Massive Robinhood ransomware attack pulled off via customer support phone call

Article

The news: The personal data of more than **7 million** Robinhood customers was compromised during a massive data breach at the trading platform November 3.

More on this: An unauthorized third party reportedly "socially engineered a customer support employee by phone" and gained access to customer support systems, per **Robinhood**. Social engineering uses deception and manipulation to get people to divulge confidential information, leading to access to internal systems.

- The attacker was able to get a **list of email addresses for approximately 5 million people** and **full names for a separate group of 2 million**.

- For a smaller group of 310 people, additional personal information, including names, dates of birth, and ZIP codes, was also exposed. "More extensive account details" were exposed for about 10 customers.

- Robinhood, which has **18.9 million active monthly users**, said no customers have had a "financial loss" due to the incident; the company uses data aggregator Plaid to connect to users' bank accounts.

- Robinhood said the unauthorized third party sought an "extortion payment," and the company notified law enforcement but did not say whether it had made any payments.

The bigger picture: Robinhood's breach through social engineering exposes potential weaknesses in customer support departments. Would-be hackers can gain access to a business's customer support systems, where vital personal data is stored.

- The ransomware attack reveals that data in a secure and distributed service or app can be compromised, exposing the fact that **people can be the weakest link in cybersecurity**.

- Personal user data can be held hostage in ransomware attacks or sold to identity thieves.

- The **average cost of a data breach had been $3.8 million** since 2015, per IBM, but has risen 15% to **$4.4 million since the pandemic began**.

Dive deeper: Read how the Robinhood data breach won't help falling trading volume in our Fintech Briefing.

Average Global Cost of a Data Breach
Cost in millions of US dollars

Year	Cost
2015	3.8
2016	4.0
2017	3.7
2018	3.8
2019	3.9
2020	3.8
2021	4.4
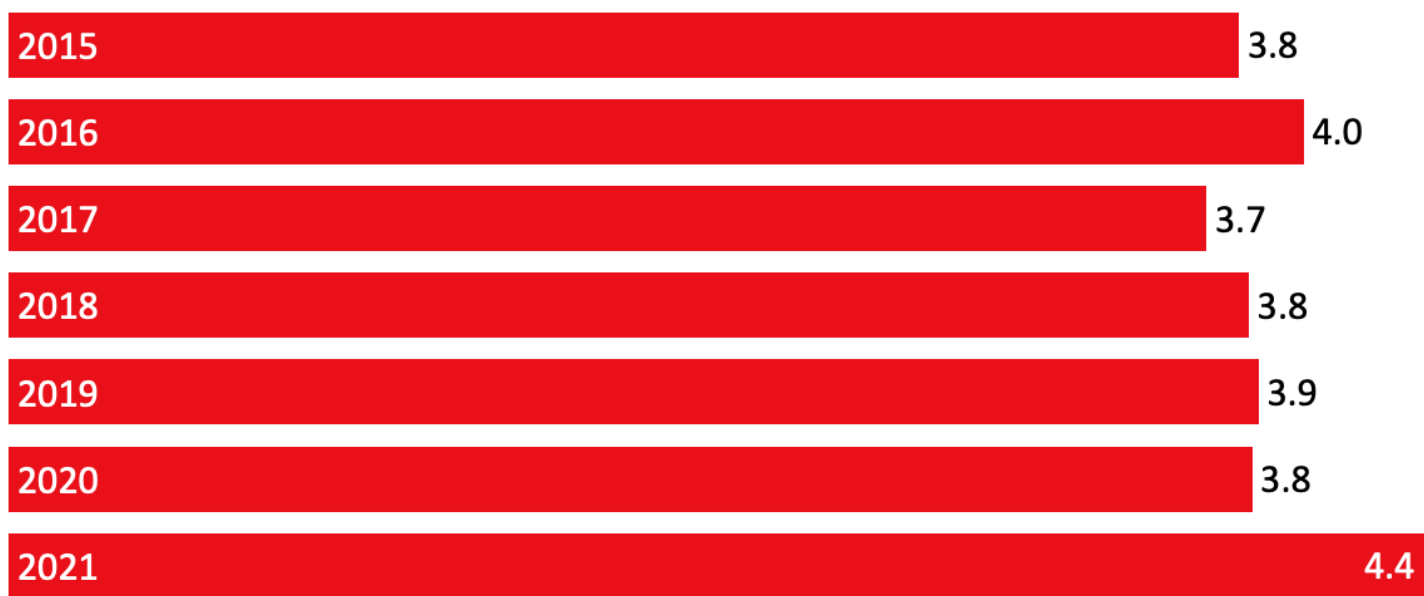
Source: IBM, 2021
Methodology: Data for "2021" comes from March 2020 to May 2021

1057568018083

InsiderIntelligence.com

INSIDER INTELLIGENCE | eMarketer