FOREFRONT MANAGEMENT, LLC

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip code>> <<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>> <<Name 2>>,

Forefront Management, LLC is committed to protecting the confidentiality and security of our current and former employees' information. We are writing to inform you that we recently identified and addressed a data security incident that may have involved some of your information. This notice explains the incident, measures that have been taken, and some steps you can take in response.

What Happened: On June 24, 2021, Forefront concluded our investigation of an intrusion into our IT network by cyber criminals and determined that the incident resulted in unauthorized access to certain files on our IT systems that contain employee information. We first identified the intrusion on June 4, 2021 and immediately took our entire network offline to protect the information we maintain and to secure our systems. We also launched an investigation and notified law enforcement.

What Information was Involved: Through our investigation, we determined that the intrusion resulted in an unauthorized party gaining access to our IT network between the dates of May 28, 2021 and June 4, 2021. While in our IT network, the unauthorized party accessed certain files that contain information pertaining to a small number of Forefront employees. **While our investigation did not find evidence that your information was specifically involved**, we could not rule out the possibility that, files containing some of your information, including your name and Social Security number, may have been subject to unauthorized access as a result of this incident.

Additionally, our investigation determined that the unauthorized party also accessed certain files that contain a small number of Forefront Dermatology patients' information. If you are a current or former Forefront Dermatology patient, we cannot rule out the possibility that some of your patient information could have been involved, **although investigation did not find evidence that patient information relating to our employees was specifically involved**. This information may have included your name, address, date of birth, patient account number, health insurance plan member ID number, medical record number, dates of service, provider names, and/or medical and clinical treatment information.

What We are Doing: Out of an abundance of caution, and because we take this incident seriously, we are offering you a complimentary **12**-month membership to TransUnion's *my*TrueIdentity Credit Monitoring Service. This service helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. *my*TrueIdentity is free and enrolling in this program will not affect your credit score. **For more information on *my*TrueIdentity, including instructions on how to activate your complimentary 12-month membership and steps you can take to protect your information, please see the pages that follow this letter.**

What You Can Do: We recommend that you remain vigilant by reviewing your financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, you should contact your financial

institution immediately. Additionally, if you are also a current or former patient of Forefront Dermatology, we recommend that you review the statements you receive from your healthcare providers and health insurance plan. If you see any services that were not received, please contact the provider or health plan immediately.

For More Information: We deeply regret any inconvenience or concern this incident may cause. We take this matter very seriously and are continuing to enhance our security protocols to help prevent a similar incident from occurring in the future. If you have any questions about this incident, please call 855-899-4166, Monday through Friday, between 8:00am and 8:00pm, Central Time.

Sincerely,

Scott Bremen

Scott Bremen
Chief Executive Officer

As a safeguard, we have arranged for you to enroll, at **no cost to you**, in an online credit monitoring service (*my*TrueIdentity) for **12 months** provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies. This service helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate *my*TrueIdentity Now in Three Easy Steps

1. ENROLL by: **<<Enrollment Deadline>>** (Your code will not work after this date.)
2. VISIT the **TransUnion *my*TrueIdentity website** to enroll: **www.MyTrueIdentity.com**
3. ENTER the **12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.**

If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>.** Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

• Once you are enrolled, you will be able to obtain 12 months of unlimited access to your TransUnion credit report and credit score.

• The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.

• The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.) * Offline members will be eligible to call for additional reports quarterly after enrolling.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. 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

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 state. You can obtain information from these sources 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. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

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, 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 they 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, contact each of the credit reporting agencies at the addresses below:

- **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'll 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 some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

FOREFRONT DERMATOLOGY®

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name1>>,

Forefront Dermatology, S.C. and its affiliated practices are committed to protecting the confidentiality and security of our patients' information. We are writing to inform you that we recently identified and addressed a data security incident that may have involved some of your information. This notice explains the incident, measures that have been taken, and some steps you can take in response.

On June 24, 2021, Forefront Dermatology concluded our investigation of an intrusion into our IT network by unauthorized parties and determined that the incident resulted in unauthorized access to certain files on our IT systems that contain patient information. We first identified the intrusion on June 4, 2021 and immediately took our entire network offline out of an abundance of caution to protect our patients and to secure our systems. We also launched an investigation and notified law enforcement.

Through our investigation, we determined that the intrusion resulted in unauthorized parties gaining access to our IT network between the dates of May 28, 2021 and June 4, 2021. While in our IT network, the unauthorized parties accessed certain files that contain information pertaining to some Forefront Dermatology patients. **While our investigation did not find evidence that your information was specifically involved,** we could not rule out the possibility that files containing some of our patient information may have been subject to unauthorized access as a result of this incident. This information may have included some of your information that Forefront Dermatology has on file, including name in combination with your address, date of birth, patient account number, health insurance plan member ID number, medical record number, dates of service, provider names, and/or medical and clinical treatment information.

To date, Forefront has no evidence that patient Social Security numbers, driver's license numbers, or financial account/payment card information were involved in this incident.

We recommend you review the statements you receive from your healthcare providers and health insurance plan. If you see any services that were not received, please contact the provider or health plan immediately.

We deeply regret any inconvenience or concern this incident may cause. We take this matter very seriously and are continuing to enhance our security protocols to help prevent a similar incident from occurring in the future. If you have any questions about this incident, please call 855-899-4166, Monday through Friday, between 8:00 a.m. to 8 p.m., Central Time.

Sincerely,

Betsy J. Wernli

Betsy J. Wernli, M.D., FAAD
President

FOREFRONT DERMATOLOGY®

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name1>>,

Forefront Dermatology, S.C. and its affiliated practices are committed to protecting the confidentiality and security of our patients' information. We are writing to inform you that we recently identified and addressed a data security incident that may have involved some of your information. This notice explains the incident, measures that have been taken, and some steps you can take in response.

On June 10, 2021, Forefront Dermatology determined that, through an intrusion into our IT network, unauthorized parties may have gained access to files on our IT systems that contain information for some patients. We first identified the intrusion on June 4, 2021 and immediately took our entire network offline out of an abundance of caution to protect our patients and to secure our systems. We also launched an investigation and notified law enforcement.

Through our investigation, we determined that the intrusion resulted in unauthorized parties gaining access to our IT network between the dates of May 28, 2021 and June 4, 2021. While in our IT network, the unauthorized parties accessed certain files containing some of your information, including your name in combination with your provider's name, accession number (a certain number assigned to identify pathology slides), and status as a Forefront patient.

In addition, we could not rule out the possibility that files containing your name, address, date of birth, patient account number, health insurance plan member ID number, medical record number, dates of service, provider names, and/or medical and clinical treatment information may have also been accessed.

To date, Forefront has no evidence that patient Social Security numbers, driver's license numbers, or financial account/payment card information were involved in this incident.

We recommend you review the statements you receive from your healthcare providers and health insurance plan. If you see any services that were not received, please contact the provider or health plan immediately.

We deeply regret any inconvenience or concern this incident may cause. We take this matter very seriously and are continuing to enhance our security protocols to help prevent a similar incident from occurring in the future. If you have any questions about this incident, please call 855-899-4166, Monday through Friday, between 8:00 a.m. to 8 p.m., Central Time.

Sincerely,

Betsy J. Wernli

Betsy J. Wernli, M.D., FAAD
President