

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

February 16, 2022

Re: Vital Voices Global Partnership (“Vital Voices”) Security Incident

To the Maryland Attorney General’s Office:

We are contacting you on behalf of our client, Vital Voices, about a data security incident that involved the personal identifying information of approximately 6 residents of Maryland. Vital Voices is a global nonprofit that ensures, among other things, that victims and survivors of gender-based violence and harmful practices around the world have better access to services, protection, and the justice they deserve. The affected Maryland residents will be notified of this data breach on or about February 16, 2022, substantially in the same form as the letter attached here in **Exhibit A**. Please note that in submitting this notice, Vital Voices does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

What Happened

On August 3, 2021, Vital Voices discovered suspicious activity in an employee’s email account. Vital Voices worked with its IT support team and later retained an attorney specializing in cybercrime to lead its investigation and response, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The FBI was also contacted. On December 16, 2021 the investigation determined that an unauthorized actor accessed two email accounts between June 27 and August 26, 2021. The threat actors induced two donors into wiring funds to fraudulent bank accounts. However, the forensic specialists were able to confirm that the email environment was secured on August 26, 2021. Vital Voices thereafter conducted an in-depth review process to analyze the contents of the emails that were accessed to determine what, if any, sensitive information was contained within them.

On December 16, 2021, Vital Voices determined that the compromised emails contained personal identifying information of certain individuals. Vital Voices then undertook the process of determining the residence and address of potentially impacted individuals. Given the global nature of Vital Voices’ outreach and mission (including resettling survivors of gender-based violence), identifying and subsequently validating all potential addresses was a difficult, time-consuming process. Ultimately, Vital Voices determined that 6 Maryland residents had the following information impacted: full name, date of birth, address, Social Security number, other government-issued ID number, personal banking information (such as financial institution name, account number, and routing number), and information related to the provision of disability benefits. There is no evidence at this time of any fraud or misuse of the data involved.

Vital Voices also engaged a third party who put impacted individual contact information into a consistent format and validated relevant contact information for notification. Vital Voices believed this was necessary to ensure appropriate precautions and that proper next steps were taken.

Steps to Protect Your State Residents

Vital Voices is providing Maryland residents identity theft protection services through CyberScout, a well-known data breach and recovery services expert that specializes in consumer support. CyberScout identity theft protection services include 12 months of credit and Dark Web monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. Vital Voices is also providing all individuals with information on how to place a fraud alert and security freeze on one’s credit file, 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, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Lastly, Vital Voices is also notifying regulators as required.

To prevent similar events from occurring in the future, Vital Voices took significant steps to enhance security safeguards for information in its care. These measures included changing all user account passwords, enforcing multi-factor authentication and implementing malware scanners for attachments, notifications of email logins from new locations, external sender warnings, and a password management system.

Contact Information

If you have any further questions regarding this incident, please do not hesitate to contact me either by telephone at (214) 969-2713, or by email at mreed@akingump.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Michelle A. Reed". The signature is fluid and cursive, with the first name "Michelle" being more prominent than the last name "Reed".

Michelle A. Reed

EXHIBIT A

Vital Voices Global Partnership, Inc.
P.O. Box 3923
Syracuse, NY 13220



February 16, 2022

NOTICE OF DATA BREACH

We are writing to let you know about a data security incident that may have involved your personal information. Vital Voices Global Partnership ("Vital Voices") takes seriously our commitment to protecting your personal information. Although we have no evidence at this time that your information has been misused for identity theft or fraud, we are contacting you to explain the circumstances of this data security incident, and to provide information about the service we will provide to help you protect yourself.

What Happened?

As you may know, cybercriminals have increasingly targeted nonprofits as victims for their illegal activities. On August 3, 2021, we discovered suspicious activity in an employee's email account. We worked with our IT support team and later retained an attorney specializing in cybercrime to lead our investigation and response, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The FBI was also contacted. On December 16, 2021 our investigation determined that an unauthorized actor accessed two email accounts between June 27 and August 26, 2021, and personal information related to certain individuals, including you, was contained in those email accounts. Again, at this time, we have no evidence of any fraud or misuse of your personal information.

What Information Was Involved?

The personal information potentially impacted by this incident included your: name, date of birth, address, telephone number, email address, social security number, passport number, other government-issued ID number, student identification number, personal banking information (such as financial institution name, account number, routing number, and password), credit/debit card number, alien registration number, clinical information, health insurance information, and photographic copies of your birth certificate, marriage certificate, work-related evaluation, facial photograph, and handwritten signature.

What We Are Doing.

We take the security of information in our care seriously. We engaged an attorney specializing in cybercrime who retained third-party forensic specialists to aid in our investigation and to determine the scope of information impacted. We immediately took steps to identify and remediate the cause of the incident, including strengthening preexisting account authentication procedures and confirming the security of all user accounts. Specifically, we began enforcing two-factor authentication and implemented malware scanners for attachments, notifications of

* Services marked with an "*" require an internet connection and e-mail account and will require enrollment by parent or guardian first. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

EXHIBIT A

email logins from new locations, external sender warnings, and a password management system. We are in the process of further enhancing our cloud-based security.

We are providing you with access to Single Bureau Credit Monitoring* services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout, a company specializing in fraud assistance and remediation services.

What You Can Do.

We encourage you to enroll in complimentary credit monitoring and identity protection services through Cyberscout. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

We also 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. Criminals prey upon an outpouring of generosity, particularly in times of crisis. Your security and trust is important to us.

For More Information.

In addition to enrolling in the complimentary identity protection and credit monitoring services described above, we encourage you to please review the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud*, which describes other steps you can take to help protect your personal information. These steps include recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also always recommend that you do not wire money to Vital Voices or other charitable organizations without verbally reconfirming financial instructions.

We understand you may have questions about this incident that are not addressed in this letter. Should you have additional questions, please contact the call center we set up to respond to this event at 1-800-405-6108 from 8:00 am to 8:00 pm Eastern time, Monday through Friday. We take the privacy and security of the information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Sara Vandepeute", with a long horizontal flourish extending to the right.

Sara Vandepeute
Vice President, Finance & Administration

* Services marked with an "*" require an internet connection and e-mail account and will require enrollment by parent or guardian first. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

EXHIBIT A

Steps You Can Take to Help Protect Against Identity Theft and Fraud.

Enroll in Credit Monitoring

To enroll in Credit Monitoring* services at no charge, please log on to <https://www.myidmanager.com> and follow the instructions provided. When prompted please provide the following unique code to receive services: kzhduak4epwa In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer’s 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 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); 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 credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

* Services marked with an “*” require an internet connection and e-mail account and will require enrollment by parent or guardian first. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

EXHIBIT A

Additional Information You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 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 California residents, this notification was not delayed by law enforcement. Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Kentucky residents, the Office of the Attorney General of Kentucky may be contacted at: 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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 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.

For Oregon residents, Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

For all US residents, Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft or www.ftc.gov/credit, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

* Services marked with an “*” require an internet connection and e-mail account and will require enrollment by parent or guardian first. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.