



October 15, 2024

VIA ELECTRONIC AND FIRST-CLASS MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202
idtheft@oag.state.md.us

Re: Notice of Data Breach

Office of the Attorney General:

At Hot Topic, Inc. ("Hot Topic"), safeguarding personal information is one of our top priorities. We actively and routinely monitor and audit our systems to ensure that each customer's data is protected. However, despite our efforts, there was a data security incident that may have involved customers' personal information. Below is a summary of this incident and our response.

What Happened?

We recently identified suspicious login activity to certain Hot Topic Rewards accounts. Following a careful investigation, we determined that unauthorized parties launched brief automated attacks against our website and mobile application on July 3 and 6, 2024 using valid account credentials (e.g., email addresses and passwords) obtained from an unknown third-party source. Hot Topic was not the source of the account credentials used in these attacks.

Fortunately, our bot detection software quickly recognized this suspicious activity, and we took immediate action to block the attacks. Because of this prompt response, we were able to contain the incident early, significantly limiting its scope and duration.

Based on our investigation to date, we are not able to determine which, if any, accounts were accessed by unauthorized third parties as opposed to legitimate customer logins during the relevant time periods. To be clear, we have not determined that any login to any customer's Hot Topic Rewards account was unauthorized. We are sending this notice simply out of an abundance of caution.

What Information Was Involved?

If the login to a customer's account was not an authorized login, the information that may have been accessed includes the customer's name, email address, order history, phone number, month and day of birth, and mailing address. Importantly, if the customer saved a payment card to their Hot Topic Rewards account, the unauthorized parties would **only** have been able to view the last four digits of the card number.

HOT TOPIC

What We Are Doing

Hot Topic takes this event very seriously. After detecting the suspicious activity, we promptly began an investigation and took action to address the issue. We have been working with outside cybersecurity experts and have implemented specific steps to safeguard our website and mobile application from automated “credential stuffing” attacks, including implementing improvements to our bot protection software designed to stop such attacks. We also updated each customer’s online account to require the setting of a new password.

Finally, we will be sending a Data Breach Notification Letter to customers explaining the breach and its scope, and steps they can take to protect themselves against the misuse of their information.

Each customer’s privacy is of the utmost importance to us, and we sincerely regret any concern this incident may cause.

Sincerely,

Hot Topic, Inc.