[DIODE DYNAMICS LETTERHEAD]

[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]
[DATE]

NOTICE OF DATA BREACH

Dear [INDIVIDUAL NAME]:

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information.

WHAT HAPPENED?

On or about September 26, 2020, bad actors injected a piece of malicious code into Diode Dynamics' databases, exploiting a vulnerability in the e-commerce platform used by Diode Dynamics to process credit card transactions. Our investigation indicates that the malicious code was capable of reading information that customers entered in data fields in the payment processing area of our website and transmitting that information to the bad actors. The sophisticated nature of the malicious code allowed it to operate undetected, even though Diode Dynamics regularly runs security scans of its software using two separate, sophisticated scanning tools. Once Diode Dynamics became aware of this exploit, it moved quickly to have it removed from its website software, and the malicious code was completely removed on October 27, 2021. This vulnerability did not affect purchases made by our customers using PayPal.

WHAT INFORMATION WAS INVOLVED?

The data accessed may have included personal information such as names, addresses, phone numbers, and credit card numbers, expiration dates and security (CVV) codes.

WHAT WE ARE DOING

Diode Dynamics values your privacy and deeply regrets that this incident occurred. Diode Dynamics is conducting a thorough review of the potentially affected systems and will notify you if there are any further significant developments. Diode Dynamics has implemented additional security measures designed to prevent a recurrence of such an attack and to protect the privacy of Diode Dynamics's valued customers.

Diode Dynamics also is working closely with major credit card suppliers and law enforcement to ensure the incident is properly addressed.

WHAT YOU CAN DO

Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information[, and how to receive free [credit monitoring/identity theft protection] services for one year].

FOR MORE INFORMATION

For further information and assistance, please contact Diode Dynamics at **(314) 205-3033** between 10:00 a.m.- 5:00 p.m. CST daily or visit **http://www.diodedynamics.com**.

Sincerely,

Paul J. McCain
C.E.O., Diode Dynamics

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, including your state attorney general and the Federal Trade Commission (FTC). You can visit the FTC's website at https://www.consumer.ftc.gov/ topics/ privacy-identity-online-security for additional information. You may have the right to file and obtain a police report from your local law enforcement agency.

To file a complaint with the FTC, go to IdentityTheft.gov 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.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing a Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Currently, the three major credit reporting agencies are offering free online credit reports on a weekly basis. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

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 90 days. 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 http://www.annualcreditreport.com.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

[STATE] residents may obtain information about steps you can take to prevent identity theft from the [STATE] Attorney General at [WEBSITE] or at:

[STATE] Attorney General's Office

[Consumer Protection Division]

[ADDRESS]

[CITY, STATE, ZIP]

[PHONE NUMBER]/[TOLL FREE NUMBER]

OTHER IMPORTANT INFORMATION

- **Security Freeze**

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. [There is no charge to request a security freeze or to remove a security freeze./There is a charge of [$] to request or remove a security freeze.]