Data Breach Case Study

The case of **Adult Friend Finder**

Date of Event : October 2016

Impact: 412.2 million accounts

Summary of Breach

The adult-oriented social networking service The FriendFinder Network had 20 years' worth of user data across six databases stolen by cyber-thieves in October 2016. Given the sensitive nature of the services offered by the company – which include casual hookup and adult content websites like Adult Friend Finder, Penthouse.com, and Stripshow.com – the breach of data from more than 414 million accounts including names, email addresses, and passwords had the potential to be particularly damming for victims. What's more, the vast majority of the exposed passwords were hashed via the notoriously weak algorithm SHA-1, with an estimated 99% of them cracked by the time LeakedSource.com published its analysis of the data set on November 14, 2016.

The Breach Checklist

01 What types of data were affected?

02 What happened?

03 Who was responsible?

04 Were any escalation(s) stopped - how?

05 Was the Business Continuity Plan instigated?

06 Was the ICO notified?

07 Were affected individuals notified?

08 What were the social, legal and ethical implications of the decisions made?

What types of data were affected?

Personal data; names, email, addresses, and passwords

What happened?

- **20 years' worth of user data across six databases stolen by cyber-thieves in October 2016.**
- **339 million accounts from AdultFriendFinder.com, including 15 million supposedly deleted accounts. Another 62 million belong to Cams.com, and 7 million come from Penthouse.com, as well as a few million from smaller properties owned by the company.**
- **hackers took advantage of a file inclusion vulnerability disclosed in October by a researcher. The vulnerability permitted the disclosure of private information such as server passwords(GHEORGHE, 2016).**
- **Security researchers have said that the flaw the hacker used to get at the database was a very common one known as Local File Inclusion (LFI)(Vaas, 2016)**
- **The attacker got access to SQL databases containing stored usernames, email addresses, and passwords saved in plaintext or secured with SHA-1(GHEORGHE, 2016).**

Who was responsible?

- Twitter user 1×0123 posted images of a Local File Inclusion vulnerability found on Adult Friend Finder's servers (Cox, 2016)
- Two notorious hackers – one known as Revolver or 1×0123 and one known as Peace – are separately claiming to have broken into the hookup site AdultFriendFinder (AFF) and breached millions of user account details(Vaas, 2016).
- Peace said that he'd pried open a backdoor that had been publicized on the hacking forum Hell: the place where last year's breach data was listed for sale for 70 Bitcoin(Vaas, 2016).
- The second time its being hit. In May 2015, it was hit by a hacker known as ROR[RG](Vaas, 2016)

Were any escalation(s) stopped - how?

- The Twitter User account was deleted few days later(Cox, 2016)
- notified law enforcement and the FBI
- hired Mandiant to “investigate the incident, review network security and remediate the system
- launched an internal investigation to “review and expand existing security protocols and processes
- temporarily disabled the ability to search by username, and masked the usernames of “any users we believe were affected by the security issue.
- All potentially affected members are being advised to change their usernames and passwords.

.(Goldman, 2015)

Was the Business Continuity Plan instigated?

- There was no evidence of a business continuity plan in the review.
- **The affected servers should be isolated for proper forensic.**
- **Another temporary server can be setup while investigation is going on so as not to completely shut down network**

Was the ICO notified?

- Although it appears the legal entity was incorporated in the USA. The company was based in California and with offices in Florida(Whittaker, 2016)
- Upon learning of the incident, the company immediately took several steps to review the situation, notified law enforcement and retained external partners to support its investigation(FriendFinder Networks Inc., 2016)
- **We must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay (ico.org.uk, 2022).**

Were affected individuals notified?

- Twelve hours later, 1x0123 said he had worked with Adult FriendFinder and resolved the problem adding that, “...no customer information ever left their site.” However, those claims don’t align with leaked source code and the existence of the databases obtained by LeakedSource(Ragan, 2016)
- FFN is in the process of notifying impacted users so they can take steps to protect themselves. FFN has since taken a number of steps to remediate and, based on the investigation to date, no credit card or payment information was compromised. Based on the ongoing investigation, FFN has not been able to determine the exact volume of compromised information. However, because FFN values its relationship with customers and takes seriously the protection of customer data, FFN is in the process of notifying affected users to provide them with information and guidance on how they can protect themselves.FFN encourages users to change their passwords and visit ffn.com/security_recommendations.html for additional security information and recommendations(FriendFinder Networks Inc., 2016)

continued...Were affected individuals notified?

- FFN needs to give the details: their names and contact details; the estimated date of the breach; a summary of the incident; the nature and content of the personal data; the likely effect on the individual; any measures you have taken to address the breach; and

  how they can mitigate any possible adverse impact.

What were the social, legal and ethical implications of the decisions made?

No further comments noted from the Law enforcement perspective

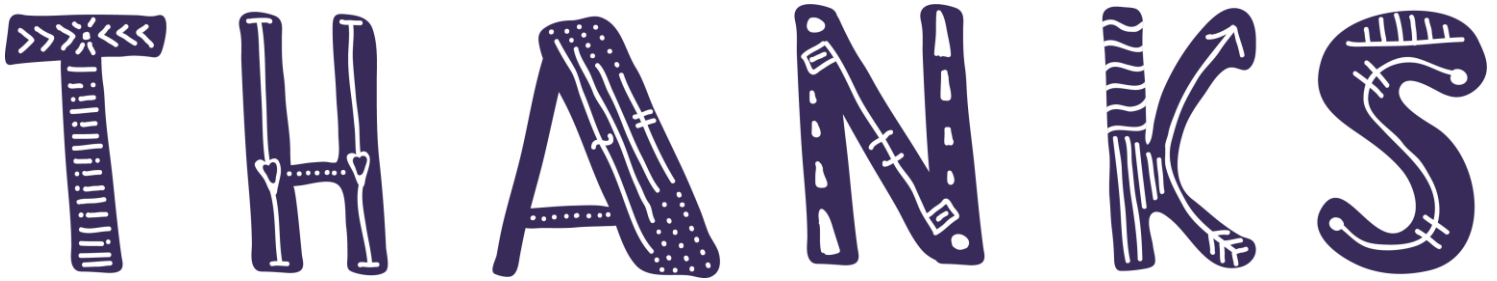
In the event of failure to comply to GDPR laws, the are two categories of Sanction by the ICO. The Higher Maximum and the Standard Maximum

- The higher maximum amount, is £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher.
- standard maximum; If there is an infringement of other provisions, such as administrative requirements of the legislation, the standard maximum amount will apply, which is £8.7 million or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

(ICO, 2021)

If you had been the ISM for the organisation you selected what mitigations would you have put in place to stop any reoccurrences?

- Implement strong password policies
- Stronger encryption technologies like The Advanced Encryption Standard(AES). Also commonly paired with Rivest-Shamir-Adlemanencryption algorithm RSA
- Whitelisting: Restrict our input parameter to accept a whitelist of acceptable files and reject all the other inputs that do not strictly conform to specifications(Chandel, 2020).
- Exclude the directory separators “/” to prevent our web-application from the directory traversal attack which may further lead to the Local File Inclusion attacks(Chandel, 2020).


THANKS