MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

James Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

October 18, 2018

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 Renaissance Philanthropic Solutions Group ("RenPSG"), 8910 Purdue Rd, Suite 500, Indianapolis, IN, 46268, and are writing to notify you of a recent incident that may affect the security of the personal information of one hundred and fifty-eight (158) New Hampshire residents. RenPSG's response to this incident is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, RenPSG does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data incident notification statute, or personal jurisdiction.

Nature of the Data Security Incident

On June 13, 2018 RenPSG became aware of suspicious activity relating to certain employee email accounts hosted by a third-party service provider, possibly related to a malicious phishing email received by employees. They immediately launched an investigation with the assistance of a leading outside computer forensics expert to determine what may have happened and what information may have been affected. During the investigation, RenPSG determined certain employee email accounts were logged into by an unauthorized actor(s) between June 5, 2018 and June 13, 2018. The compromise was limited to the email accounts hosted by the third-party service provider. No RenPSG systems were subject to unauthorized access.

Because the investigation was unable to determine which email messages may have been seen or taken by the unauthorized individual, RenPSG engaged a forensic review team to review the email account contents to identify all individuals for whom personally identifiable information ("PII") was contained within the impacted email accounts. The large volume and variety of documents in need of review required a combination of automated forensic tools and manual document review to check this data for the presence of PII. Once the impacted individuals were identified, RenPSG then engaged in an additional process of

researching and confirming address information for the affected population. This was a lengthy process that continued through September 27, 2018.

The types of PII relating to New Hampshire residents determined to be stored within the impacted email account were not identical for every potentially affected individual, and they included the following: name, Social Security number, financial account information, and taxpayer identification number.

Notice to New Hampshire Residents

On October 18, 2018, RenPSG began mailing written notice of this incident to potentially impacted individuals, including approximately one hundred and fifty-eight (158) New Hampshire residents. Such notice is being provided in substantially the same form as the letter attached here as ***Exhibit A.***

Other Steps Taken

RenPSG is offering affected individuals complimentary access to two years of free credit monitoring and identity restoration services through Experian. Additionally, RenPSG is providing potentially affected individuals with information on how to protect against identity theft and fraud, including information on how to contact the Federal Trade Commission, the state attorney general, and law enforcement to report any attempted or actual identity theft and fraud. In addition to providing notice of this incident to you, RenPSG will be providing notice to other state regulators.

RenPSG has taken several immediate steps to protect against similar incidents in the future. Upon learning of this incident, the email login credentials for all employee email accounts were quickly reset to prevent further unauthorized access, and they implemented mandatory company-wide password resets. RenPSG migrated its email service host to a different service provider, and added Multi-Factor Authentication for all devices that access RenPSG email and RenPSG network directories. RenPSG is currently reviewing its existing information security procedures and continuing to provide additional training and education for employees to prevent similar future incidents. They are also reviewing their existing information security procedures and implementing additional safeguards and software programs including Digital Guardian Data Loss Prevention, Cisco Umbrella, and additional anti-malware and virus programs to further secure the information on RenPSG's systems.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me at (267) 930-4798.

Very truly yours,

James E. Prendergast of
MULLEN COUGHLING LLC

JEP:plm

EXHIBIT A

Renaissance- Individual Notice Template

RenPSG
PHILANTHROPIC SOLUTIONS GROUP

[Name]
[Address]
[City, State Zip Code]

Re: Notice of Data Breach

Dear [Name]:

Renaissance Philanthropic Solutions Group ("RenPSG"), is writing to notify you of an incident that may affect the security of your personal information. We take this incident seriously. This letter provides details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On June 13, 2018 RenPSG became aware of suspicious activity relating to certain employee email accounts, possibly related to a malicious phishing email received by employees. We immediately launched an investigation with the assistance of a leading outside computer forensics expert company to determine what may have happened and what information may have been affected. During the investigation, we determined certain employee email accounts were logged into by an unauthorized individual(s) on several occasions between June 5, 2018 and June 13, 2018. Because we were unable to determine which email messages may have been seen or taken by the unauthorized individual, we reviewed the email account contents to identify what personal information was stored within it. This was a lengthy process, and on September 27, 2018, we confirmed the individuals impacted by this incident.

What Information Was Involved? Our investigation determined the following types of your personal information were stored within the impacted email account and may have been viewed by an unauthorized individual: name and [data elements].

What Are We Doing? Information privacy and security are among our highest priorities. RenPSG has strict security measures to protect the information in our possession. Upon learning of this incident, we quickly changed the log-in credentials for the impacted email accounts and implemented mandatory company-wide password resets. We are also providing training and educational material to our employees to prevent similar future incidents. Additionally, as part of our ongoing commitment to the security of personal information in our care, we are working to review our existing information security procedures and to implement additional safeguards to further secure the information on our systems.

What You Can Do. Although we are not aware of any actual or attempted misuse of your information, we arranged to have Experian protect your identity for two years at no cost to you as an added precaution. Please review the instructions contained in the attached "Steps You Can Take to Protect Your Information" to enroll in and receive these services. RenPSG will cover the cost of this service; however, you will need to enroll yourself in the credit monitoring service. In the coming weeks, you will be prompted to change your password when you access your Program for Charitable Giving account, as part of our continued efforts to increase information security protocols.

For More Information: We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 888-610-7657 (toll free), Monday through

Friday, 9:00 a.m. to 9:00 p.m. EST. You may also write to us at 8910 Purdue Rd, Suite 500, Indianapolis, IN, 46268.

We sincerely regret that this incident occurred. RenPSG remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

[Signature]

Sean Reddington
Chief Information Officer
Renaissance Philanthropic Solutions Group

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring **[Activation code: xxx]**

To help protect your identity, we are offering a **complimentary** two-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **1.9.19** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit** PROVIDE the **Activation Code**: **[Code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **[DB08891]** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

Monitor Your Accounts.
To further protect against possible identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity.

Credit Reports. 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.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. 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	1-800-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

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 19106	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

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. This notice has not been delayed by law enforcement. ***For Maryland residents***, the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov. ***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 North Carolina Residents:*** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at www.ncdoj.gov. *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); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General.