Published on *The National Law Review* https://natlawreview.com

SHEIN's $1.9 Million Data Breach: A Cautionary Tale for Online Fashion Brands

Article By:

Grace E. Fucci

The New York Attorney General ("NYAG") fined fast-fashion company, Shein Distribution Corporation ("SHEIN"), $1.9 million for failing to properly handle a data breach in late 2022. Hackers attacked SHEIN and stole the credit card and personal information of nearly 40 million SHEIN customers. In an Assurance of Discontinuance issued by the NYAG in 2022, the NYAG determined that SHEIN "made a misrepresentation" on its website. According to the NYAG, SHEIN knew that customer credit card information was stolen but told website visitors that the company saw "no evidence" that customer credit card information was compromised. In addition to the fine imposed by the NYAG, SHEIN must implement a comprehensive information security program, as well as safeguards and controls for handling, storing, and processing personal information. The NYAG also mandated the company to submit third-party assessments of these systems, networks, and policies annually until 2027.

How Can Fashion Brands Avoid Legal Consequences for Data Breaches?

Fashion companies can avoid outcomes like SHEIN's by strictly following applicable laws and ensuring there are internal information security programs in place. The Federal Trade Commission ("FTC") offers many recommendations for businesses who experience data breaches. The three most important recommendations according to the FTC are:

1. Secure your operations (secure physical areas and change access codes; establish and mobilize a breach response team; and assemble data forensic and legal experts);

2. Fix vulnerabilities in your systems (e.g., network segmentation and communications) as soon as they are identified; and

3. When required by law, timely notify the appropriate parties.

Another fast-fashion retailer, experienced a breach of over half a million former and current employees' social security numbers. By sending data breach notification letters as advised by the FTC, the retailer complied with regulatory requirements and was not subjected to penalties. Notification statutes vary by state, so it is best to understand your state's notice and regulatory requirements.

Why Should Fashion Companies Remain Concerned About Information Security Issues?

According to *Global Data* and *Yahoo Finance*, retail companies are "prime targets" for cyberattacks given that they operate on small margins and funding for robust cybersecurity software is limited. Furthermore, retailers have more points of entry for workers given the need for access to perform daily operational tasks. The more people have access to the system, the more physical or virtual vulnerabilities are generated.

Jax England contributed to this article

National Law Review, Volume XIV, Number 207