Over 71k Impacted by Credential Stuffing Attacks on Chick-fil-A Accounts

American fast food restaurant chain Chick-fil-A has started notifying roughly 71,000 individuals that their user accounts have been compromised in a two-month-long credential stuffing campaign.

In a notification letter to impacted customers, a copy of which was submitted to multiple Attorney General offices, Chick-fil-A says the accounts were compromised in a series of automated attacks targeting both its website and mobile application.

A low cost, low risk type of cyberattack, credential stuffing relies on automation – typically via bots – to test hundreds of thousands of username-password pairs against new targets. What makes credential stuffing possible, however, is users' habit of reusing the same password across multiple online services.

The tested credentials come from other data breaches and can often be acquired relatively easily and at low cost from various underground sources, and this is what happened in the Chick-fil-A incident as well.

"Following a careful investigation, we determined that unauthorized parties launched an automated attack against our website and mobile application between December 18, 2022 and February 12, 2023 using account credentials (e.g., email addresses and passwords) obtained from a third-party source," Chick-fil-A says.

The fast food company says that the attackers eventually gained access to Chick-fil-A One accounts and to the information available within.

The compromised information, the company says, includes names, email addresses, masked credit/debit card numbers, Chick-fil-A One membership information, and the available Chick-fil-A credit for each account.

“In addition, if saved to your account, the information may have included the month and day of your birthday, phone number, and address. Importantly, unauthorized parties would only have been able to view the last four digits of your payment card number,” Chick-fil-A tells customers.

Chick-fil-A says it has already prompted impacted users to reset their passwords, removed stored credit/debit card payment methods, and temporarily froze any funds that users might have loaded into their Chick-fil-A One accounts.

The company says it has restored account balances for the impacted accounts, which in some cases included refunding to users’ original form of payment, and added rewards to accounts.

Chick-fil-A told the Maine Attorney General’s Office that more than 71,000 individuals were impacted in the incident.

Related: Media Giant News Corp Discloses New Details of Data Breach

Related: Pepsi Bottling Ventures Discloses Data Breach

Related: Patient Information Compromised in Data Breach at San Diego Healthcare Provider

Over 71k Impacted by Credential Stuffing Attacks on Chick-fil-A Accounts