



Marbles The Brain Store

1918 N. Mendell St. Ste 400
Chicago, IL 60642

SAMPLE DATA BREACH NOTIFICATION

[Customer First Name] [Customer Last Name]
[Address 1]
[Address 2]
[City, State, Zip]

Dear [Customer First Name] [Customer Last Name]:

We are writing to you because of an incident involving access to information associated with online purchases made on our website www.marblesthebrainstore.com

Although we are unaware of any actual misuse of your information, we are providing notice to you about the incident and about tools you can use to protect yourself against possible identity theft or fraud.

What Happened?

Aptos, Inc. ("Aptos"), the third-party company, contracted to operate our e-commerce platform informed us on February 7, 2017 that an intrusion occurred on their systems.

The intruder or intruders placed malware on Aptos' servers, and by doing so gained access to our customers' payment card data. To date Aptos' investigation indicates that the intrusion began in approximately February 2016 and ended in December 2016.

The attackers gained access to customer information, including payment card numbers, as customers made transactions on the platform provider's systems, and also had access to historical payment card data.

Our records indicate your credit card(s) ending in [XXXX] was impacted during this timeframe.

You may wonder why you are hearing about the breach now. Aptos did not discover the breach until November 2016. In addition, law enforcement is investigating, and asked that notification to customers be delayed to allow the investigation to move forward.

What Are We Doing?

Aptos has worked with a leading cybersecurity firm to remove the malware from its systems and is actively monitoring the platform to safeguard personal information.

Aptos is also working with law enforcement authorities in their investigation. The credit card companies and issuing banks have been contacted for the purposes of identifying unauthorized charges.

What You Can Do?

To protect yourself from the possibility of identity theft, we recommend you immediately contact your credit or debit card company and inform them that your card information may have been compromised, so that they can issue you a replacement card.

Review your banking and card statements and report any suspicious activity to the relevant financial institutions. Furthermore, the reference guide, <https://www.identitytheft.gov/> provides recommendations by the U.S. Federal Trade Commission on the protection of personal information; we have included a copy of the guide for your convenience.

We hope this information is useful to you, but if you have further questions, please contact our Customer Support team at (877) 527-2460. We regret any inconvenience this may cause you.

Sincerely yours,

Michael Smith
Chief Executive Officer & Chief Financial Officer

Steps You Can Take to Further Protect Your Information

We encourage customers to remain vigilant, review payment card account statements, monitor credit reports, and consider these additional steps.

Review Your Account Statements

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.

You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission ("FTC").

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Credit Reports

To order a free copy of your credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the FTC website at <http://www.ftc.gov/bcp/edu/resources/forms/requestformfinal.pdf> and mail it to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

The three national credit bureaus provide free annual credit reports only through the website, toll-free number, or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be internal review and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

Consulting the FTC

If you detect any incident of fraud, promptly report the incident to your local law enforcement authority, your state Attorney General and the FTC. If you believe your account has been compromised, the FTC recommends that you take these additional steps:

Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. When you dispute new unauthorized accounts, use the FTC's ID Theft Affidavit, which is available at <http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf>

File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the crime.

You can contact the FTC to learn more about how to protect yourself:

Federal Trade Commission Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

Police Report

If you find suspicious activity on your credit reports or account statements, or have reason to believe that your personal information is being misused, contact your local law enforcement authorities immediately and file a police report. You have the right to request a copy of the police report and should retain it for further use, as creditors may request such documentation to waive your potential liabilities in connection with fraudulent activity.

Fraud Alerts

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert notifies you of an attempt by an unauthorized person to open a new credit account in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a free fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus. You can also place a fraud alert on your credit report online at the websites listed below.

Equifax
Phone: 800-525-6285
P.O. Box 105069
Atlanta, GA 30348-5069
http://www.equifax.com/answers/set-fraud-alerts/en_cp

Experian
Phone: 888-397-3742
P.O. Box 9532
Allen, TX 75013
https://www.experian.com/fraud/center_rd.html

TransUnion
Phone: 800-680-7289
P.O. Box 6790
Fullerton, CA 92634-6790
<https://fraud.transunion.com>

Security Freeze

Some state laws allow you to place a security freeze on your credit reports. A security freeze would prohibit a credit reporting agency from releasing any information from your credit report without your written permission. You should be aware, however, that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services. The specific costs and procedures for placing a security freeze vary by state, but this Reference Guide provides general information. You can find additional information at the websites of any of the three credit reporting agencies listed below.

If you believe that you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, the agency will not charge you to place, lift or remove a security freeze on your credit reports. In all other cases, a credit reporting agency may charge you a fee, which generally ranges from \$5.00 to \$20.00 per action.

Requirements vary by state, but generally you may place a security freeze on your credit report by sending a written request to each of the three credit reporting agencies noted below, which may require the following information to verify your identity:

- (1) Full name (including middle initial as well as Jr., Sr., II, III, etc.);
- (2) Social Security Number;
- (3) Date of birth;
- (4) Addresses for the prior five years;
- (5) Proof of current address; and
- (6) A legible copy of a government issued identification card.

You also may provide a copy of any relevant police report, investigative report, or complaint to a law enforcement agency concerning the incident.

Equifax
Phone: 800-525-6285
P.O. Box 105788
Atlanta, Georgia 30348
http://www.equifax.com/answers/help/security-freeze/en_cp

Experian
Phone: 888-397-3742
Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze

TransUnion
Phone: 888-909-8872
P.O. Box 6790
Fullerton, CA 92634-6790
<https://freeze.transunion.com>

Additional Free Resources on Identity Theft

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

A copy of Taking Charge: What to Do If Your Identity Is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, is available at www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.shtm

For North Carolina Residents

You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (toll-free in North Carolina)
919-716-6400
www.ncdoj.com

For Maryland Residents

You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
888-743-0023 (toll-free in Maryland)
410-576-6300
<http://www.oag.state.md.us>

For Massachusetts Residents

The credit bureaus may charge you a fee of up to \$5.00 to place a security freeze on your account, and may require that you provide proper identification prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you provide the credit bureaus with a valid police report.

You have the right to obtain a police report regarding the breach.