

17468

Board of Directors
Nell Painter
Chair
Andrew M. Senchak
President
Thomas P. Putnam
Vice Chair
Peter Wirth
Treasurer
Robert M. Olmsted
Secretary

Philip Himberg
David Macy
Assistant Secretaries

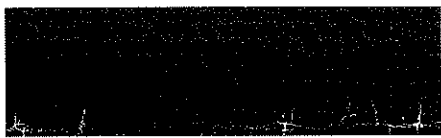
Susan Davenport Austin
David Baum
William B. Beekman
Eleanor Briggs
Ken Burns
Peter Cameron
Michael Chabon
Nicholas Dawidoff
Amelia Dunlop
Rosemarie Fiore
Edmée de M. Firth
Christine Fisher
Sarah Garland-Hoch
Gerald J. Gartner
Elizabeth F. Gaudreau
Adele Griffin
John A. Hargraves
Larry Harris
Darrell Harvey
Dan Hurlin
Lewis Hyde
Catherine Ingraham
Julia Jacqueline
Carol Krinsky
Michael Krinsky
Lisa Kron
Robert M. Larsen
Monica Lehner
Tania León
Anne Stark Locher
Robert MacNeil
Scott Manning
Terrance McKnight
Mollie Miller
Paul Moravec
Carlos Murillo
Julie Orringer
Olivia Parker
Ileana Perez Velazquez
Peter C. Read
Paul Reyes
Barbara Case Senchak
Vijay Seshadri
Josh Siegel
Arthur Simms
Alvin Singleton
Julia Solomonoff
Amy Davidson Sorkin
Charles F. Stone III
Robert Storr
Jamie Trowbridge
Mabel Wilson

Vartan Gregorian
Chair Emeritus

Philip Himberg
Executive Director

David Macy
Resident Director

August 14, 2020



NOTICE OF BLACKBAUD SECURITY INCIDENT

Dear [Redacted]

We are writing to tell you about a recent incident we learned about from a service provider that may have impacted 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, Inc., a vendor that provides software and hosts MacDowell's accounting and donor databases informed us that it had been the victim of a cybersecurity attack that began on February 7, 2020. Blackbaud discovered and stopped the attack in May 2020.

Blackbaud worked with third-party forensic experts and law enforcement and told us that they determined that there is little risk of harm to anyone whose information may have been impacted, but we wanted to alert you regardless.

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

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 steps you can take to protect yourself against the risks of fraud and identity theft.

For More Information

We take our responsibility to protect your information extremely seriously. We sincerely regret any inconvenience this has caused you. If you have any questions, or would like additional support in finding helpful resources please email us at finance@macdowell.org or give us a call at 917.740.1336.

Sincerely,



Andrew Zimmerman
Finance Director

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.

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.
