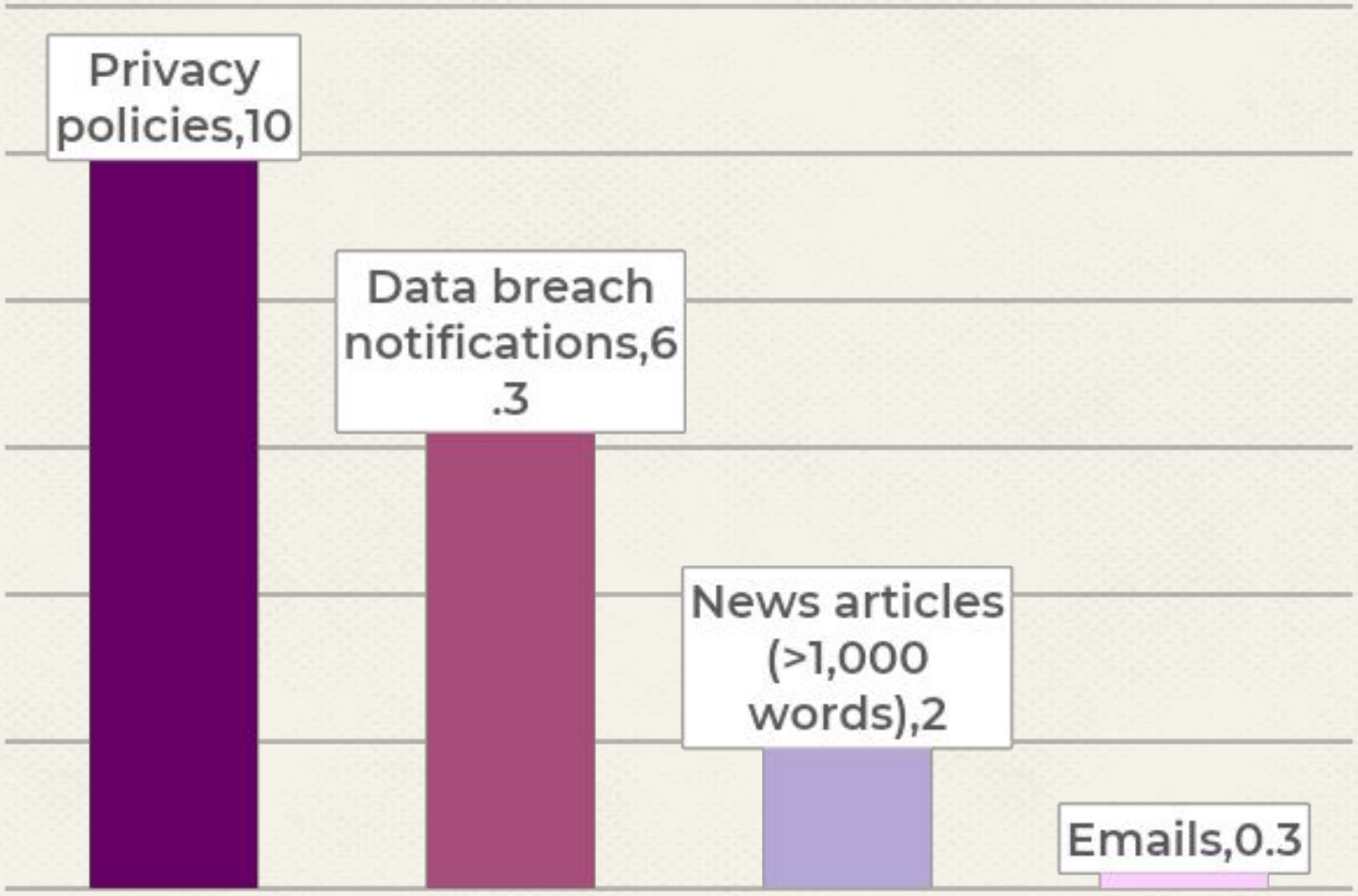
	Range:	Median:	
Word Count	**213-3,414**	**1,575**	**(words)**

250 words / minute

	Range:	Median:	
Reading Time	**0.85-13.66**	**6.3**	**(minutes)**

Findings

Reading Time Comparison In Minutes



[5] McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *ISJLP*, *4*, 543.
[6] Mitchell, A., Stocking, G., & Matsa, K. E. (2016). Long-form reading shows signs of life in our mobile news world. *Pew Research Center*, *5*.
[7] https://www.marketingsherpa.com/article/average-email-open-time-is

2. Ambiguity and Obfuscation in risk communication.

Key findings

37% did not report when the breach occurred;
35% did not report when the breach was discovered.

“

We are writing to inform you that due to a security incident at a Citizens Bank ATM, your ATM/Debit card may have been compromised.

70% used hedge terms such as “maybe” and “likely” when describing the likelihood of being affected.

The information **potentially** involved in this incident **may** have included your name, credit or debit card number, and card expiration date.

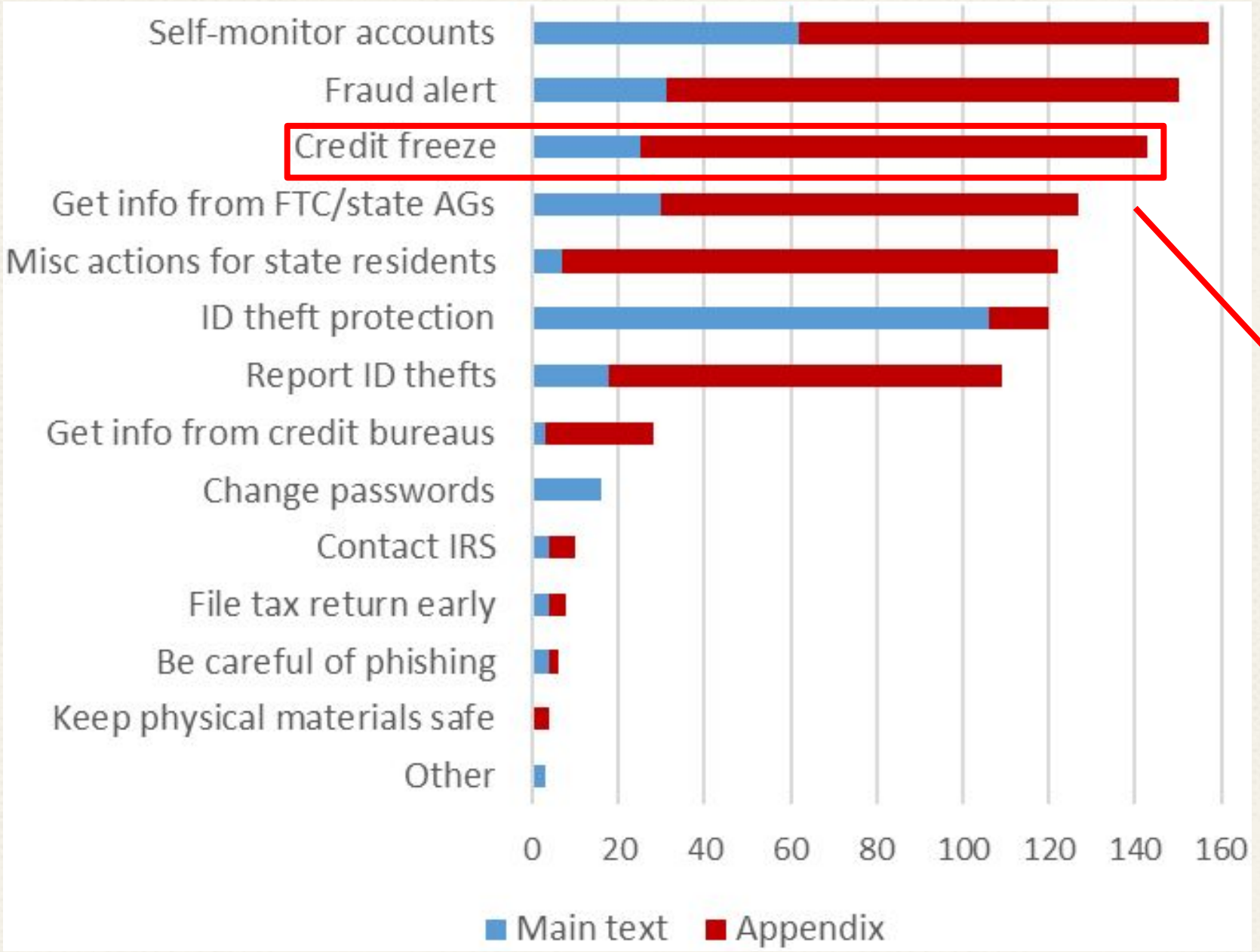
40% claimed that there was no evidence of exposed data being misused.

“

We **are not aware of** any fraud or misuse of your information as a result of this incident.

3. Multiple actions with no priorities and little actionability.

Key findings



All notifications provided at least one suggested action, with a median of 8 (Mean = 7.19, SD = 2.24).

Credit freeze: 118 (73%) notifications described it as one of the many options in the appendix.

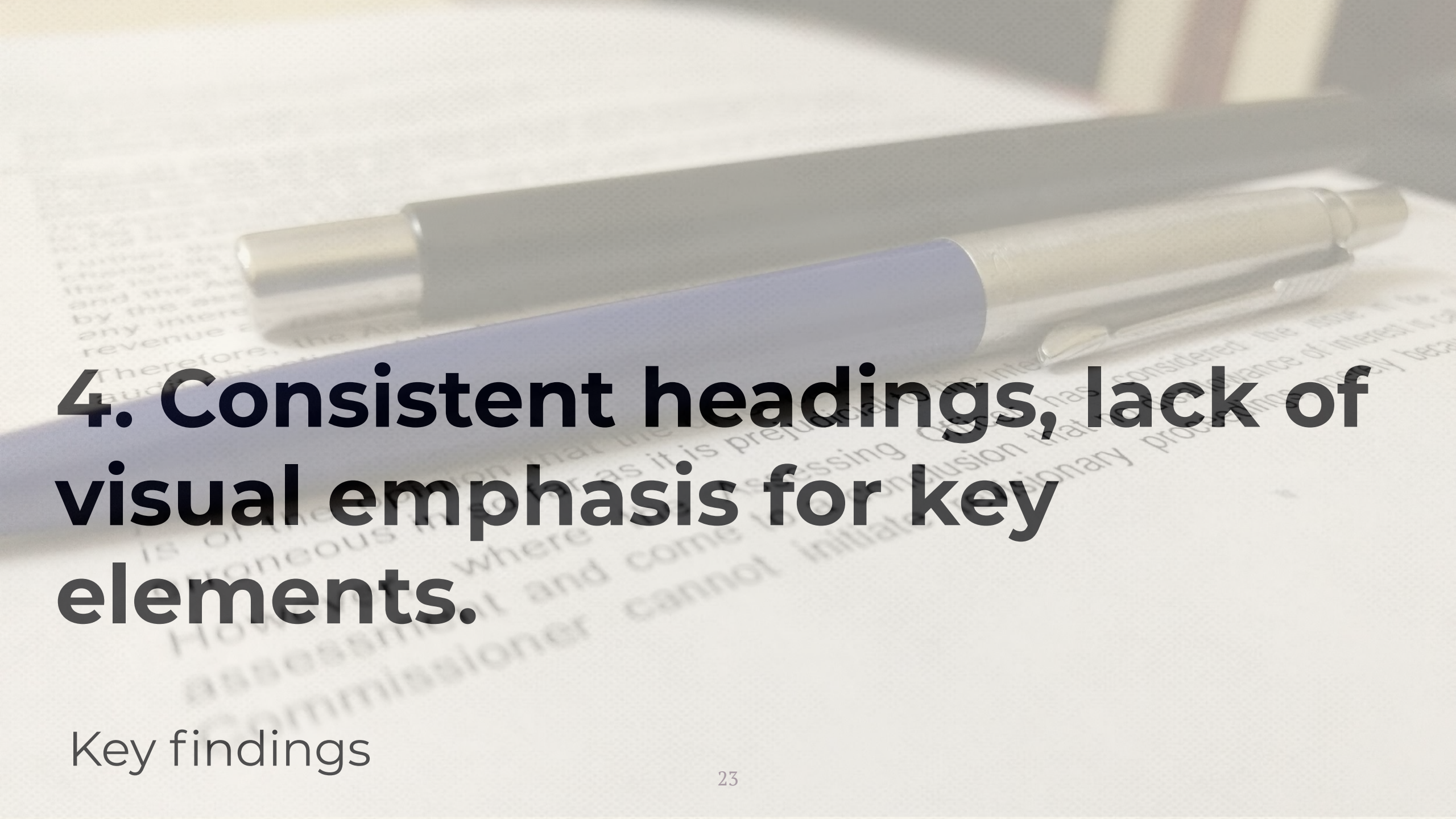
What is each paragraph about?

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	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	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.

Between fraud alert vs. credit freeze, which one is more effective?



4. Consistent headings, lack of visual emphasis for key elements.

Key findings

Findings

(a) Plain text without heading **(N=55, 34%)**

We are writing to inform you that we recently discovered that on or around March 31, 2018 an employee file was infected with ransomware. As a result, your personal information, including your name, address, and Social Security Number may have been accessed. At this time, there is no evidence that this information has been removed from our premises. Further, rather than paying the ransom to the attackers, we recovered files from our backup copies.

(b) Heading in separate line **(N=72, 45%)**

What Happened?
On or about March 14, 2018, Mumm Napa and Kenwood Vineyards became the victim of a malicious cyberattack, which compromised a single employee's account credentials. The account included a number of emails that contained personal information. We currently have no reason to believe that any Mumm Napa systems were compromised beyond limited information contained in the employee's email account. Upon discovery of the compromise, we promptly acted to secure the compromised account and investigate the incident.

(c) Heading in paragraph's first line **(N=34, 21%)**

What Happened? On or about August 3, 2017, certain Broward College employees received a spam phishing email to their Broward College email accounts. The phishing email contained a link that asked the employee to enter their Broward College log-in credentials. On Friday, August 18, 2017, Broward College learned that certain employees had clicked on the link in the email and provided their credentials. Broward College identified and corrected the issue by contacting all potentially affected employees and ensuring that all passwords were changed. Broward College also immediately initiated an investigation, with the assistance of a third-party forensic investigator, to determine what personal information, if any, was subject to unauthorized access or acquisition.

(d) Heading in table **(N=2, 1%)**

What Happened?	A former employee may have accessed consumer data during her employment other than for the purposes of carrying out her assigned duties, during the time period between September, 2017 and February 2018.

(D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO] _____ _____ Date: [insert date]

NOTICE OF DATA BREACH

What Happened?

What Information Was Involved?

94% of notifications with headings used the exact wording and order as the template in California's data breach notification law. [9]

[8] https://www.oag.ca.gov/privacy/databreach/reporting

Text formatting was rarely used to highlight important details of complimentary protection services.

Among 124 notifications that provided such services:

WHAT YOU CAN DO. We recommend that you review the information provided in this letter for some steps that you may take to protect yourself against any potential misuse of your personal information. As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

87% did not use visual highlights for the **duration of benefits.**

We take our responsibility of protecting your personal data seriously. Therefore, we have retained LifeLock to provide you one (1) year of complimentary identify theft protection and credit monitoring services. To "activate" your membership, call 1-800-899-0180 or go online at https://store.lifelock.com/enrollment?promocode=UWSAA2018. You will need to provide a Membership ID. Your Membership ID is your first name last name plus 5-digit zip code. The enrollment period will expire on March 30, 2018.

63% did not use visual highlights for the **enrollment deadline.**

Design Implications

1. Use clear and concise language.

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?

Design Implications

1. Use clear and concise language.

2. Support consumers in prioritizing and executing multiple actions.

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	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	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.

- Credit freeze should be placed on top of fraud alert.
- Explain "why important" first, rather than dumping all definitions and enrollment instructions together.

Design Implications

1. Use clear and concise language.

2. Support consumers in prioritizing and executing multiple actions.

3. Discourage hedge terms and “no evidence” claims.

The information stored in the affected email account includes certain individuals' names, Social Security numbers, birthdates, and/or financial information. Based on our investigation, it appears your information was included in the affected email account and, therefore, could be affected by this incident. Our investigation has not found any evidence that this incident involves any unauthorized access to or use of any 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.

Avoid making the "no evidence" statement, or at least combine it with clear warnings of potential misuse in the future.

Overstating risks is more desired than understating risks:

- Trigger more immediate actions.
- Address cognitive heuristics, such as optimism bias.

Policy Implications

1. Clear readability expectations beyond “plain language.”

The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

What does “clear and plain language” mean?

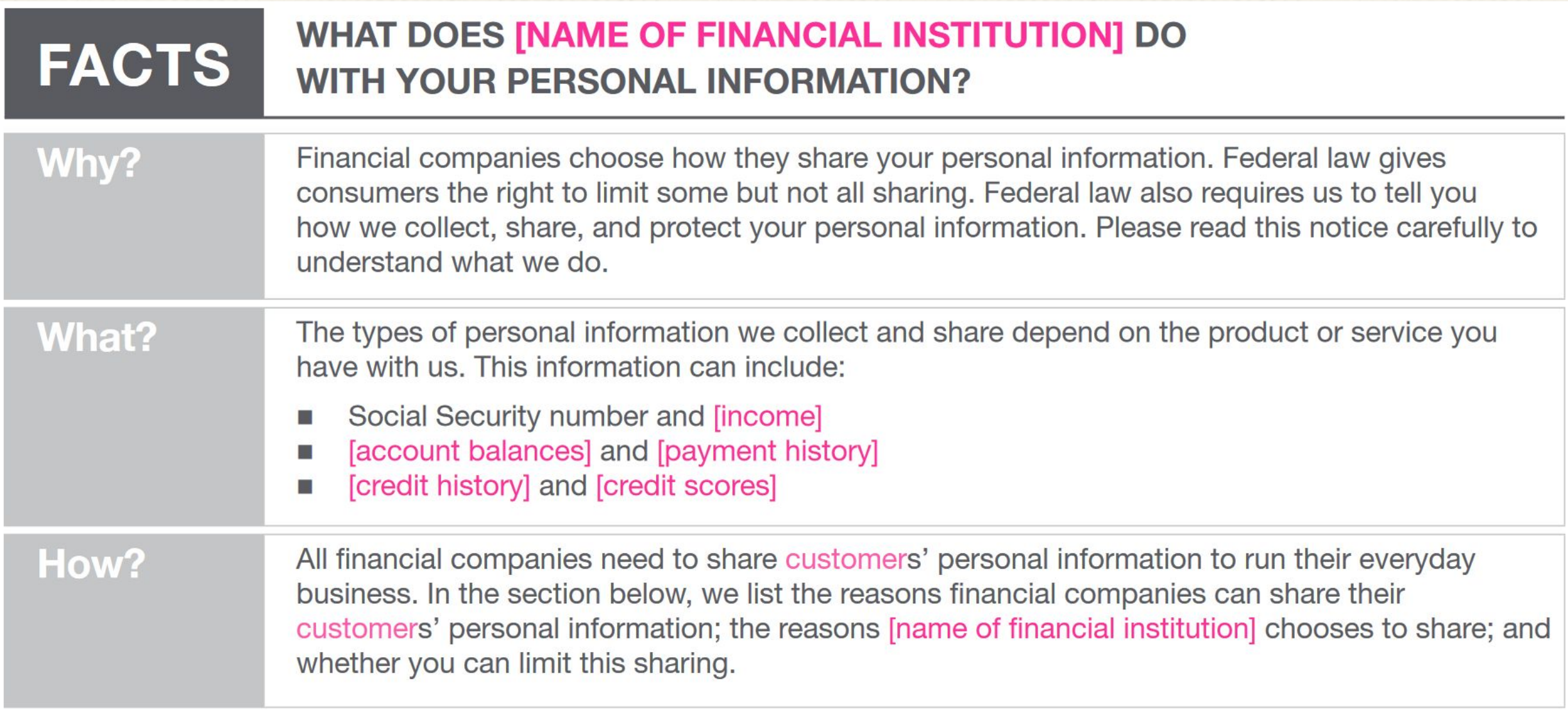
- Clarify expectations of “plain language” and provide specific **guidance** and **examples** of how it can be achieved.

- Incorporate readability assessment requirement based on **standardized metrics**, similar to what’s been done in the insurance industry.

Policy Implications

1. Clear readability expectations beyond “plain language.”

2. Consistent standards for content and format.



FACTS	WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

The GLBA model privacy form. [10]

[9] 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

Policy Implications

1. Clear readability expectations beyond “plain language.”

2. Consistent standards for content and format.

3. Encourage using multiple channels to deliver data breach notifications.

Primary: mailed letters

Secondary: emails, website notice, media etc.

47740
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

March 22, 2018

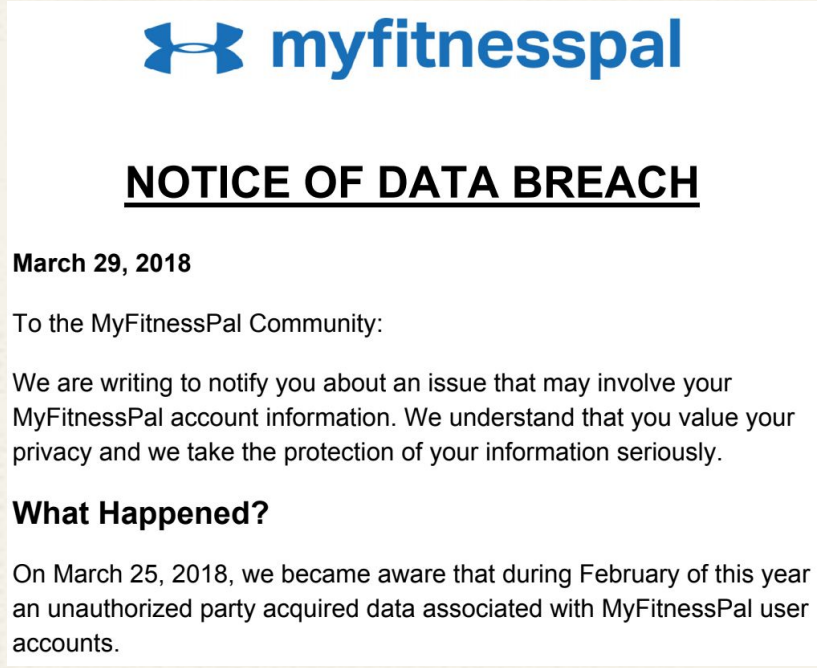
NOTICE OF DATA BREACH

We are writing to share important information about a data security incident that may have affected some of your personal information.

First and foremost, we want to reinforce that keeping the personal data of our customers safe and secure is very important to us, and we deeply regret this occurred. We can assure you that as soon as we determined there was likely unauthorized access to some personal information, we took swift action to address the issue and protect our customers. You should know that the current Orbitz.com website was not in any way involved in this incident.

What Happened?

While conducting an investigation of a legacy Orbitz travel booking platform (the "platform"), we determined on March 1, 2018 that there was evidence suggesting that, between October 1, 2017 and December 22, 2017, an attacker may have accessed personal information, stored on this consumer and business partner platform, that was submitted for certain purchases made between January 1, 2016 and June 22, 2016. We took immediate steps to investigate the incident and enhance security and monitoring of the affected platform, and made every effort to remediate the issue, including taking swift action to eliminate and prevent unauthorized access to the platform.



myfitnesspal

NOTICE OF DATA BREACH

March 29, 2018

To the MyFitnessPal Community:

We are writing to notify you about an issue that may involve your MyFitnessPal account information. We understand that you value your privacy and we take the protection of your information seriously.

What Happened?

On March 25, 2018, we became aware that during February of this year an unauthorized party acquired data associated with MyFitnessPal user accounts.

- Letters increase consumers' "uninformed exposure time" to potential risks.
- Electronic methods create extra momentum for readability and aesthetics.

Summary

Motivation: data breach notifications are mandatory but not effective.

Method: a content analysis of 161 breach notifications from Maryland AG.

Findings: low readability;
ambiguous and obfuscated risk communication;
multiple actions with provided with no priorities and little actionability;
consistent headings but lack of visual emphasis on key elements.

Implications: use clear and concise language;
discourage hedge terms and “no evidence” defense;
support execution of recommended actions;
unify structure and format requirements;
encourage delivery through multiple mediums.

SCHOOL OF INFORMATION
UNIVERSITY OF MICHIGAN

Yixin Zou

yixinz@umich.edu

@yixinzou1124