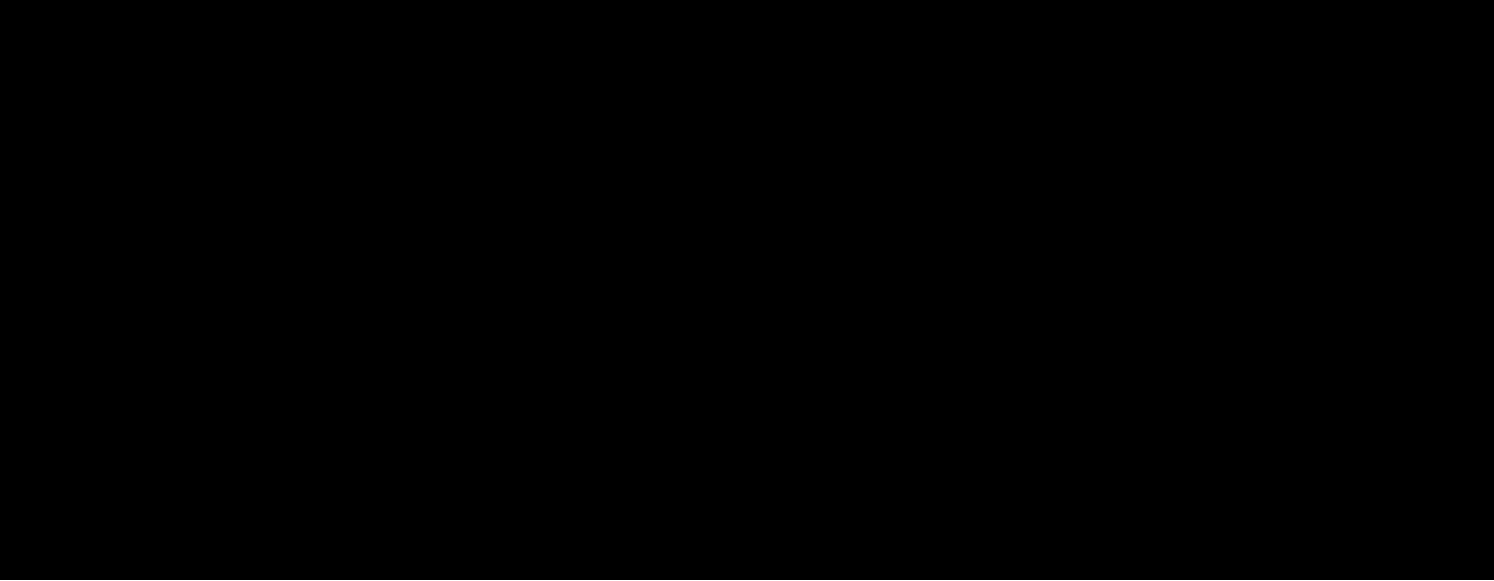




Without Prejudice

To whom it may concern

I would like to notify you of a data breach incident that occurred on our website www.ergopouch.com

Date Occured

Between 7.50 pm 18th April to 6.00pm on the 19th April 2022

What Happened?

23,000 bot attacks on our server gained a brute force entry and inserted a malware script that has been used to scrape personal data from consumers purchasing products on our website www.ergopouch.com

How many Maryland Citizens were affected?

Only 2 customers were affected

Type of information that has been compromised?

Credit Card Numbers

CVV

Name

Email address

Delivery address

What steps have been taken to secure the site and protect information?

1. We confirmed the site was exploited by using the Sucuri Site Check service and reported this to Digital Outlook (DO)
2. Once DO had removed the malicious JavaScript we then cleared the CloudFlare cache so that it rebuilt the cache from the new code
3. We also blocked access to the admin manage area from the 4 specific IPs AND installed a CAPTCHA when end users attempt to access this URL
4. We also blocked on the server itself ANY access from the 4 specific IP addresses just

in case the access was DIRECT to the server (bypassing the CloudFlare steps we took in #3

EDM Notification to affected customers is attached

Kind regards,

--

Jodi Lancaster

General Manager

ergoPouch



+61 0429 58 55 73

www.ergopouch.com.au

13 Corporate Drive, Heatherton, VIC 3202 Australia





Notification of privacy incident

We value your business and respect the privacy of your information which is why, as a precautionary measure, we are writing to advise you about a recent privacy breach that involved a possible disclosure of your personal information, including credit card information. This letter will explain what happened, how we have responded and what it means for you.

What happened?

We have recently been notified of a breach of our www.ergopouch.com website, sometime between 7:50pm on the 11th of April and 6pm on the 19th of April ASES. The breach involved a malware virus, which has the potential to collect data you may have entered via your web browser on our www.ergopouch.com website and resulted in the possible disclosure of your personal data.

What information was affected?

Based on our investigation, we understand that your personal information that has been affected by this incident includes:

- Name
- Address
- Email address
- Credit card details including expiry date and CVV
- Contact phone number
- Postal address

What have we done in response to the breach?

Once we were made aware of the issue, we worked with our IT service providers to immediately remove the offending malware virus from our servers. We have also conducted a full review with our IT service providers and have implemented new security measures and enhancements to increase the level of security across all our systems and platforms. Additionally, we have also implemented several recommendations to minimize any further impacts or potential attacks on our site and safeguard our customers personal information and privacy.

What does this mean for you?

- You value your privacy and deeply regret the incident has occurred. You should carefully review the information that was affected by this incident and think about whether this could result in you experiencing any harm. Some of the steps you may consider taking to protect yourself include:
- Be aware of emails and telephone calls from people requesting your personal details, (especially things like your date of birth, residential address, email address, username or passwords which are often used to verify your identity).
 - Change your account password.
 - Alert your financial institutions so that they can implement additional monitoring and security measures to protect your account.
 - Closely monitor your financial statements for unauthorized transactions. If you identify a transaction you didn't make, report it immediately to your financial institution.
 - Change your online bank account password, banking PIN and enable multi-factor authentication if possible.

More information and making a complaint

If you have any concerns about what has happened or would like further information, please contact:

ergoPouch Customer Support
cs@ergopouch.com

If you are not satisfied with how we have handled this incident or you have experienced some harm as a result, you can make a privacy complaint. You can do so by contacting us by email at cs@ergopouch.com. It would be helpful if you could explain how you have been affected by the breach and what you would like us to do to resolve your complaint.

Yours sincerely,

Jodi Lancaster
General Manager
ergoPouch

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.

To file a complaint with the FTC, go to www.consumer.ftc.gov/identity-theft or call 1-877-43-THIEF (877-438-4238). 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.

Copy of 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 www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 100281, Atlanta, GA 30341.

You can print a copy of the request form at www.annualcreditreport.com/annualcreditreport.pdf. Or 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

(800) 685-1111
www.equifax.com
P.O. Box 742041
Atlanta, GA 30314

Experian

(800) 391-3742
www.experian.com
535 Ardon Blvd., Suite 100
Costa Mesa, CA 92626

TransUnion

(800) 916-8800
www.transunion.com
P.O. Box 6780
Ft. Worth, TX 76163

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 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 www.annualcreditreport.com.

Security Freeze

In order to ensure you have the right to put a security freeze on your credit file, this will prevent any credit from being issued 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 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.identity theft.gov or call 1-877-ID-THEFT (877-438-4238). A guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at www.identitytheft.gov/fakeid-look-or-shield.