<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (Re: Notice of Data [HEADER])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We are writing to notify you of a data security incident relating to your purchase through our online store that may have involved your payment card information. At TytoCare, Inc. and TytoCare, Ltd., ("TytoCare"), we take the privacy and security of your information very seriously. We are writing to both inform you of the incident, and to advise you about steps you can take to protect your information.

What Happened? On or about September 1, 2023, we were alerted of unusual activity involving TytoCare's online store. Upon becoming aware of the activity, we took immediate steps to secure the system. We also engaged a nationally-recognized digital forensics firm to conduct an independent investigation into what happened and determine whether any customer payment card information had been accessed or acquired without authorization.

What Information was Involved? After an extensive forensics investigation, we determined on October 3, 2023 that this incident may have involved payment card information of customers who purchased products through our online stores between January 26, 2021 and February 10, 2023. We then worked diligently to identify all potentially affected customers. The information that may have been involved includes names, payment card numbers, expiration dates, and security codes.

Please note this issue did not involve any systems that transmit health information.

What Are We Doing? As soon as we discovered the incident, we took the steps discussed above. In addition, this incident has been reported to the payment card brands in an effort to protect your information and prevent fraudulent activity. Since the time of the incident, our online store has been upgraded and incorporates additional measures to enhance the security of our ecommerce platform.

Additionally, TytoCare is providing you with information about steps that you can take to help protect your personal information.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

For More Information: If you have any questions, we encourage you to contact our dedicated call center at <<Number>>, between 9:00 a.m. and 6:30 p.m. Eastern Time, excluding U.S. holidays.

We take our customers' trust in TytoCare and this matter very seriously. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

Ofer Tzadik, COO
Tyto Care, Inc. & Tyto Care, Ltd.
264 West 40th St.
16th Floor
New York, NY 10018

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: 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).

Request a Copy of Your Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Place a Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at https://www.annualcreditreport.com.

Put a Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission (FTC)
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.