My FitnessPal

What types of data were affected?

Personally identifiable information was affected in this data breach. Any set of data that can be used to identify an individual is regarded as personally identifiable data.

Grimes (2021) states that Social Security numbers, mailing or email addresses, and phone numbers have most commonly been considered PII, but technology has considerably expanded PII's scope. It can include an IP address, login IDs, social media posts, or digital images. Geolocation, biometric, and behavioural data can also be classified as PII.

What happened?

The organisation did not know how the data got stolen. The stolen data appeared on sale on the dark web a year later. They notified the law enforcement authorities, and they also appointed a data security firm to assist with the investigation.

Who was responsible?

The responsible party was known, and the data security firm is investigating.

Were any escalation(s) stopped - how?

There were no actions taken to stop the escalations. The organisation only notified users after the fact, implying that the organisation became aware of the bridge after it took place.

Was the Business Continuity Plan instigated?

No. The article does not say if the breach impacted business continuity.

Was the ICO notified?

The Law enforcement authorities were informed. However, it is unclear if the Information Commissioner's Office is also a law enforcement authority.

Were affected individuals notified?

They notified the system users. However, the affected individuals may be current users, and some be previous users of the system. Article 5 of the GPDR states that personal data should only be collected and processed for a legitimate specific purpose. If the stolen data contained PII for previous users, this would imply a violation of GPDR

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

Data breaches need to be reported within a prescribed period after discovery, and by notifying the authorities, the organisation complied with the law. It was ethical of the organisation to inform users of the breach.

15. My Fitness Pal

Date: February 2018
Impact: 150 million user accounts

In February 2018, diet and exercise app MyFitnessPal (owned by Under Armour) exposed around 150 million unique email addresses, IP addresses and login credentials such as usernames and passwords stored as SHA-1 and bcrypt hashes. The following year, the data appeared for sale on the dark web and more broadly. The company acknowledged the breach and said it took action to notify users of the incident. "Once we became aware, we quickly took steps to determine the nature and scope of the issue. We are working with leading data security firms to assist in our investigation. We have also notified and are coordinating with law enforcement authorities," it stated.