[MSI LETTERHEAD]

[Individual Name]
[Individual Address]

Notice of Data Breach

MSI United States ("MSI") takes the protection of your personal data very seriously. We write to inform you of an incident that took place with one of our vendors, DonorPerfect, that may have involved some of that information. Although we are unaware of any actual misuse of your information, we are providing notice to you and other potentially affected individuals to provide information about the incident, the personal data that may have been involved, the steps we have taken to ensure the security of our systems and data, and the resources available to you to protect yourself against any unauthorized use of your personal data. We have included our contact details below should you need any further information.

What Happened?

DonorPerfect is a third party fundraising software vendor of MSI. On January 12, 2024, we were notified that DonorPerfect experienced a security incident wherein an unauthorized actor accessed and downloaded certain files that MSI stores with DonorPerfect. You are receiving this notice because DonorPerfect's investigation has revealed that your personal information may have been affected.

Specifically, DonorPerfect discovered suspicious activity related to a subsection of its hosted file storage. DonorPerfect immediately took steps to identify, contain and remediate the issue, including locking down their systems and strengthening numerous security protocols. DonorPerfect's investigation determined that certain files may have been acquired without authorization between November 25, 2023 and December 8, 2023. We determined that your information was may have been affected on February 12, 2024.

What Information Was Involved?

You are receiving this notice because our review determined that DonorPerfect's security incident may have resulted in unauthorized access and acquisition of one or more files containing your name, address, account number, and/or credit card information (number, expiration, CVV). The fact that you are receiving this notice does not mean that all or more than one of the aforementioned files and information relating to your personal information were actually acquired.

What We Are Doing

We take your privacy seriously, and we endeavor to protect your personal data. To do so, we will continue to review, audit, and improve our security controls and processes. As noted above, as soon as DonorPerfect discovered the incident, they took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. They also notified the Federal Bureau of Investigation and local law enforcement and will continue to cooperate with them any investigations to hold the perpetrator accountable.

[MSI LETTERHEAD]

There is **no** indication that any of your information has been used to commit fraud or identity theft. However, as a precaution, DonorPerfect has arranged to provide credit monitoring services through IDX, a leader in consumer identity protection. These services include 12 months of credit monitoring, identity protection through CyberScan, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. To take advantage of the services, please contact DonorPerfect at creditmonitoring@donorperfect.com.

What You Can Do

Supplemental information is attached to this letter, including the Steps You Can Take to Protect Your Data as guidance on further protecting your personal data. We encourage you to remain vigilant for incidents of fraud and identity theft by carefully reviewing your payment card or personal account statements for unauthorized charges and monitoring free credit reports for fraudulent activity or errors resulting from the incident.

If you suspect an unauthorized charge has been placed on your account, we encourage you to report it to your payment card issuer. According to the payment card brands' policies, you are not responsible for unauthorized charges to your account if you report them in a timely manner.

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

For More Information

If you have additional questions, please contact Kate Greenberg at 718-810-2461, PO Box 35528 Washington, DC, 20033, or kate.greenberg@msichoices.org.

Sincerely,

Amanda Seller, President, MSI-US

[MSI LETTERHEAD]

STEPS YOU CAN TAKE TO PROTECT YOUR DATA

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 the Federal Trade Commission, local law enforcement, and/or the Attorney General's office in your state. You can obtain information from these sources, as well as the credit reporting agencies listed below, about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. You should obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information follows for the Federal Trade Commission, as well certain state Attorney General Offices that we are required to provide pursuant to state law.

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

For North Carolina residents: *North Carolina Office of the Attorney General*, 9001 Mail Service Center, Raleigh, NC 27699-9001, 877-566-7266, www.ncdoj.gov

For New York residents: *Office of the New York State Attorney General,* 1 Empire State Plaza, The Capitol, Albany NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, please contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If a creditor can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, please contact each of the credit reporting agencies at the addresses below:

[MSI LETTERHEAD]

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You will need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save time by lifting the freeze only at that particular credit bureau. Otherwise, you will need to make the request with all three credit bureaus.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- 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 have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.