A Bad Week For Restaurants And Foodies

September 27, 2019 - Dunkin Donuts and Door Dash are having a tough week. One of them experienced a large data breach. The other is getting sued over a data breach that it allegedly did nothing to fix. And as always, consumers are caught in the middle.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Dunkin Donuts was sued this week by the State of New York. State Attorney General, Letitia James filed suit against the chain over what was initially a relatively small 2015 data breach. According to the suit, the company was notified about the breach by one of its app developers. Over a five day period, more than 19,000 Dunkin customers had their accounts accessed as a result. But the company never took corrective action.

That lack of response led to a much larger data breach in 2018, when 300,000 Dunkin accounts were hacked. Even though the company received numerous report of fraudulent activity from their customers after the initial breach, customer notifications were never made. Customers weren't even instructed to change their passwords and the company failed to freeze their accounts, according to the suit. New York is seeking restitution and unspecified damages.

Also this week, food delivery service Door Dash has announced a much larger data breach. In this case, information was released customers, company workers and merchants; totaling around 4.9 million people.

Breached data included names, addresses, email addresses, order histories and phone numbers. Additionally, the last four digits of customer credit cards, and the last four digits of company worker bank accounts may have been affected. The company is saying that it doesn't believe that the data could be used directly to commit fraud or identity theft, but if history is any indicator then anyone with access to this data may be able to assemble the missing pieces needed to commit fraud.

The company has said that there is an ongoing investigation into the breach and that it has taken steps to better protect its stored data. The breach affects anyone who had their data stored on the company's platform prior to April 2018.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS