



Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

## Re: Notice of Data Breach

Dear <<Name>>:

I am writing to make you aware of a recent data privacy event that may affect the security of certain payment card information. It's unfortunate that these situations happen so frequently today and we take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so. We are also taking additional steps to continue to protect our customers' data in the future.

**What Happened?** Zero Water ("Zero") recently received a report of unusual card activity from its credit card processor. Upon receiving these reports, Zero worked with a third-party forensic investigator, and our website provider to identify the source of the activity and to confirm the security of our network. The investigation determined that a vulnerability existed on our website that would permit access to certain customer payment card information if the vulnerability was exploited. On or around May 24, 2019 we determined that there was evidence that the vulnerability was exploited and that there was unauthorized access to obfuscated payment card information used at [www.zerowater.com](http://www.zerowater.com).

**What Information Was Involved?** The investigation determined that the information potentially accessed as a result of this event could include some or all of the following: your name, <<Data Elements>> credit or debit card number, credit card type, expiration date and CVV for payment cards used at [www.zerowater.com](http://www.zerowater.com). Please note that the credit card number was coded in such a way to hide the card number but some risk remains that the number was exposed. Your billing and shipping address, phone number, email address, and zerowater.com account password (if provided) may have also been impacted.

**What We Are Doing.** We take the security of our customers' information very seriously and we apologize for the inconvenience this incident has caused our customers. We have security measures in place to protect data in our care and we are working diligently to enhance these protections and ensure the ongoing security of the systems involved. We are also providing you with information about this event and about the steps you can take to better protect against issue of your personal information, should you feel it appropriate to do so.

**Changes We Have Made.** After undergoing an extensive independent security audit of our web site, additional security measures were put in place to further strengthen the security and protection of credit card data. Significant enhancements were also implemented to optimize the security of our technology for future transactions.

**What You Can Do.** We encourage you to monitor your credit card statements closely and report any suspected fraud to your issuing bank. You can also review the enclosed "Steps You Can Take to Protect Your Information" for additional information about how you can protect your identity.

***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 877-848-4120, Monday through Friday, between 9 am to 9 pm Eastern Time. You can also write to us at 7 Neshaminy Interplex, Suite 116, Trevose, PA 19053.

Sincerely,

Doug Kellam  
CEO

## Steps You Can Take to Protect Against Identity Theft and Fraud

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. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which 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)

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)

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, [www.ncdoj.gov](http://www.ncdoj.gov).

**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us).

**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.

**For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 37 Rhode Island residents impacted by this incident.