

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

AMANDA RUGGIERI
ARuggieri@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

JONATHAN QUAGLIARELLO
JQuagliarello@c-wlaw.com

April 1, 2024

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Notice of Data Security Incident

To Whom It May Concern:

We serve as counsel for The Elephant Sanctuary in Tennessee (“The Elephant Sanctuary”) located at 804 Darbytown Road, Hohenwald, TN 38462 and provide this notification of a recent data security incident. By providing this notice, The Elephant Sanctuary does not waive any rights or defenses under Maryland law, including the data breach notification statute.

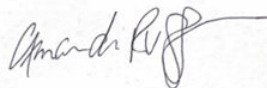
In January 2024, The Elephant Sanctuary was made aware of a data security incident that occurred at DonorPerfect, a third-party vendor whose fundraising software The Elephant Sanctuary uses. On February 5, 2024, DonorPerfect provided formal notification of the incident and confirmed that The Elephant Sanctuary’s database within DonorPerfect’s hosted file storage was likely accessed by an unauthorized actor and that the stored files associated with donor records likely were downloaded by an unauthorized actor. DonorPerfect also provided list of the files that were likely subject to unauthorized download.

After receiving this notification and list of files, The Elephant Sanctuary conducted a review of the files to determine whether any personal information relating to donors was contained therein. On March 25, 2024, The Elephant Sanctuary confirmed that five (5) Maryland residents were potentially affected. The impacted data includes donor names and bank account information.

The Elephant Sanctuary provided written notice of this incident on April 1, 2024, to the potentially impacted Maryland residents via First Class U.S. Mail. The notice letters include instructions for potentially impacted individuals to access complimentary credit monitoring and identity protection services. A copy of the notice letter is attached hereto as *Exhibit A*.

Please contact me should you have any questions.

Very truly yours,



Amanda Ruggieri, Esq.
Cipriani & Werner, P.C.

EXHIBIT A



804 Darbytown Road
Hohenwald, TN 38462

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

<<Date>>

RE: Notice of Data [Breach/Security Incident]

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

The Elephant Sanctuary in Tennessee (“The Elephant Sanctuary”) has been made aware of a data security incident that occurred at DonorPerfect, a fundraising software we use, that may have affected some of your personal information described below. While we have no evidence that any information has been misused, in an abundance of caution, we are providing you information about the incident and steps you can take to help protect your personal information.

What Happened. DonorPerfect notified The Elephant Sanctuary that it had discovered suspicious activity related to a subsection of its hosted file storage. DonorPerfect immediately took steps to identify, contain, and remediate the issue, including locking down its systems and strengthening numerous security protocols. DonorPerfect’s investigation determined that certain files may have been acquired without authorization between November 25, 2023 and December 8, 2023. After receiving notice of this incident from DonorPerfect, we undertook a review of the impacted files to determine whether any contained personal information. Following a full and thorough review, a limited amount of personal information was identified as being contained within the potentially affected data.

What Information Was Involved. The information involved included your first and last name and your bank account information.

What We Are Doing. As soon as DonorPerfect discovered the incident, it took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. DonorPerfect also notified the Federal Bureau of Investigation and local law enforcement and will continue to cooperate with any investigations to hold the perpetrator accountable.

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. To take advantage of the services, please contact DonorPerfect at creditmonitoring@donorperfect.com.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary services offered to you through IDX by contacting DonorPerfect at creditmonitoring@donorperfect.com.

For More Information. Further information about steps you can take to help protect your personal information appears on the following page. If you have questions, please do not hesitate to contact us at (888) 229-9161 or write us at 804 Darbytown Road, Hohenwald, TN 38462.

Protecting your personal information is of the utmost importance to us, and we are committed to maintaining your trust. Thank you for your understanding and continued support.

Sincerely,

<<signature image>>

Janice Zeitlin, CEO

The Elephant Sanctuary in Tennessee

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring / Identity Protection

To enroll in the complimentary credit monitoring service detailed above, please contact DonorPerfect at creditmonitoring@donorperfect.com.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); 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:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

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 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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.