PUBLIC ALLIES
Everyone Leads

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: <<Variable Header>>

Dear <<Name 1>>:

Public Allies, Inc. ("Public Allies"), is writing to inform you of an event that may impact the security of some of your information. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On or about December 17, 2020, Public Allies learned that a database of employee or applicant usernames and password information had been found on the internet as part of a much larger data leak claimed to be the result of data stolen from a number of organizations. We immediately undertook an investigation to determine the nature and scope of the issue, including whether this information had been leaked in relation to any compromise of our internal computer systems. Our investigation found no indication of unauthorized access to our internal computer systems, but nonetheless we felt it was necessary to review the impacted database found on the internet to determine the impacted individuals. We then conducted a thorough manual review of our records to determine the identities and contact information for potentially impacted individuals. We recently completed our review and are providing notice to impacted individuals.

What Information Was Involved? We determined the following types of your information were impacted: name and your organization or profile username and password.

What We Are Doing. We take this incident and the security of your personal information seriously. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to 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. We also recommend changing your password.

For More Information. Should you have additional questions, please call our dedicated hotline at 855-535-1846 Monday through Friday (excluding U.S. holidays), during the hours of 8:00 a.m. to 8:00 p.m., Central Time. You may also write to Public Allies, at 735 N. Water St., Suite 550, Milwaukee, WI 53202. We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Stephen Bauer
Chief of Staff
Public Allies, Inc.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

From: mail@msgbsvc.com on behalf of Public Allies <no-reply@publicallies.org>
Sent: Wednesday, June 2, 2021 6:14 PM
To: DL-Data Breach Team
Subject: HTML Sample -- Notification of Data Incident

To whom it may concern,

Public Allies is writing to inform you of an event that may impact the security of some of your information. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and steps you should take, should you feel it is necessary to do so.

If you have any questions on the following, please contact our dedicated call center at 855-535-1846 Monday through Friday 9:00 am to 9:00 pm Eastern Time.

What Happened & Steps Taken

On or about December 17, 2020, Public Allies learned that a database of employee or applicant usernames and password information had been found on the internet as part of a much larger data leak claimed to be the result of data stolen from a number of organizations. We immediately undertook an investigation to determine the nature and scope of the issue, including whether this information had been leaked in relation to any compromise of our internal computer systems. Our investigation found no indication of unauthorized access to our internal computer systems, but nonetheless we felt it was necessary to review the impacted database found on the internet to determine the impacted individuals. We then conducted a thorough manual review of our records to determine the identities and contact information for potentially impacted individuals.

Next Steps

As a precaution we provided notice to all individuals who are potentially impacted by this incident. We encourage you to change the password on your email account - as your email served as your username and the password you created may have been similar to passwords you used in other accounts you maintain

Thank you,

Public Allies