Cybersecurity Awareness Month –

Fast-Fashion Under the Spotlight: SHEIN and ROMWE Owner Fined $1.9M for Significant Data Breach Failures

Zoetop, the parent company behind online fashion retailers SHEIN and ROMWE, has been fined $1.9 million by New York State after it failed to properly inform customers of a data breach that affected millions of users. A popular fashion resource for millennial and Generation Z shoppers, SHEIN and ROMWE sell clothing and accessories through several websites and mobile apps. An investigation by the New York Attorney General (NYAG) revealed that Zoetop failed to safeguard consumers' information before it suffered a data breach in 2018, failed to take action to protect the impacted accounts after the breach and downplayed the extent of the cyberattack to customers.

In June 2018, Zoetop (now SHEIN Distribution Corporation in the United States) was the victim of a cyberattack. Zoetop's payment processor alerted Zoetop that the retailer's systems were breached, following fraud reports from a credit card company and a bank. The credit card network found SHEIN customers' card data for sale on an internet forum known for exposing stolen credit card data. Afterward, Zoetop hired a cybersecurity firm to conduct a forensic investigation and a payment card industry (PCI) forensic investigator to look into the cyberattack.

The cybersecurity firm confirmed hackers stole credit card information and personal information, including names, email addresses and hashed account passwords of certain SHEIN customers. While storing passwords in hashed format would arguably mitigate risk of compromise because hashing should turn plain text into an unintelligible series of numbers and letters, here the NYAG determined that the hashing algorithm used by Zoetop had been known to be insufficient to protect against attacks. In total, 39 million SHEIN account credentials were stolen across the globe, including the credentials of more than 375,000 New York residents.

Of the 39 million impacted accounts, Zoetop identified a subset of 6.42 million accounts that had previously placed an order with SHEIN and, of this subset, contacted account holders in the United States, Canada and Europe, recommending that these account holders independently initiate a password reset. Additionally, Zoetop offered identity theft protection for the subset of United States account holders contacted. The NYAG concluded that Zoetop issued misleading information about the June 2018 breach via a website FAQ in which Zoetop claimed that only 6.42 million customers were affected by the breach and that Zoetop would directly notify affected customers. However, 32.5 million account holders affected by the breach were not notified that their credit card information and personal information may have been compromised.

In addition to the cybersecurity firm investigation, the payment card industry requires merchants retaining cardholder data to adhere to self-regulated PCI Data Security Standards. According to the NYAG findings, Zoetop didn't provide a PCI forensic investigator sufficient access to conduct a thorough cyber investigation. However, the PCI forensic investigator still identified multiple PCI Data Security Standards (DSS) failures, including a failure to protect stored credit card data.

Further, the PCI forensic investigator indicated Zoetop did not adhere to network monitoring and testing

and had not developed, or refused to provide, the forensic investigator with copies of Zoetop's documented cybersecurity policies and procedures. The NYAG findings state Zoetop independently became PCI DSS-certified in April 2019, and SHEIN Distribution Corporation has been compliant since.

In June 2020, two years after the 2018 cyberattack, Zoetop discovered that customer login credentials for ROMWE were available in plain text on the dark web. Again, Zoetop hired a cybersecurity firm to investigate. The investigation revealed ROMWE customer credentials were likely stolen in the 2018 data breach incident. The investigation revealed that more than 7 million ROMWE accounts were stolen, 500,000 of which belonged to New York residents.

Realizing the severity of the cyberattack, Zoetop began forced password resets on all affected ROMWE and SHEIN accounts. However, Zoetop did not contact customers to inform them of the data breach. According to the NYAG report, customers saw the following message: "Your password has not been updated in more than 365 days. For your protection, please update it now."

As additional login credentials from ROMWE customer accounts continued to appear on the dark web, Zoetop decided to force password resets for the ROMWE accounts that existed at the time of the data breach. On Dec. 30, 2020, Zoetop finally notified ROMWE customers about the data breach and offered identity theft protection for United States account holders.

As a result of Zoetop's agreement with the NYAG, Zoetop must pay $1.9 million in penalties and costs. Zoetop must also refrain from misrepresenting the collection, use and maintenance of customer personal information, and relatedly, any aspect of a security event. Additionally, Zoetop shall implement and maintain a comprehensive information security program that "includes robust hashing of customer passwords, network monitoring for suspicious activity, network vulnerability scanning and incident response policies requiring timely investigation, timely consumer notice and prompt password resets." Finally, Zoetop must provide the NYAG copies of any third-party cybersecurity documents and assessments for the next five years. Zoetop is offering identity theft protection for impacted customers and all customers who purchased from SHEIN or ROMWE prior to the cybersecurity incident.

Organizations must heed the lessons learned from Zoetop's data breach and its subsequent missteps. As a primary lesson learned, prompt investigation and notification to affected individuals is critical. As indicated by Zoetop's situation, failure to preliminarily assess data privacy and cybersecurity practices could result in significant fines. Additionally, the directive from NYAG is just another reminder to organizations that hold New York resident electronic data that compliance with the administrative, technical and physical safeguards delineated in New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act is an absolute necessity when it comes to risk management and mitigation.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters, including cybersecurity planning and prevention. If you have any questions about the information presented in this memo, please contact Jessica Copeland, Maureen Milmoe or any attorney in Bond's cybersecurity and data privacy practice.

BOND SCHOENECK & KING ATTORNEYS