



[Date]

[First name], [Last name]

[Street address], [Unit number]

[City], [Province or State], [Postal or Zip Code]

Re: Notice of Data Security Incident

Timeless Medical Systems (“TMS”) is a service provider for [Name of Milk Bank] (“[Short Form]”) and is reaching out about a data security incident which may have affected some of the personal information that you or a family member provided to [Short Form].

At present, there is no evidence that any information has been misused. Out of an abundance of caution, we are notifying you of this incident and offering you the resources discussed below so that you can take certain precautionary steps to protect yourself, should you wish to do so.

What happened?

On December 18, 2022, TMS learned of unauthorized third-party access to an application used by [Short Form] as part of our services. When we discovered the incident, we immediately took steps to secure our systems and investigate with the assistance of external cybersecurity experts. As part of our investigation, we worked diligently to determine what happened and which information was potentially involved.

Our investigation established that some files were acquired by an unknown third party, after which TMS took steps to mitigate the potential impact of the incident, recovered the files, and informed affected parties such as [Short Form] of the situation, including confirming that the incident involved unauthorized access on [●].

What information was involved?

[Donor Version] The types of affected information are different for each individual, and may include name, address, date of birth, [social security number,] and other information provided in your donor application form, including health information such as lab results or doctors’ notes, to the extent you or a family member provided the foregoing information in dealing with [Short Form] as a donor.

[Outpatient Version] The types of affected information are different for each individual, and may include name, address, date of birth, [social security number,] and other information provided in relation to the services provided by [Short Form] including health information such as lab results or doctors’ notes, and certain financial information such as [credit card information or] banking information, to the extent you or a family member provided the foregoing information in dealing with [Short Form].

At present, we have no evidence that any information has been misused as a result of the incident.

What is TMS doing in response?

We take the security of information that our clients entrust us seriously. Upon discovery of the incident, we immediately took steps to secure our systems, conducted an investigation with the assistance of third-party cybersecurity experts, and filed a report with the FBI and other law enforcement agencies. We also worked with [Short Form] to facilitate notices to privacy regulators, state Attorney General, and other parties, as required.

As part of our ongoing commitment to the security of information in our care, we are in the process of implementing additional safeguards and security measures to further enhance the security of our applications.

We also want to make sure you have the information you need so that you can take steps to help protect yourself from harms such as identity theft. We encourage you to remain vigilant, regularly review and monitor relevant account statements and credit reports, and report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission. Please see below for more information about these steps.

What can I do to protect myself?

In addition to the measures TMS took to mitigate the immediate impacts of the incident, TMS is offering you [●] years of free credit monitoring and identity theft protection services. We encourage you to sign up for the service.

How do I enroll?

Credit monitoring helps protect you by alerting you to key changes in your credit file. Signing up will take about five minutes. No credit card information is required. You must enroll within [90 days] from the date of this letter. The enrollment requires an internet connection and e-mail account. The service may not be available to minors. When signing up for monitoring services, you may be asked to verify personal information to confirm your identity.

What else can I do?

We encourage you to remain vigilant by monitoring your accounts and credit reports, and immediately report any suspicious activity or suspected misuse of your personal information. In addition, we have enclosed information about steps you can take to protect yourself. Please see attached *Additional Important Information* on the following page.

Moving forward

TMS and [Short Form] are committed to maintaining the privacy and security of all the information in our custody and control. We sincerely regret that this incident occurred. Since the incident, TMS has deployed extensive resources to understand what happened, further enhance our safeguards, and comprehensively review the exposure with the help of [Short Form].

Representatives are available for [●] days from the date of this letter to assist you with questions regarding this incident. You can contact them by calling (XXX) XXX-XXXX between the hours of X a.m. and X p.m., 24 hours or Monday to Friday or by sending an e-mail message to xxxx@xxxx.org and supply the representative with your unique code listed above.

Sincerely,

[Name and title of individual with knowledge of the incident at Timeless]

ADDITIONAL IMPORTANT INFORMATION

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are below.

Security Freezes: You can also place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

equifax.com/personal/credit-report-services/

1-800-349-9960

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

experian.com/freeze/center.html

1-888-397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

transunion.com/credit-freeze

1-888-909-8872

Monitoring: You should always remain vigilant, review your financial statements and monitor your accounts for suspicious, unusual, or unauthorized activity.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia*: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, follow the instructions above. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (<https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Vermont*: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of *New Mexico*: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For Residents of *Washington, D.C.*: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

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

For residents of *Maryland, Rhode Island, Illinois, New York, and North Carolina*: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft:

- **Federal Trade Commission** Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
- **Maryland Office of the Attorney General** Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us
- **Rhode Island Office of the Attorney General** Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov
- **North Carolina Office of the Attorney General** Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com
- **New York Office of Attorney General** Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>