HOT TOPIC

<<Date>>

<<ADDRESS>>

Dear <<Name>>:

Re: Notice of a Data Breach

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 your data is protected. However, despite our efforts, there was a data security incident that may have involved your personal information. We have no evidence at this time that your personal information was compromised or accessed by an unauthorized third party during this incident. However, out of an abundance of caution, we are notifying you of this incident.

Below is a summary of this incident, our response, and the steps you can take to protect yourself against potential misuse of your information.

What Happened?

We recently identified suspicious login activity to certain Hot Topic Rewards accounts. Following a careful investigation, we determined that unauthorized parties launched automated attacks against our website and mobile application on November 18-19 and November 25, 2023 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.

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. However, we determined that your account credentials were used to access your Hot Topic Rewards account during the time periods of suspicious login activity. To be clear, we have not determined that any login to your Hot Topic Rewards account was unauthorized. We are sending you this notice simply out of an abundance of caution.

What Information Was Involved?

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

What We Are Doing

Hot Topic takes this event very seriously. After detecting suspicious activity, we promptly began an investigation and took action to address the activity. 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 deploying bot protection software designed to stop such attacks. We will also be updating your online account to require you to set a new password. When this update happens, your old password will no longer work and you must set a new password in order to shop with us. We understand setting a new account password may be inconvenient, but this action will ensure that any third parties who may have your access credentials can no longer use them on our website or mobile app.

What You Can Do

If you have not done so already, please reset your Hot Topic Rewards account password as soon as possible. We urge you to choose a strong password (not easy-to-guess) and unique to Hot Topic (e.g., not a password that you use on other websites/accounts).

Please review the enclosed Steps You Can Take to Protect Your Information ("Guide") for additional information on steps you can take to monitor and protect your personal information. We encourage you to remain vigilant against potential identity theft and fraud by carefully reviewing credit reports and account statements to ensure that all activity is valid.

For More Information

If you have any questions about this matter or would like additional information, please refer to the enclosed Guide or call toll-free 1-800-892-8674.

Your privacy is of the utmost importance to us, and we sincerely regret any concern this incident may cause you. The security of your personal information remains a top priority at Hot Topic.

Sincerely,

Hot Topic, Inc.

Steps You Can Take to Protect Your Information

Monitor Your Accounts.

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Request A Security Freeze on your Credit Report.

You can place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Place A Fraud Alert on Your File.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-836-6351
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information.

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission.

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement

For District of Columbia residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.
For Maryland residents, the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov.
For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.
For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.
For North Carolina Residents: The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716- 6400, and online at www.ncdoj.gov.
For Oregon Residents: You can obtain information from the Oregon Attorney General's Office about preventing identity theft. You can contact the Oregon Attorney General at: Oregon Department of Justice 1162 Court St. NE Salem, OR 97301 1-(877) 877-9392 (toll-free) https://www.doj.state.or.us/.
For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 367 Rhode Island residents impacted by this incident. This notice has not been delayed by a law enforcement investigation.