CONFIDENTIAL AND PRIVILEGED

[SAMPLE]

[FOR CALIFORNIA RESIDENTS]

CSID PIN Code: [Insert]

NOTICE OF DATA SECURITY INCIDENT

Dear _____,

The Topps Company, Inc. ("Topps") understands the importance of protecting our customers' personal information and therefore, we are writing to inform you that personal information collected through the Topps website, www.topps.com, may have been compromised. We deeply regret this incident occurred, and because you are potentially affected, we want to share with you what we know.

WHAT HAPPENED?

On October 12, 2016, Topps became aware that one or more intruders gained unauthorized access to its website. Topps immediately launched an investigation and determined that the intruders may have gained access to payment card and other data that customers entered when placing orders through the website.

WHAT INFORMATION WAS INVOLVED?

This incident may have compromised names, addresses, e-mail addresses, phone numbers, credit or debit card numbers, card expiration dates, and card verification numbers for customers as they placed orders through the Topps website between approximately July 30, 2016 and October 12, 2016. Based on our investigation, we have no reason to believe that information Topps customers may have submitted through the PayPal website to complete their purchases was accessed, but we are notifying all potentially affected customers out of an abundance of caution.

WHAT WE ARE DOING

Once we became aware of this incident, we engaged a security firm to examine our network, and we worked with the security firm, as well as our website development and hosting companies to implement multiple measures to strengthen the security of our system. We stopped the incident and continue to work with our security firm to help prevent a similar incident from happening again.

To help you monitor your information, Topps has contracted with CSID to provide one year of CSID Protector services (effective for one year from the date of enrollment), which includes CyberAgent® Internet Surveillance, Identity Theft Insurance and Identity Restoration coverage at no cost to you. If you are a victim of fraud, simply call CSID at (877) 926-1113 by December 31, 2017 and a dedicated Identity Theft Restoration agent will help you. Please provide the PIN

Code in this letter as proof of eligibility. While Identity Restoration assistance is immediately available to you, we also encourage you to activate your CSID Protector coverage as quickly as possible before December 31, 2017 to take advantage of CSID Protector coverage. Details on the coverage and instructions on how to complete enrollment in CSID Protector are enclosed with this letter.

WHAT YOU CAN DO

We recommend that you take steps to protect yourself from the possibility of identity theft. First, you should review your credit and debit card account statements, and immediately report any suspicious or unauthorized activity to your provider. 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 attached to 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 a year. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly. If a report shows accounts you did not open, inquiries from creditors that you did not initiate, personal information, such as a home address, that is inaccurate, or other information you do not understand, contact one of the credit bureaus immediately. 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.

FOR MORE INFORMATION

If you have any questions, please feel free to contact us by mail at One Whitehall Street, New York, NY 10004, Attn: Topps.com Website, by e-mail at contactus@topps.com, or by phone at 800-489-9149, Monday through Friday, 9 am to 4 pm ET.

Topps is committed to maintaining and protecting the confidentiality of our customers' personal information. 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

A fraud alert is a statement added to your credit report that alerts creditors of possible fraudulent activity within your report, and requests that they contact you prior to establishing any accounts in your name. To place a fraud alert on your credit file, you may call or write to any of the CRAs. As soon as one CRA confirms your fraud alert, the others will be notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax	**Experian**	**TransUnion**
1-888-766-0008	1-888-397-3742	1-800-680-7289
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Security Freeze

A security freeze restricts a CRA from releasing any information from your credit report without your prior written consent. Many state laws provide consumers with a right to request a security freeze, and the three CRAs voluntarily offer this service to all U.S. consumers. To place a security freeze on your credit report, you must send a written request (some states permit telephone requests) to one of the three major CRAs at the addresses identified below.

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

CRAs may charge a fee for implementing the security freeze (generally from $5 to $10) depending on the laws of the state in which you reside, but many state laws require the CRAs to waive the fee for victims of identity theft who submit a valid investigative or incident report or complaint filed with a law enforcement agency. Additional fees may apply for temporarily or permanently removing a security freeze. CRAs may also require you to submit a copy of a government issued identification card and other documents as proof of your identity. However, note that the CRAs treat security freezes differently from fraud alerts.

To effectively freeze access to your credit files, you should request the security freeze at all three major CRAs, as the CRAs do not share security freeze information with each other. Each of the CRAs requires slightly different information, so you should contact each CRA to find out exactly what is required.

CSID Protector

After you complete registration for CSID Protector coverage that Topps is providing for you at no charge, you will have increased visibility into possible fraudulent activity so you can respond more quickly if such activity is detected. You will also have a dedicated Identity Restoration agent to guide you through the recovery process should you become a victim of identity theft, and you may be eligible for reimbursement of certain expenses of up to $1,000,000, subject to the terms and conditions of the applicable insurance policy that has been issued to CSID. Topps encourages you to complete registration as quickly as possible before December 31, 2017 to take advantage of CSID Protector coverage for one year from the date of enrollment.

The sign-up process is conducted online via CSID's secure website https://www.csid.com/csid1yprotector/. You will need your CSID PIN Code shown at the top of the first page of this letter. This PIN Code can only be used once and cannot be transferred to another individual. Once you have provided your PIN Code, you will be prompted to answer a few security questions to authenticate your identity, including: previous addresses, names of creditors and payment amounts.

Should you have any questions regarding the coverage or the sign-up process, please contact CSID Member Services at (877) 926-1113 or email support@csid.com. Once you have enrolled and created your username and password, you will return to CSID's page to log in and access your personal information on future visits.

CSID Protector includes:

- **CyberAgent®:** CSID's Internet surveillance technology scours websites, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Theft Insurance**: You are eligible for reimbursement for certain expenses in the event that your identity is compromised with a $1,000,000 insurance policy that has been issued to CSID.
- **Identity Restoration**: Work with a certified identity theft restoration specialist, who will work on your behalf to restore your identity and let you get on with your life