# CHICK-FIL-A CONFIRMS DATA BREACH

*Hodgson Russ Food & Beverage Alert*
March 20, 2023

Chick-fil-A is warning its customers about a data breach that may have put their personal information at risk. The fast food giant says it received information that hackers launched an attack on its website and mobile app between December 18, 2022, and February 12, 2023. After commencing an investigation with a national forensics firm, Chick-fil-A determined the app was actually attacked on February 12. However, in early January, Chick-fil-A had received reports from several customers that their Chick-fil-A app credentials were used to access linked bank accounts and transfer funds.

On March 2, the corporation sent a letter to customers who it believes were affected, detailing the breach, which is estimated to have impacted at least 71,000 of mobile app customers. Chick-fil-A says hackers obtained email addresses and passwords from a third party source and used them to gain access to customers' information stored in Chick-fil-A One accounts, including names, emails, masked credit and debit card numbers (including the last four digits of card numbers), Chick-fil-A One membership numbers and mobile pay numbers, QR codes, and Chick-fil-A One credits. It also says, in some cases, hackers were able to access customers' birthdays, phone numbers, and addresses.

According to Chick-fil-A, they immediately required customers who use its app to reset their passwords and remove stored payment methods. The corporation also temporarily froze funds in Chick-fil-A One accounts and in some cases, restored the balances of those accounts if fraudulent activity had been found.

In its letter to customers, Chick-fil-A also outlined additional steps customers could take to protect their personal information, including by reviewing account statements, ordering a free credit report, and placing a fraud alert on a credit file.

Data breaches have been skyrocketing in the food and beverage industry, and elsewhere. Cybersecurity firm Surfshark recently reported that it saw a 70% increase in data breaches globally in the third quarter of 2022 compared to the previous quarter. Further, the breadth and scope of the breaches are increasing. In 2019, DoorDash was hit by a data breach which impacted approximately 4.9 million consumers. In 2021, JBS, the world's largest meat supplier, was hit with a ransomware attack that shut down operations in the United States and Australia and resulted in an $11M bitcoin payout to the hackers. Five Guys job applicant data was breached in late 2022.


### Attorneys

Christine Bonaguide
Jillian Brevorka
Reetuparna Dutta
Asia Evans
George Eydt
Joshua Feinstein
Emily Florczak
Andrew Freedman
Neil Friedman
Nathaniel Lucek
Ryan Lucinski
Michael Maxwell
Elizabeth McPhail
Michelle Merola
Michael Risman
Hugh Russ III
Christian Soller
Daniel Spitzer


### Practices & Industries

Cybersecurity & Privacy
Food & Beverage

# CHICK-FIL-A CONFIRMS DATA BREACH

On Monday, March 6, 2023 a class action suit was filed against Chick-fil-A in federal district court in Georgia. While very few states have data privacy laws in place that permit a private right of action by the victim of a breach, many consumers are pursuing complaints under the Federal Trade Commission Act as well as violations of Deceptive Trade Practices Acts. However, states are beginning to act in providing consumers and victims of breaches further causes of action.

California recently passed the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act which provide for a private right of action for the victims of a data breach. New York has a number of bills pending that may expand its laws surrounding data privacy and data breaches.

*Key Takeaways for the Food and Beverage Industry*

It is imperative that the food and beverage industry continues its aggressive data protection efforts (and keeps up with changing trends and new threats) as it digitally innovates its customer outreach and streamlines the consumer interaction experience. The Federal Bureau of Investigation and the United States Cybersecurity & Infrastructure Security Agency have put together materials for companies to follow on best practice to protect data both internally and externally. Further, if a company becomes aware of a data breach they should investigate immediately and notify the victims as quickly as possible. Finally, it has become common place for companies to offer free credit monitoring to victims as well.

For more information on this security breach, contact Jillian E. Brevorka (336.271.4780) or any other member of the Hodgson Russ LLP Food & Beverage Practice.