The Topps Company, Inc.
One Whitehall St. 5th fl. New York, NY 10004-2109
Telephone: (212) 376-0300

February 21, 2019

Via U.S. Mail
New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Breach Notification

To Whom it May Concern:

On December 26, 2018, The Topps Company, Inc. (Topps) became aware of possible unauthorized access to the www.topps.com website. Topps immediately launched an investigation with the assistance of an external security firm. On January 10, 2019, following the investigation, Topps confirmed that an unauthorized third party placed malicious code at the website, which might have resulted in access to or acquisition of payment card and other information that customers provided when placing orders through the website between November 19, 2018 and January 9, 2019. Topps cannot confirm whether any personal information was accessed or acquired, but the investigation confirmed that this was possible during the relevant time period.

The personal information potentially accessed or acquired includes names, mailing addresses, e-mail addresses, and payment information (including credit or debit card number, card expiration date, and security code) for customers who completed a purchase through the Topps website between November 19, 2018 and January 9, 2019.

Once Topps became aware of this incident, the company engaged a security firm to examine the network. They cut off all known means through which unauthorized parties could gain access to the website. Topps worked with the security firm and website development company to implement measures to strengthen the security of the system and help prevent a similar incident from happening again. Topps has since upgraded the website platform.

Approximately 33 New Hampshire residents may have been affected by this incident. A copy of the notice that will be mailed to potentially affected New Hampshire residents on February 22, 2019 is enclosed.

Should you have any questions, please feel free to contact me by mail at One Whitehall Street, New York, NY 10004, by phone at (212) 376-0300, or by e-mail at JThaler@topps.com.

Sincerely,

Jason Thaler

Jason S. Thaler
General Counsel

Enclosure

4812-5284-1094, v. 1

The Topps Company, Inc.
One Whitehall St. 5th fl. New York, NY 10004-2109
Telephone: (212) 376-0300

February 22, 2019

NOTICE OF DATA BREACH

Dear Topps Customer,

The Topps Company, Inc. ("Topps") understands the importance of protecting the personal information of our customers, and we are therefore writing to inform you that certain personal information you submitted through the www.topps.com website when making a purchase recently may have been compromised. This incident may have affected customers who completed a purchase through the website between November 19, 2018 and January 9, 2019. Topps has since upgraded the website platform, and this notice does not apply to purchases made through the website after January 9, 2019. Because you are potentially affected, we want to share with you what we know and steps you can take to help protect your personal information.

WHAT HAPPENED?

On December 26, 2018, Topps became aware of possible unauthorized access to the www.topps.com website. We launched an investigation with the assistance of an external security firm. On January 10, 2019, following the investigation, we confirmed that there was unauthorized access to the website, which may have resulted in access to or acquisition of payment card and other information that customers provided when placing orders through the website between November 19, 2018 and January 9, 2019. While we cannot confirm whether your personal information was accessed or acquired, the investigation confirmed that this was possible during the relevant time period.

WHAT INFORMATION WAS INVOLVED?

It is possible that this incident compromised names, mailing addresses, telephone numbers, e-mail addresses, and payment information (including credit/ debit number, card expiration date, and security code) for customers who completed a purchase through the Topps website between November 19, 2018 and January 9, 2019. Based on our investigation, we have no reason to believe that information for customers who completed a purchase through PayPal was affected.

WHAT WE ARE DOING

Once we became aware of this incident, we engaged an external security firm to examine our network. We stopped the incident and worked with the security firm and our website development company to implement measures to strengthen the security of our systems and help prevent a similar incident from happening again. We have since upgraded the www.topps.com website platform.

WHAT YOU CAN DO

We recommend that you take steps to protect yourself from the possibility of identity theft. First, you should review your payment card statements and immediately report any suspicious or unauthorized activity to the issuer. Second, we recommend that you contact the three major credit reporting agencies ("CRAs") to place a fraud alert and/or security freeze on your credit file. We have enclosed with this letter contact information for the CRAs and additional information about fraud alerts and security freezes. Please read it carefully, as there are differences between a fraud alert and security freeze.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission ("FTC") recommends that you check your credit reports periodically. Under federal law, you are entitled to a free credit report once per year from each of the CRAs. Checking your credit reports periodically can help you identify problems and address them quickly. You may visit www.annualcreditreport.com, a website sponsored by the three CRAs, for more information on how to request your credit report.

If you find suspicious activity on your credit reports or have reason to believe your personal information is being misused, you should take two steps. First, call local law enforcement and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. Second, file a complaint with the FTC at www.ftc.gov/idtheft or 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. For additional information, you can write to: FTC Consumer Response Center, Room 130-B, 600 Pennsylvania Avenue, N.W., Washington, D.C., 20580. Your state's Attorney General can also provide you with information about the steps you can take to avoid identity theft.

Additional information for residents of Maryland, North Carolina, and Rhode Island is enclosed with this letter. This notification was not delayed as a result of a law enforcement investigation.

FOR MORE INFORMATION

If you have any questions, please feel free to contact us (1) by mail at One Whitehall Street, New York, NY 10004, Attn: General Counsel, (2) by e-mail at contactus@topps.com, or (3) by phone at 800-489-9149, Monday through Friday, 9 am to 4 pm ET. We sincerely apologize for any inconvenience this may have caused.

Sincerely,

The Topps Company, Inc.

Enclosures

How to Request a Credit Fraud Alert and Security Freeze

It is important to monitor your credit and be aware of unusual or fraudulent activity on any of your accounts. Here is some information on how to request a fraud alert and ask for a credit freeze, along with contact information for the three major national credit reporting agencies ("CRAs"), Equifax, Experian and TransUnion. There are differences between how the CRAs handle fraud alerts and security freezes, so please read this carefully.

Fraud Alert

There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any one of the three national CRAs:

Equifax	**Experian**	**TransUnion**
1-800-685-1111	1-888-397-3742	1-800-916-8800
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze

You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place, lift, or remove a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the CRAs at the addresses below:

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com

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;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The CRAs have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. They must also send written confirmation to you within five business days and provide you with a unique PIN or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies 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 as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus 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 one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Additional Information for MD, NC, and RI Residents

Maryland Residents: The Maryland Attorney General can provide you with information about the steps you can take to avoid identity theft: Consumer Protection Division, Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, Toll-free: 1-888-743-0023, idtheft@oag.state.md.us.

North Carolina Residents: The North Carolina Office of the Attorney General Consumer Protection Unit can provide you with information about the steps you can take to avoid identity theft: Consumer Protection Division, NC Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, Toll Free: (877) 566-7226, http://www.ncdoj.gov/.

Rhode Island Residents: The Rhode Island Office of the Attorney General Consumer Protection Unit can provide you with information about the steps you can take to avoid identity theft: RI Office of the Attorney General, 150 South Main Street, Providence, RI 02903, Phone: (401) 274-4400, E-mail: contactus@riag.ri.gov, http://www.riag.ri.gov/ConsumerProtection/About.php.