



November 12, 2020

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

## Notice of Data Breach

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

T3 Micro Inc. ("T3 Micro") writes to inform you of a recent event affecting the systems of one of T3 Micro's service providers that may have resulted in unauthorized access to your personal information. We take this incident very seriously and as a precaution, we are providing you with information about the incident, our service provider's response, and steps you may wish to take to better protect against the possibility of identity theft and fraud.

### What Happened?

On October 28, 2020, T3 Micro was notified by one of our third-party service providers, which manages portions of our information technology infrastructure, that it had discovered a potential security issue with its network. The service provider informed T3 Micro that the event occurred on September 4 and 5, 2020. Upon learning of the issue the service provider took immediate action to remediate the issue. The service provider also notified federal law enforcement.

The investigation revealed that an unauthorized individual obtained the credentials of an employee of the service provider and used those credentials to access the service provider's network, including a limited number of resources and applications used to support T3 Micro's website. The attacker changed certain files to redirect customers to a third-party website with a fraudulent checkout page that mirrored T3 Micro's. Not all customers were redirected to the fraudulent site during this period, but for those that were, the attacker may have been able to capture payment information during the checkout process.

### What Information Was Involved?

The information that was vulnerable may have included name, address, debit or credit card number, expiration date, and Card Verification Value (CVV) number.

### What We Are Doing.

Our service provider took immediate action to remediate the issue to stop the redirection to the fraudulent site. Additionally, we are working with our service provider to see that steps are taken to reduce the risk of similar incidents occurring in the future. Steps our service provider has taken to date include enhancing its security and monitoring, hardening its systems, and reinforcing its employee cybersecurity and privacy training.

### What You Can Do.


We recommend you take steps to cancel any cards that may have been affected by the incident. You can also find out more about how to protect against potential identity theft and fraud in the enclosed Steps You Can Take to Better Protect Your Information.

**For More Information.**

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call us at 1-866-376-8880, Monday through Friday from 8:00 a.m. to 4:00 p.m. PST. You may also write to T3 Micro at 228 Main Street, STE 12, Attn. Legal Dept., Venice, CA 90291.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

A handwritten signature in black ink, appearing to read "Paul Pofcher", with a stylized flourish at the end.

Paul Pofcher  
President  
T3 Micro

## STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228.

Additionally, you can order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to:

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

You may also contact the three nationwide credit reporting agencies directly to request a free copy of your credit report.

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

You have the ability to place a "security freeze", also known as a credit freeze, on your credit report free of charge. A security freeze 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**

PO Box 9554

Allen, TX 75013

1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

### **TransUnion**

P.O. Box 2000

Chester, PA 19016

1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

### **Equifax**

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://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, 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. Social Security Card, pay stub, or W2;
8. 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.

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**

P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com/fraud-victim  
-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-  
report-services](http://www.equifax.com/personal/credit-report-services)

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at [www.irs.gov/Individuals/Identity-Protection](http://www.irs.gov/Individuals/Identity-Protection) for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit [www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft) for more information.

**Federal Trade Commission and State Attorneys General Offices.** If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/), 1-877-IDTHEFT (438-4338).

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), 1-877-566-7226.

**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 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 violator. 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](http://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.

**Reporting of identity theft and obtaining a police report.**

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.