

<<Date>>

<<First >> <<Last >>  
<<Address1>>  
<<City>>, <<State>> <<Zip>>

Subject: Notice of Data Security Incident

Dear <<First>> <<Last>>:

We have been made aware of a recent data security incident that occurred at DonorPerfect, a fundraising software we have used for over 15 years. Unfortunately, the data security incident may have affected your personal information.

DonorPerfect determined that certain files may have been acquired by an unauthorized actor between November 25, 2023 and December 8, 2023. The information in these files may have included your name and financial account information (via a check image). Our legal counsel has advised us this data breach is considered low risk since check account information is readily available by the public.

DonorPerfect has arranged to provide credit monitoring services through IDX, a leader in consumer identity protection. These services include 12 months of credit monitoring, identity protection through CyberScan, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. If you are interested in taking advantage of these services, please connect with the DonorPerfect team at [creditmonitoring@donorperfect.com](mailto:creditmonitoring@donorperfect.com). Further information about how to protect your personal information is provided on the following page.

Protecting your personal donor information is of the utmost importance to us. We are committed to maintaining your trust. If you have any questions, please call Deanna Tavares, Development Officer/ Operations at 781-610-1409 or email at [dtavares@nvna.org](mailto:dtavares@nvna.org).

Sincerely,

Michael R. Rogers  
Senior Vice President of Advancement and External Relations

**Review Your Account Statements for 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 (FTC).

**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 <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

**Equifax**  
P.O. Box 740241  
Atlanta, GA 30374  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

**Experian**  
P.O. Box 4500  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-800-916-8800  
[www.transunion.com](http://www.transunion.com)

**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 one year. 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>.

**Security Freeze:** You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened 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:** You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

**Federal Trade Commission**  
600 Pennsylvania Ave, NW  
Washington, DC 20580  
[consumer.ftc.gov](http://consumer.ftc.gov), and  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

**Massachusetts Attorney General**  
1 Ashburn Place, 20<sup>th</sup> floor  
Boston, MA 02108  
<https://www.mass.gov/orgs/office-of-the-attorney-general>  
1-617-727-2200

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.