MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Jeffrey J. Boogay
Office: 267-930-4784
Fax: 267-930-4771
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

March 15, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Cherrydale Fundraising ("Cherrydale"), located at 707 N. Valley Forge Road, Lansdale, PA 19446, and are writing to notify your office of an incident that may affect the security of personal information relating to twenty (20) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Cherrydale does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about January 25, 2019, Cherrydale began investigating suspicious activity occurring on their online e-commerce website, www.cherrydale.com. Cherrydale immediately took down the website to protect the safety of its customers payment information. Cherrydale also began working with third-party forensic investigators to determine what happened and what information was affected as well as to implement additional procedures to further protect the security of customer debit and credit cards. Cherrydale identified and removed the malware at issue to prevent any further unauthorized access to customer debit or credit card information. Once Cherrydale confirmed the security of its website, with assistance of third-party experts, Cherrydale safely brought the website back up for customer use. Customers can safely and securely use their payment card at Cherrydale's website.

On February 4, 2019, the investigation determined that Cherrydale was the victim of a sophisticated cyber-attack that may have resulted in a compromise to some of its customers' credit and debit cards used to make purchases on its e-commerce website between October 28, 2018 and January 25, 2019. This may include customers who completed purchases on its e-commerce website and those who began transactions but did not complete the sale. Cherrydale took steps to confirm the identity of the customers whose personally

identifiable information was impacted. On or around February 4, 2018, Cherrydale confirmed the identities of the individuals who may have had information affected by this incident.

The information that could have been subject to unauthorized access includes name, address, credit card number, expiration date, and CVV.

Notice to New Hampshire Residents

On or about March 15, 2019, Cherrydale provided written notice of this incident to all affected individuals, which includes twenty (20) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Cherrydale moved quickly to investigate and respond to the incident, assess the security of Cherrydale systems, and notify potentially affected individuals. Cherrydale is also working to implement additional safeguards and training to its employees.

Additionally, Cherrydale is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Cherrydale is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Cherrydale is also providing written notice of this incident to other state regulators, as necessary, and to the three major consumer reporting agencies.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB/ara

EXHIBIT A

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 1>>:

Cherrydale Fundraising ("Cherrydale") is writing to inform you of a recent event that may impact the privacy of some of your payment information. We wanted to provide you with information about the event, our response, and steps you may wish to take to better protect against the possibility of identity theft and fraud.

What Happened? On or about January 25, 2019, Cherrydale began investigating suspicious activity occurring on our online e-commerce website, www.cherrydale.com. Cherrydale immediately took down the website to protect the safety of our customers' payment information. Cherrydale also began working with third-party forensic investigators to determine what happened and what information was affected as well as to implement additional procedures to further protect the security of customer debit and credit cards. We identified and removed the malware at issue to prevent any further unauthorized access to customer debit or credit card information. Once we confirmed the security of our website, with assistance of third-party experts, we safely brought the website back up for customer use. You can safely and securely use your payment card at our website.

On February 4, 2019, the investigation determined that Cherrydale was the victim of a sophisticated cyberattack that may have resulted in a compromise to some of our customers' credit and debit cards used to make purchases on our e-commerce website between October 28, 2018 and January 25, 2019. This may include customers who completed purchases on our e-commerce website and those who began transactions but did not complete the sale. Cherrydale took steps to confirm the identity of the customers whose personally identifiable information was impacted. On or around February 4, 2018, we confirmed the identities of the individuals who may have had information affected by this incident.

What Information Was Involved? Through the third-party forensic investigation, we confirmed on February 4, 2018 that malware may have stolen credit or debit card data from some credit and debit cards used on our website, www.cherrydale.com, between October 28, 2018 and January 25, 2019. The information at risk as a result of the event includes the cardholder's name, address, credit card number, expiration date, and CVV.

What We Are Doing. We take this incident and the security of your information seriously. Upon learning of this incident, we immediately shut down the e-commerce website and eliminated the unauthorized access. 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 payment information. In addition to notifying potentially impacted individuals we also notified state regulators, as required.

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 Better Protect Your Information.*

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 our dedicated assistance line at 855-255-4842, Monday through Friday, from 9 am to 9 pm Eastern Time.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Ross Cherry, CEO

STEPS YOU CAN TAKE TO BETTER 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. 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 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	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

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	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

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, 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.

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.

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, 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, 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 sixty-three (63) Rhode Island residents impacted by this incident.