

Breach Analysis

Adrianna Holden-Gouveia

Website: aholdengouveia.name

: [aholdengouveia](https://github.com/aholdengouveia)

: [aholdengouveia](https://twitter.com/aholdengouveia)

Accessibility Notice

This document is also available in HTML format at:

Link: <https://aholdengouveia.name/InfoSec/labs/breachanalysis.html>

The HTML version provides enhanced accessibility features including keyboard navigation, screen reader support, responsive design, dark mode support, and high contrast options.

Learning Outcomes

By the end of this lab, you will be able to:

- Find a recent data breach, and the notice the company sent to the people affected
- Compare a company's breach response with the FTC's best practices and Massachusetts law
- Explain how combining stolen data with other data can cause more harm, and whether a breach was an insider or outsider threat
- Check whether your own data has been in a breach, and take steps to protect yourself

Lab Instructions

When a company has a data breach, it's supposed to tell the people affected. In this lab, you'll find a real breach notice, check it against best practices, follow how the company handled it, and then check your own data.

Screenshots

This lab asks for at least 8 screenshots. Each screenshot should have your name, term, and year. One of the easiest ways to do that is make a text document with your name and term/year on your computer and save it to use all term. Any screenshots that don't include this information won't be counted.

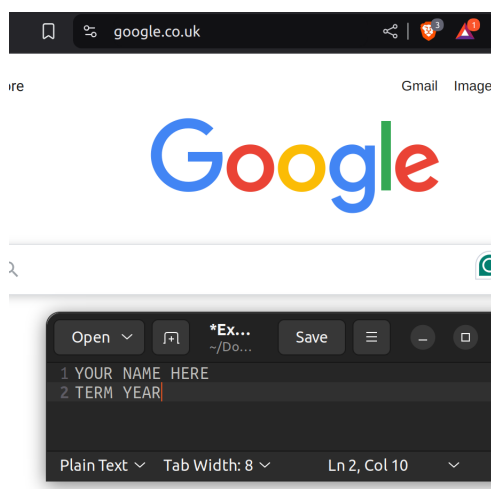


Figure 1: This is an image of what each of your screenshots should look like

You can blur or cover anything private in a screenshot, such as your email address, as long as your name and term note still shows.

Part 1: Find a Breach and Its Notice

Pick a data breach from the last 2 years. It can be from anywhere, but you need to be able to find the notice the company sent to the people affected. Good places to look:

- Massachusetts posts the breach notice letters companies send to residents, sorted by month (linked under Resources)

- The company’s own website, often on a page called “notice of data security incident”
- News articles, which often link to the notice

Breaches from class, such as PowerSchool (2024) and Canvas (2026), are fine to use.

1. Give the company’s name, when the breach happened, and a link to the notice.
2. Take a screenshot of the notice, showing the company’s name and the date.

Part 2: Build a Timeline

Find at least 4 dated events, each from a different kind of source:

- The notice itself
- A news article
- A statement from the company, such as a press release, a blog post, or a post on its social media
- One more, such as a social media post from someone affected, a state filing, or a second news article

For each event, include the date, what happened, a citation, and a screenshot of the source showing its title and date.

3. Put the events in order. When did the breach start? When did the company find it? When did people find out?
4. How long did people wait between the company finding the breach and being told? Was that reasonable? Why or why not?
5. Did the company’s story match what the news reported? Point out anything that was different.

For the news articles, also include a CRAAP check. My guide to evaluating sources, linked under Resources, shows how.

Part 3: Score the Notice

The FTC’s Data Breach Response guide lists what a good notice should include. Massachusetts law, Chapter 93H, adds its own rules. Both are linked under Resources.

6. Make a table with three columns: the item, your score (Met, Partly met, or Not met), and your evidence. For evidence, quote the exact words from the notice, or write “not in the notice”. Score these items:

- (a) Says what information was taken
- (b) Says what the company has done to fix the problem
- (c) Tells you what you can do to protect yourself
- (d) Offers help, such as free credit monitoring or identity protection
- (e) Gives a way to contact the company, such as a phone number or website
- (f) Was sent quickly. Use your timeline.
- (g) Is written so someone without a tech background could understand it
- (h) Says how the breach happened. **Massachusetts letters aren't allowed to include this**, so if yours is a Massachusetts letter, write "not allowed in Massachusetts", and find out how it happened from the news instead.
- (i) Tells you that you have the right to get a police report (Massachusetts law)
- (j) Explains how to freeze your credit, and that a credit freeze is free (Massachusetts law)

If your breach isn't from Massachusetts, still score the last two. Would the notice have met Massachusetts law?

7. Overall, how well did the company do? Give 2 things it should have done better, and support each one with the FTC guide or an expert source.

Part 4: Connect the Dots

8. List every type of data the notice says was taken, such as names, email addresses, Social Security numbers, or medical information.
9. Pick one other place an attacker could get information about the same people, such as another breach, social media, or a people-search website. What could an attacker learn by combining the two? Give one specific way they could use it to cause harm.
10. Was this breach an insider threat, from someone inside the company, or an outsider threat, from someone outside? Remember, insider threats include mistakes, not just people doing harm on purpose. If it's not known, say what you think and why.
11. Would you still trust this company with your data? Why or why not?

Part 5: Check Your Own Data

Have I Been Pwned is a free website that checks whether an email address has been in a known data breach. Use an email address you use, or a family member's with their permission. You can blur the address in your screenshot.

12. Search the address, and take a screenshot of the results.
13. If it was in a breach, pick one. What data was taken? If it wasn't in any breaches, pick a breach from the site's list of recent breaches, and answer for that one.
14. Take 2 steps to protect yourself, and take a screenshot of each. For example: change the password for that account, turn on two-factor authentication, or find the page that explains how to freeze your credit at Equifax, Experian, or TransUnion. You don't have to actually freeze your credit.
15. Which of your 2 steps would help most if your data from Part 4 was combined with other data? Why?

Deliverables

One file that includes:

- Part 1: your breach, the link, and your screenshot of the notice
- Part 2: your timeline of at least 4 events, each with a citation and screenshot, CRAAP checks for the news articles, and your answers
- Part 3: your scoring table, and your answer
- Part 4: your answers
- Part 5: your 3 screenshots, and your answers

Resources

References, a video, a PowerPoint and some notes are available at my website Link: <https://www.aholdengouveia.name/InfoSec/PolicyCompliance.html>

FTC: Data Breach Response, A Guide for Business, for Part 3 Link: <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business>

Massachusetts General Laws Chapter 93H, Section 3: what a breach notice to residents must and must not include, for Part 3 Link: <https://malegi>

slature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H/Section3

Massachusetts data breach notification reports and letters, for Part 1
Link: <https://www.mass.gov/lists/data-breach-notification-reports>

Have I Been Pwned, for Part 5 Link: <https://haveibeenpwned.com/>

FTC: Credit Freezes and Fraud Alerts, for Part 5 Link: <https://consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts>

My guide to evaluating sources Link: <https://www.aholdengouveia.name/Howtos/Sourceeval/sourceEvaluation.html>

The CRAAP test, with questions to ask about each source Link: <https://web.archive.org/web/20250814000638/https://guides.lib.uchicago.edu/c.php?g=1241077&p=9082343>