Name: Amber Radune

Class: CYBR-1100

Date: August 22, 2025

Project 1-3: Comparing Data Breach Notification Letters

Below are the steps I took to gather the information for the data breach tables.

1. Access the Database

- I went to the California Attorney General's Data Breach website (https://oag.ca.gov/privacy/databreach/list).

2. Select Three Breach Notices

- Farmers New World Life Insurance Company
- The Computer Merchant, Ltd.
- Mutual of America Life Insurance Company

3. Download and Review the Letters

- For each listing, I clicked **Submitted Brief Notification Sample → Sample of Notice (PDF)**.
- I read through the letters and highlighted key sections:
    - *What Happened*
    - *What Information Was Involved*
    - *What We Are Doing*
    - *What You Can Do*
    - Free protection offer (provider + months)
    - Enrollment method and deadline

    - Contact info
    - Extra resources (FTC, state Attorney General info)

4. Extract Key Facts from Each

- **Farmers Insurance (Aug 22, 2025):** Vendor database accessed, 24 months of CyberScout monitoring, enrollment deadline Nov 25, 2025.
- **The Computer Merchant (Aug 19, 2025):** Cyberattack, full system restore, IDX protection (12–24 months + $1M insurance), deadline Nov 19, 2025.
- **Mutual of America (Aug 20, 2025):** Mis-sent secure email, Experian IdentityWorks 12 months, deadline Nov 28, 2025.

5. Build Comparison Tables

- **Table 1 (Similarities):** Elements all three letters had in common (company header, what happened, what info, monitoring services, deadlines, contact info, extra guidance).
- **Table 2 (Differences):** Unique details (breach type, protection provider, length of coverage, tone, extra services like $1M insurance or dark web monitoring).

6. Summarize Findings

- Similarities: All three offered free credit/identity monitoring, included deadlines and codes, and gave customers clear "What You Can Do" steps.
- Differences: Each had a different breach type, monitoring service provider, and length of coverage. Tone varied—Farmers was very formal, The Computer Merchant was more customer-focused, and Mutual of America emphasized prevention/education.

7. Create Deliverables

- I placed both tables into a Word document (**Data_Breach_Comparison.docx**) and also drafted an **improved notification letter** that combines the best elements: clear plain language, a precise description of data compromised, strong identity protection support, enrollment instructions, and practical next steps for victims.

Project 1-3: Comparing Data Breach Notification Letters

Below are the comparison tables based on three sample data breach notification letters (Farmers Insurance, The Computer Merchant, and Mutual of America).

Table 1 – Similarities (Common Elements)

Element	Farmers Insurance	The Computer Merchant	Mutual of America
Company name/logo & letterhead	✅	✅	✅
Date of letter	✅ (Aug 22, 2025)	✅ (Aug 19, 2025)	✅ (Aug 20, 2025)
“What Happened” section	✅ (vendor DB hack)	✅ (cyberattack, delayed discovery)	✅ (mis-sent email)
“What Information Was Involved”	✅ (personal info)	✅ (name + SSN)	✅ (name, SSN, ID#, account balance)
“What We Are Doing”	✅ (investigation, 24m monitoring)	✅ (investigation, IDX, $1M insurance)	✅ (investigation, 12m Experian, education)
“What You Can Do”	✅ (monitor, freeze, alerts)	✅ (monitor, alerts, enroll IDX)	✅ (monitor, alerts, enroll Experian)
Free credit monitoring	✅ (24m)	✅ (12/24m)	✅ (12m)
Enrollment deadline	✅ (Nov 25, 2025)	✅ (Nov 19, 2025)	✅ (Nov 28, 2025)
Contact info provided	✅ (phone, web)	✅ (phone, QR, web)	✅ (phone, Experian site, code)
Extra resources (FTC/State AG)	✅	✅	✅

Table 2 – Differences (Unique Features)

Element	Farmers Insurance	The Computer Merchant	Mutual of America
Breach type	Vendor DB hacked	Cyberattack w/ delayed discovery	Misdirected email
Technical detail	Medium	High (wipe/restore, delayed)	Low (focus on email)
Identity protection	CyberScout (24m)	IDX (12/24m, $1M insurance, recovery)	Experian IdentityWorks (12m)
Enrollment method	Website + code	Website, QR, phone	Website + code, Experian support
Extra services	Fraud alerts, credit freeze, state info	$1M insurance reimbursement	Identity restoration, $1M theft insurance, dark web monitoring
Tone	Formal/legal-heavy	Customer-centered, insurance-heavy	Reassuring, prevention-focused

Improved Notification Letter

Subject: Notice of Data Breach

Dear Valued Customer,

We are writing to inform you about a data security incident that may have involved your personal information. Protecting your privacy is essential to us, and we want to explain what happened, what information may have been affected, and the steps we are taking to support you.

What Happened
On August 22, 2025, we discovered that a cyberattack exposed certain customer information. As soon as we became aware, we secured our systems, launched a full investigation with cybersecurity experts, and notified law enforcement.

What Information Was Involved
The review confirmed the potential exposure of your personal information, which could include your name, Social Security number, date of birth, and account details. Not all customers were affected, but we are notifying everyone out of caution.

What We Are Doing
We have taken steps to enhance our security, reinforce employee training, and prevent a recurrence of this incident. To protect you, we are offering **24 months of complimentary identity protection services**, which include:

- Credit monitoring at all three major bureaus (Equifax, Experian, and TransUnion)
- Fraud detection and alerts
- Up to $1,000,000 of identity theft insurance coverage
- Identity restoration services if your information is misused

You must complete your enrollment by **November 20, 2025**. To activate your protection, visit www.signupnow.com and use activation code 8675309.

What You Can Do
We recommend that you:

- Monitor your credit reports at AnnualCreditReport.com.
- Watch your bank, credit card, and insurance statements for suspicious activity.
- Consider placing a fraud alert or credit freeze with the credit bureaus.
- Please promptly report any suspicious activity to us and your financial institution.

For Assistance
If you have questions, please call us toll-free at 1-800-555-5555, Monday through Friday from 8 a.m. to 5 p.m., or visit our support website. Our dedicated response team is ready to help you.

We sincerely apologize for this incident and any concern it may cause. Thank you for trusting us as we work to enhance the security of your information.

Sincerely,
Amber Radune
Chief Privacy Officer

Reflection

Which elements would be most useful if you were a victim?

The most useful elements in these letters are the clear explanations of what happened, the list of what personal information was exposed, and the specific steps the customer can take to protect themselves. I also find it helpful that they offer free credit monitoring and identity theft protection, which is especially valuable since they provide reassurance and practical tools to detect fraud. Finally, having a deadline and enrollment code included makes it easy to act quickly without confusion.

What additional information would help?

As a victim, I would want more precise details, such as the exact date the breach occurred, how long my information may have been exposed, and whether law enforcement is directly involved in the investigation. Knowing how the breach was detected and what specific security measures were taken afterward would also help me feel more confident. More transparency about the risk level of my data being misused would make the notice more helpful and less stressful.