[Month] [Day], 2021

RE: Notice of Data Security Incident

[FirstName] [LastName]

[Address1]

[Address2]

[City] [State] [Zip]

Dear [FirstName] [LastName],

Midwest Transplant Network (MTN) deeply values your efforts in support of our mission. I am writing to inform you about a data security incident caused by a malicious ransomware attack on February 11, 2021. Despite the incident, our staff made it possible for MTN to continue carrying out our lifesaving mission of organ, eye and tissue donation.

MTN’s information technology (IT) staff and retained IT security experts worked tirelessly to quickly isolate and halt the unauthorized access, as well as restore and protect our electronic systems. MTN notified the FBI promptly of the incident and continues to cooperate with its investigation.

A ransomware attack is different from other types of cybersecurity incidents you have likely heard about in the media. This type of attack occurs when cybercriminals gain sufficient control of a company’s network and prevent access by authorized users. In the incident experienced by MTN, we were locked out of our files for a brief time before regaining access. The cybercriminals also exfiltrated limited information. There is no evidence that the exfiltrated data has been misused or distributed by the cybercriminals.

Most of the compromised information concerned deceased donor information provided by hospitals for the purpose of organ and tissue donation, or, in some cases, health information. Some of the exfiltrated data contained personally identifiable information (PII) — for example, one or more of the following identifiers: Social Security number (SSN), full name, street address and email address.

We recently learned that a file used to prepare 1099 tax documents and containing your PII was exfiltrated by the cybercriminals. MTN is notifying you of the data security incident because the exfiltrated file contained your name, address, SSN or some combination thereof.

*Consultation and identity theft restoration services*

Although there is no evidence that the cybercriminals misused or distributed the exfiltrated PII, we have contracted with Kroll — an experienced risk management, identity monitoring and breach notification firm — to staff a call center on MTN’s behalf to answer any inquiries about the incident. Through Kroll, MTN is also offering credit monitoring services at no charge to you. Please contact Kroll at XXX-XXX-XXXX to activate a suite of credit monitoring and identity theft solutions more fully described below, or to ask any questions you may have about the data security incident. We encourage you to take advantage of these services:

**Single bureau credit monitoring**

You will receive alerts when there are changes to your credit data — for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you’ll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

**Web Watcher**

Web Watcher monitors internet sites where criminals may buy, sell and trade personally identifiable information. An alert will be generated if evidence of your personal identity information is found.

**Public Persona**

Public Persona monitors and notifies when names, aliases and addresses become associated with your Social Security number. If information is found, you will receive an alert.

**Quick Cash Scan**

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

**$1 million identity fraud loss reimbursement**

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

**Fraud consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Identity theft restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft and then work to resolve it.

MTN has taken all appropriate steps to restore our electronic systems, maintain and ensure cybersecurity and investigate the incident so we can take steps to improve cybersecurity measures to prevent a similar incident in the future. MTN is utilizing an intelligence and analytics platform designed and developed to monitor cybercriminal organizations, including on the dark web. Additionally, the platform will enable us to discover whether credentials are being misused, assist with cybersecurity training and enhance information access controls.

I sincerely appreciate your understanding and contributions to MTN. I am sorry for any concern or inconvenience you have experienced as a result of this incident. Please feel free to call me if you have any questions.

Sincerely,

A picture containing weapon

Description automatically generated

Jan Finn, RN, MSN, President/Chief Executive Officer

*Additional resources*

**Contact information for the three nationwide credit reporting agencies:**

**Equifax**, PO Box 740241, Atlanta, GA 30374, equifax.com, 1-800-685-1111

**Experian**, PO Box 2104, Allen, TX 75013, experian.com, 1-888-397-3742

**TransUnion**, PO Box 2000, Chester, PA 19016, transunion.com, 1-800-888-4213

**Free credit report.** It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report, please visit **annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission’s (“FTC”) website at consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico and Vermont 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 reporting agencies directly to obtain such additional report(s).

**Fraud alerts.** There are two types of 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 at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Security freeze.** You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible and display your name, current mailing address and the date of issue.

**Federal Trade Commission and state Attorneys General offices.** 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 and/or the Attorney General’s office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

**For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, oag.state.md.us, 1-888-743-0023.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, ncdoj.gov, 1-877-566-7226.

**For New York residents:** The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; ag.ny.gov/.

**For Connecticut residents:** You may contact the Connecticut Office of the Attorney General, 165 Capitol Ave., Hartford, CT 06106, 1-860-808-5318, ct.gov/ag.

**For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, mass.gov/ago/contact-us.html

**Reporting of identity theft and obtaining a police report.**

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission and the Oregon Attorney General.