August 21, 2020

Via Email

Attorney General Gordon MacDonald
Office of the Attorney General
Security Breach Notification
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

To Whom It May Concern:

On behalf of The MacDowell Colony Inc. ("MacDowell"), and pursuant to N.H. Rev. Stat. Ann. §359-C:20, this letter provides notice of a computer data security incident. MacDowell is a non-profit organization that provides artist residencies of up two months to 300 creative individuals per year.

Blackbaud Security Incident

On July 16, 2020, Blackbaud, Inc., a software vendor used by MacDowell and many other non-for-profit organizations globally, informed us that it was the victim of a ransomware attack. According to Blackbaud, it thwarted the attackers' attempt to disrupt its operations, but the attackers acquired a subset of information contained in a backup file. Though Blackbaud initially indicated that no personal information was implicated in this attack, on July 20, 2020, it informed MacDowell that some employee personal information may have been acquired.

Blackbaud has said publically that it paid the attackers' ransom and received confirmation that the acquired data was deleted. According to Blackbaud, it worked with third-party forensic experts and the FBI and determined that the motivation behind this attack was to receive payment, not to monetize the acquired personal data. Additionally, Blackbaud says it has conducted dark-web searches, which it will continue to monitor, and has found no evidence that the acquired information has or will be disseminated beyond the attackers. Based on this, Blackbaud determined that the risk of harm stemming from this incident is low.

Nevertheless, MacDowell worked diligently to determine from Blackbaud the scope of the incident as it pertained to MacDowell supporters and employees and what, if anything, is needed to properly protect MacDowell's information.

Impact on MacDowell's Accounting Data

Blackbaud provides software and hosting for MacDowell's accounting and donor databases. The accounting database provides financial capabilities, such as hosting payroll information for employees. Employees' and former employees' information is hosted by Blackbaud and may have been acquired by the attacker. The employee information acquired may have included Social Security number, driver's license number, or other government ID number. Though Blackbaud typically stores this sensitive information in secure, encrypted fields, an oversight on Blackbaud's part left certain fields that may contain these types of data unencrypted. MacDowell only became aware of this issue after the incident. In order to protect MacDowell's employees, we have removed all data from these unencrypted fields until Blackbaud has confirmed that the fields are encrypted.

MacDowell began formally notifying these affected individuals, including the 89 who reside in your state, via letter on August 15, 2020. A sample of the letter is enclosed. As stated in the attached sample notice, MacDowell has engaged Experian to offer two years of free credit monitoring and identity theft protection services to individuals who may have had personal information acquired.

Impact on MacDowell's Supporter Data

The donor database Blackbaud hosts for MacDowell provides customer relationship management capabilities and does not contain any personal information as defined by N.H. Rev. Stat. Ann. §359-C:19. The donor database contains supporters' names, contact information, giving history, and sometimes dates of birth or other demographic information. In the interest of transparency and out of an abundance of caution, MacDowell is also informing supporters of the incident.

MacDowell takes this incident seriously and is committed to answering any questions your office may have about it. Please do not hesitate to contact me at (917)-740-1336.

Sincerely,

Andrew Zimmerman
Finance Director

August 14, 2020

[redacted]

NOTICE OF BLACKBAUD SECURITY INCIDENT

Dear [redacted]

I hope you are well. Blackbaud, Inc., a vendor that provides software and hosts MacDowell's accounting and donor databases, recently informed us of a security incident that may have exposed some of your personal information. I am writing today because we want you to know what happened, as well as the steps that MacDowell has taken and will take to protect your information. MacDowell takes its responsibility to protect its employees extremely seriously. The security of your personal information is very important to us, and we will continue working hard to protect it.

What Happened?

On July 16, 2020, Blackbaud informed MacDowell that it had been the victim of a ransomware attack. Blackbaud told us that the earliest date of unauthorized access was February 7, 2020 and that they discovered and stopped the attack in May.

Although Blackbaud was able to avoid a disruption to its system and services, the hackers did acquire a copy of some backup data, including limited types of information belonging to some of MacDowell's supporters and some of our former and current employees. Blackbaud informed us that, after paying the attackers' demands, they received confirmation of the deletion of this data. Blackbaud has worked with third-party forensic experts and law enforcement agents to determine that there is little risk of harm to anyone whose information was exposed.

To be clear, this incident involved only Blackbaud's systems and had no impact on MacDowell's network or servers.

What We Are Doing

Once Blackbaud informed us of this ransomware attack, MacDowell immediately began working with Blackbaud to determine the extent of the breach and actively investigating what data may have been compromised. I have had extensive conversation with Blackbaud about their plans to strengthen their security and will continue to press them on this issue. We are also working closely with lawyers who specialize in these types of cyber incidents.

As an extra precaution, we are offering a complimentary two-year membership of Experian's® IdentityWorks℠. Your identity monitoring services include: daily 3-Bureau credit monitoring; daily credit alerts; credit reports; customer and fraud resolution support; identity theft insurance; educational resources; and ExtendCare, which is fraud resolution support extending beyond the life of initial membership.

To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: 11/30/2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: [redacted]

Additional details regarding your IdentityWorks membership are enclosed. 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)-890-9332 by 11/30/2020. Be prepared to provide engagement number DB21902 as proof of eligibility for the identity restoration services by Experian.

What Information Was Involved?

The exposed information varies by person, but included names, contact information, dates of birth, and payroll information. Based on your employee record, we believe that the exposed information also included your See FN1 Below. Though Blackbaud typically stores this sensitive information in secure, encrypted fields, we learned from our discussions with them that, through an oversight on their part, some of this information was left unencrypted. We are working to ensure Blackbaud corrects this, and until they do, all sensitive information has been removed from unencrypted fields.

FN1

Social Security number, passport number, driver's license number, or other government ID number.

What You Can Do

Although Blackbaud, with the assistance of their outside experts and law enforcement, determined that they believe the data was deleted and not used or disseminated, we always recommend that you carefully review your financial accounts for fraudulent activity and report any transactions that you did not initiate. We recommend that you remain vigilant in doing so.

It is also good to be vigilant regarding so-called "spear phishing" attacks – deceptive emails that use information about you in order to trick you into clicking on malicious links or downloading malware to your computer.

Other Important Information

Included with this letter are some additional helpful tips, and some steps that you can take to protect yourself against future risks of fraud and identity theft.

For More Information

MacDowell takes our responsibility to protect your information extremely seriously. I sincerely regret any inconvenience or worry this has caused you. If you have any questions or would like additional support in finding helpful resources please email me at finance@macdowell.org or give us a call at 917.740.1336. I look forward to hearing from you.

Sincerely,

Andrew Zimmerman
Finance Director

Additional Resources

MacDowell takes your security seriously and we encourage you to do the same. The resources below can help.

- **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 **https://www.annualcreditreport.com**, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	**Experian**:	**TransUnion**:
equifax.com equifax.com/personal/credit-report-services P.O. Box 740241 Atlanta, GA 30374 866-349-5191	experian.com experian.com/help P.O. Box 2002 Allen, TX 75013 888-397-3742	transunion.com transunion.com/credit-help P.O. Box 1000 Chester, PA 19016 888-909-8872

- **You may place a fraud alert on your credit file**. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.
- **You also have the right to place a security freeze on your credit file** free of charge. 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.
- We also recommend that you remain vigilant by reviewing your credit reports and account statements 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 incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft.
- You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.
- You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

- **For Maine residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

Additional Information and Helpful Contacts

- You can learn more by contacting the FTC or your state's Attorney General to obtain information including about how to avoid identity theft, place a fraud alert, and place a security freeze on your credit report.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; 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 reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

***