DATA BREACH ALERT

Inside the Home Chef Data Breach

Rippleshot

WHAT HAPPENED

8 Million People

A database of an estimated 8 million Home Chef customer records was found on a dark web marketplace. Home Chef acknowledged a data breach 11 days after security site Bleeping Computers broke the news on May 9.

$500-$2,500 Price Tag

Reports indicate Shiny Hunters, a hacking group, was selling the Home Chef database of user records for up to $2,500.

Partial CC Data Impact

The last four digits of credit card numbers were among the compromised details.

7 Types of Personal Data

Breached data included the user's name, email address, phone number, encrypted password, last four digits of their credit card, home address and subscription information

WHAT YOU NEED TO KNOW

- Home Chef, a Chicago-based meal kit and food delivery company, announced a data breach after a hacker attempted to sell information on a dark web marketplace.
- Home Chef said the last four digits of a customer's credit card was accessed, as they don't store complete payment information in their databases.
- Home Chef emailed affected customers. The company didn't officially announced how many customers were impacted by the security incident, but the security site Bleeping Computer reported that hackers claimed to be selling a database of 8 million users.
- The Home Chef breach was announced among 10 other companies who allegedly had databases of customer records for sale on the dark web. So far, only Home Chef and The Chronicle of Higher Education have confirmed or acknowledged a breach.

Questions? Contact Customer Success Director Jesse Sherwood at jesse@rippleshot.com

DATA BREACH ALERT

Inside the Home Chef Data Breach

Rippleshot

Rippleshot's Take: The Potential Fraud Fallout

Partial credit card payment numbers were exposed in latest data breach, along with a large amount of exposed PII data. While the company indicated that full card data is not stored on its systems, having partial card data along side the other PII that was compromised can be enough for some hackers to confirm an identity. Other types of fraud that can occur as a result of the stolen data being sold on the dark web include: **Synthetic Fraud**, **Account Takeove**r and **New Account Opening Fraud.**

Although passwords were encrypted, threat actors can use programs to decrypt the password. For users that use the same passwords on other sites, those accounts could become compromised. Dark Web crime rings are increasing as the availability of exposed PII grows substantially.

We recommend educating customers on the above types of fraud and the impact of these breaches

- Remind customers of data security best practices and common fraud schemes associated with these incidents — i.e. that they should never be contacted by their bank to verify personal information like birthdays and SSNs.
- Remind customers to regularly update passwords, especially if their information has been breached.

For Rippleshot Sonar Clients:

1. Because only the last 4 digits of cards were breached, we don't currently anticipate a spike in compromised cards.
2. Within Sonar, a list of cards from your portfolio that have transacted with the merchant "Home Chef" or "homechef.com" during the last 12 months will be uploaded to your Alerts page.
3. See if any of those cards are red and re-issue those cards.
4. Continue to monitor the alert file to understand how fraud activity related to this compromise is trending.
5. Potentially place all cards identified, but not reissued, in a watch list.

Questions? Contact Customer Success Director Jesse Sherwood at jesse@rippleshot.com