EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, CareTree, Inc. ("CareTree") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about August 16, 2023, CareTree became aware of suspicious activity in their CareTree platform. CareTree immediately took steps to secure the platform and minimize any disruption to operations. CareTree launched an investigation into the nature and scope of the incident. The investigation determined an unauthorized actor gained access to certain information held on that platform, and potentially to certain data, on July 21, 2023. Following this determination, CareTree began an in-depth process to identify the individuals whose information may have been impacted, and reviewed internal CareTree records to identify address information for potentially impacted individuals. This process concluded on October 13, 2023. As CareTree is not the owner of the affected data, CareTree began notifying its affected customers who are the owners of the data on October 25, 2023.

The information that could have been subject to unauthorized access includes name, address, driver's license, Social Security number, financial account information, date of birth, medical information (including diagnosis, lab results, medications or other treatment information), and/or health insurance information.

Notice to Maine Residents

On or about December 11, 2023, CareTree provided written notice of this incident to three (3) Maine residents on behalf of affected data owners. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, CareTree moved quickly to investigate and respond to the incident, assess the security of CareTree systems, and identify potentially affected data owners and individuals. Further, CareTree notified federal law enforcement regarding the event. CareTree is also working to implement additional safeguards and training to its employees. CareTree is providing access to credit monitoring services for twelve (12) months, through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, CareTree is providing impacted individuals with guidance on how to better protect against identity theft and fraud. CareTree is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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 by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

CareTree is providing written notice on behalf of customers of this incident to relevant state and federal regulators, as necessary. CareTree is also notifying the U.S. Department of Health and Human Services, attached here as ***Exhibit B***.

EXHIBIT A

CareTree, Inc.
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>>

RE: NOTICE OF <<Variable Data 1>>

Dear <<First Name>> <<Last Name>>:

CareTree, Inc. ("CareTree") is writing to make you aware of an incident that *may* affect the security of some of your personal information. CareTree is an application that centralizes patient care information for caretaker professionals, including <<Data Owner>>. Safeguarding information is among CareTree's highest priorities, and this letter provides details of the incident, our response to it, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or about August 16, 2023, CareTree became aware of suspicious activity in our CareTree platform. We immediately took steps to secure the platform and minimize any disruption to our operations. We launched an investigation into the nature and scope of the incident. The investigation determined an unauthorized actor gained access to certain information held on that platform, and potentially to certain data, on July 21, 2023.

Following this determination, we began an in-depth process to identify the individuals whose information may have been impacted, and reviewed internal CareTree records to identify address information for potentially impacted individuals. This process concluded on October 13, 2023. CareTree is notifying you out of an abundance of caution because the investigation determined that certain information relating to you may have been accessed or acquired by an unknown unauthorized person.

What Information Was Involved? Our investigation determined certain limited information was accessed without authorization. Unfortunately, we are unable to confirm the specific information related to you because it is no longer available as a result of this incident. This information may include your name, address, driver's license, Social Security number, financial account information, date of birth, medical information (including diagnosis, lab results, medications or other treatment information), and/or health insurance information. CareTree is not aware of any attempted or actual misuse of your information.

What We Are Doing. Upon becoming aware of this incident, we immediately took steps to confirm the security of our systems. We are reviewing existing security policies and implemented additional cybersecurity measures to further protect against similar incidents moving forward. We reported this incident to law enforcement and are cooperating with their investigation. We are notifying potentially impacted individuals, including you, so that you may take steps to best protect your information, should you feel it is appropriate to do so. We are also reporting to regulatory authorities, as required.

As an added precaution, we are offering you immediate access to credit monitoring and identity theft protection services for <<CM Duration>> months at no cost to you, through Equifax." We encourage you to enroll in these services as we are not able to do so on your behalf.

To enroll, go to ***www.equifax.com/activate***

Enter your unique Activation Code of ***<<ACTIVATION CODE>>*** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Help Protect Your Information."*

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call 855-457-7890, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

CareTree, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.

EXHIBIT B

Breach Tracking Number: **C4DQ43V228**

Thank you for filing a breach notification via the website of the Office for Civil Rights (OCR) at the Department of Health and Human Services. This is an automated response to acknowledge receipt of your breach notification.

Please do not fax, email, or mail a copy of this breach notification to us as that may delay the processing of your breach notification.

If you have questions or would like to provide feedback about the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification process, or OCR's investigative process, please send us an email at OCRbreachreportingfeedback@hhs.gov.

* Breach Affecting:	500 or More Individuals
* Report Type:	Addendum to Previous Report
* Breach Tracking Number:	C4DQ43V228

* Are you a Business Associate filing on behalf of a Covered Entity? Yes

---

Business Associate

Completion of this section is required if the breach occurred at or by a Business Associate or if you are filing on behalf of a Covered Entity.

Name of Business Associate:	CareTree, Inc.
Street Address Line 1:	222 W Merchandise Mart Plaza
Street Address Line 2:	Suite 1230
City:	Chicago
State:	Illinois
ZIP:	60654

Business Associate Point of Contact Information

* First Name: Vince * Last Name: Regan

* Email: vregan@mullen.law

* Phone Number: (Include area code):

Contact Phones

Phone Number	Usage
(267) 930-4842	Work

Enter the contact information for all Covered Entities you are filing on behalf of.

Covered Entity 1

* Name of Covered Entity:	TBD
* Street Address Line 1:	TBD
Street Address Line 2:	TBD
* City:	TBD

* State: Illinois
* ZIP: TBD

Business Associate Point of Contact Information

* First Name: TBD * Last Name: TBD
* Email: TBD

* Phone Number: (Include area code):

Contact Phones

Phone Number	Usage
(000) 000-0000	Work

* Type of Covered Entity: Healthcare Provider

* Breach Start Date: 07/21/2023 * Breach End Date: 08/16/2023
* Discovery Start Date: 08/16/2023 * Discovery End Date: 10/13/2023
* Approximate Number of Individuals Affected by the Breach: 5856

---

* Type of Breach: Hacking/IT Incident

---

* Location of Breach: Network Server

---

* Type of Protected Health Information Involved in Breach:

Clinical
Demographic
Financial

* Clinical

Diagnosis/Conditions
Lab Results
Medications
Other Treatment Information

* Demographic

Address/ZIP
Date of Birth
Drivers License
Name
SSN

* Financial

Credit Card/Bank Acct #
Other Financial Information

---

* Brief Description of the Breach: On or about August 16, 2023, CareTree became aware of suspicious activity in their CareTree platform. CareTree immediately took steps to secure the platform and minimize any disruption to operations. CareTree launched an investigation into the nature and scope of the incident. The investigation determined an unauthorized actor gained access to certain information held on that platform, and potentially to

certain data, on July 21, 2023. Following this determination, CareTree began an in-depth process to identify the individuals whose information may have been impacted, and reviewed internal CareTree records to identify address information for potentially impacted individuals. This process concluded on October 13, 2023. As CareTree is not the owner of the affected data, CareTree began notifying its affected customers who are the owners of the data on October 25, 2023.

---

* Safeguards in Place Prior to Breach:	Privacy Rule Safeguards (Training, Policies and Procedures, etc.) Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.) Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.) Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

* Individual Notice Provided Start Date:	11/15/2023	Individual Notice Provided Projected/Expected End Date:
Was Substitute Notice Required?	No	
Was Media Notice Required?	No	

---

* Actions Taken in Response to Breach:	Changed password/strengthened password requirements Implemented new technical safeguards Performed a new/updated Security Rule Risk Analysis Revised policies and procedures

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

* Name: Meghan Novak on behalf of Vince Regan Date: *12/11/2023*