ROTHWELL FIGG

FTC Actions Hold Data Privacy Lessons For 2023

Authored by Kristen Logan for Law360
Article
1.3.23

The Federal Trade Commission will have its eye on privacy and data security enforcement in 2023.

In August, the agency announced that it is exploring ways to crack down on lax data security practices. In the announcement, the FTC explained that it was "concerned that many companies do not sufficiently or consistently invest in securing the data they collect from hackers and data thieves."

These concerns are reflected in some of the FTC's recent privacy enforcement actions. This article explores two significant FTC privacy actions of 2022 and provides three key tips to avoid similar proceedings in 2023.

Recent FTC Enforcement Actions

Earlier in 2022, Chegg Inc., an educational technology company, faced enforcement action from the FTC. Chegg is an online platform that provides customers with education-related services like homework help, tutoring and textbook rentals.

According to the FTC, Chegg failed to uphold its security promises to "take commercially reasonable security measures to protect the Personal Information submitted to [Chegg]."

In its complaint, the FTC explained that Chegg's lax cybersecurity practices led to four data breaches resulting in the exposure of employees' financial and medical information and the personal information of 40 million customers.[1]

The FTC's complaint points out that three of the four data breaches suffered by Chegg involved phishing attacks targeted at Chegg's employees. The other data breach occurred when a former Chegg contractor shared login information for one of Chegg's cloud databases containing the personal information of customers.

Key Contact

Kristen Logan

Related Areas of Practice

Cybersecurity and Privacy Litigation

Privacy, Data Protection, and Cybersecurity

Chegg uses a third-party cloud service provided by Amazon Web Services Inc., the cloud computing division of Amazon.com Inc., to store customer and employee data. The information stored by Chegg on AWS includes information related to its customer's religion, ethnicity, date of birth and income.

According to the complaint, Chegg allowed employees and third-party contractors to access these databases using credentials that provided full access to the information and administrative privileges.

Moreover, the personal data stored by Chegg was stored in plain text and not encrypted. The FTC's complaint also explains that Chegg encrypted passwords using outdated cryptographic hash functions with known vulnerabilities.

With Chegg's recent data breaches in mind, the FTC's complaint highlighted these inadequacies in Chegg's data security practices:

- Chegg failed to consistently implement basic security measures such as encryption and multifactor authentication;
- Chegg failed to monitor company systems for security threats;
- Chegg stored information insecurely; and
- Chegg did not develop adequate security policies and training.

The FTC's order requires that Chegg document and limit its data collection practices. The FTC also requires Chegg to allow customers access to the data collected on them and to abide by its customers' requests to delete such data.

The order further requires Chegg to implement multifactor authentication, or another suitable authentication method, to protect customer and employee accounts.

In another FTC enforcement action in 2022, the FTC brought another enforcement action against Drizly LLC, an online platform allowing customers to place orders for beer, wine and liquor delivery.

Notably, the FTC also acted against Drizly's CEO, James Cory Rellas, in his personal capacity. Similar to Chegg, Drizly hosts its software on AWS.

As a result, Drizly's customer data, including passwords, email addresses, postal addresses, phone numbers, device identifiers and geolocation information, were all stored on AWS.

The 2022 complaint alleges that in 2018 Drizly and Rellas learned of problems with the company's data security procedures after a security incident in which a Drizly employee posted the company's AWS login information on GitHub Inc.[2]

In its complaint, the FTC states that the 2018 incident put Drizly "on notice of the potential dangers of exposing AWS credentials and should have taken appropriate steps to improve GitHub security."

But Drizly failed to address the issues with its security procedures. As a result, in 2020, a hacker gained access to Drizly's GitHub login credentials, hacked into the company's database and acquired customer information.

The FTC's complaint also alleged that Rellas contributed to these failures by not hiring a senior executive responsible for the security of consumers' personal information collected and maintained by Drizly.

The FTC's complaint attributed the following data security failures to Drizly:

- Drizly failed to develop and implement adequate written security standards and train employees in data security policies;
- Drizly failed to store AWS and database login credentials securely and further failed to require employees to use complex passwords;
- Drizly did not periodically test its existing security features; and
- Drizly failed to monitor its network for attempts to transfer consumer data outside the network.

The FTC's October order requires Drizly to destroy all unnecessary data, limit the future collection and retention of data, and implement a data security program. Drizly must also replace its authentication methods that currently use security questions with multifactor authentication.

Additionally, Drizly is now required to encrypt Social Security numbers on the company's network. The order will follow Rellas to any future companies, demanding that he personally abide by these data security requirements in future endeavors.

Enforcement actions brought by the FTC this year provide guidelines to companies wishing to avoid FTC enforcement actions.

In fact, FTC Chair Lina M. Khan's statement on the Drizly decision stated "[t]oday's action will not only correct Drizly's lax data security practices but should also put other market participants on notice."

Thus, the following steps are suggested to safeguard a company from FTC enforcement action.

Educate Employees on Cybersecurity Measures

Companies should emphasize data security education for their employees and contractors. It is suggested that companies introduce new employees to their data security practices during the onboarding process and follow up with regularly scheduled training for existing employees.

One crucial area to educate employees on is how to safeguard company credentials.

Companies should implement policies and procedures to prevent the storage of unsecured access keys on any cloud-based services. Companies should also have a policy and guidelines requiring the use of strong passwords and multifactor authentication to secure corporate accounts and information.

Companies should implement basic security measures for employees' and contractors' access to sensitive user information. For example, companies should regularly monitor who accesses company repositories containing sensitive consumer information.

Companies might also consider only allowing authenticated and encrypted inbound connections from approved Internet Protocol addresses to access sensitive consumer data.

Performing regular audits can help companies ensure each employee only have access to what is needed to perform that employee's job functions.

In addition, companies should use audits to identify and terminate unneeded or abandoned employee accounts, such as accounts that are left open after an employee leaves a company or when an employee transfers to a different division/role.

Follow Through on Privacy and Data Security Promises

The FTC tends to pursue companies that fall short of the data security promises they make to consumers.

When a company promises consumers that it will adhere to reasonable data security practices, it is their responsibility to implement basic security measures and checks to fulfill this promise. Those security measures might include encryption, multifactor authentication and complex passwords.

It is also imperative that companies regularly review and update their data security practices. The FTC's recent orders show that adhering to outdated data security measures amounts to having lax data security practices.

Individuals in charge of the company's data security practices should stay abreast of developments in the field.

Respond to Data Security Incidents Quickly and Transparently

The FTC displays little leniency for companies and executives already on notice of data security issues within their company.

It is imperative that companies act promptly when data security events are discovered, and that companies be transparent with customers when a data security event occurs — regarding the occurrence of the event, measures the company took to prevent the event and measures the company is taking to rectify the event.

Companies should be vigilant in their efforts to discover data security events. Procedures and policies should be implemented to stay on top of data security events within the company's networks and systems.

For example, adopting file integrity monitoring tools and tools for monitoring anomalous activity can assist with detecting these events.

After implementing these safeguards, they must be tested at least once a year for vulnerabilities, as suggested in the FTC's orders against Drizly and Chegg.

Conclusion

The FTC's prior enforcement actions serve as a cautionary tale for companies seeking to avoid similar enforcement actions from the agency.

Engaging in efforts to educate employees on data security practices, following through on data security promises, and responding to data security incidents properly can help companies reduce the likelihood of being subject to these proceedings.

[1] https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Complaint.pdf.

[2] https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf.

This article was originally published in Law360's Expert Analysis section on January 3, 2023. Read more at: https://www.law360.com/articles/1561075/ftc-actions-hold-data-privacy-lessons-for-2023.