Adobe Data Breach 2013:

- The 2013 Adobe breach included: credit card records, login data, hashed passwords, IDs and debit and credit information.This is what Adobe was held accountable for as it impacted customers and internal/external users. The attackers were also able to siphon valuable proprietary data as well, including source code for Adobe Acrobat and Reader as well as ColdFusion; Adobe's web app platform. Some of the Photoshop source code was also made apparent (Krebs, 2013).
- I believe Adobe is ignorant to how the information was stolen; that or they're reluctant to divulge how the attackers had gained access
- The hackers responsible were never identified
- Adobe's strategy seemed highly reactionary and guarded. Full extent of damages either weren't initially realized until additional investigation or was suppressed to preserve public image. Limited public information is available regarding Adobe's internal response, but their public response was met with heavy criticism. Ultimately Adobe was required to pay roughly one million dollars in legal fees to settle claims of breach of the Customer Records Act and unfair business practices (Swinhoe, 2021). Rubbing salt in the wound, Adobe also agreed to provide free credit scanning and alerts on those who's credit or debit information may have been compromised; though nowhere in the agreement did it say regular scans and alerts would be required on an ongoing basis effectively saying their partnered credit firms "can" as opposed to "will." The coverage above also doesn't mention any impact or recourse surrounding potential identity theft (Krebs, 2013).
- There is no mention of whether the ICO was notified in this incident
- Affected individuals were eventually notified as part of a campaign to urge compromised users with active accounts to change their passwords.
- Ultimately, Adobe was barely made to pay. The one million dollars in legal fees is a rounding error for a company as large as Adobe. Their reputation may have suffered a blow, but it's highly unlikely it made any major impact as they're still the industry standard in media editing and document processing with no major threat to their current market share.

Reflection:

Ultimately, this is a great example of how not to handle a breach. Adobe was guarded and lacked transparency surrounding their breach. Meanwhile they're having source code and user files shared with AnonNews.org. Their public response towards users potentially impacted came off as disingenuous and cheap, considering they were at fault. The backhanded "account monitoring" that offered no guarantee user credit accounts would actually be monitored is insulting to the consumer at best and

potentially damaging or leading to future identity fraud at worst. The only positive step Adobe took was to reach out to impacted users to enforce a password change on the account. In cases where potentially millions of users' financial information is compromised, delicacy, humility and sympathy are as important as the actions taken to reassure uncertain clients. Adobe's actions appeared cold, unsympathetic and shrewd in how they made assurances while contractually writing themselves out of any responsibility.
As ISM I would have favored a more transparent approach in response, notifying users and enforcing password changes. I can't speak to Adobe's internal structure, but considering no attacker is identified or made known, I would assume their audit structure and logging needs to be bolstered to avoid non-repudiation.

References:

Krebs, B. (2013). Adobe Breach Impacted At Least 38 Million Users — Krebs on Security. KrebsonSecurity. Available at: https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/ [Accessed 5 Jul. 2021].

Swinhoe, D. (2021). *The 15 biggest data breaches of the 21st century*. CSO Online. Available at: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html [Accessed 5 Jul. 2021].