Appendix

Timios detected unauthorized access to certain devices in its network that resulted in the encryption of some of its systems. Timios immediately activated its incident response plan, took measures to stop the unauthorized access, and launched an investigation. A cybersecurity firm was engaged to assist with the investigation and determine the nature and scope of the incident. Through the investigation, Timios identified unauthorized access to its systems between July 19-25, 2021.

On July 30, 2021, the investigation determined that personal information related to some individuals may have been accessed or acquired by an unauthorized actor during that time but was unable to determine whether the unauthorized actor actually viewed any of the information. Out of an abundance of caution, Timios is notifying all individuals whose data may have been accessed. Timios reviewed the files that may have been accessed or acquired and on September 7, 2021, identified 115 Maine residents' whose names and one or more of the following data elements may have been accessed: Social Security number, driver's license or state-issued identification number, passport number, tax identification number, military identification number, financial account number, payment card number and/or date of birth.

On October 11, 2021, Timios is notifying 115 Maine residents via U.S. mail in accordance with Me. Rev. Stat. Tit. 10, §1348.[1] A copy of the notification letter is enclosed. Timios is offering eligible individuals a complimentary one-year membership in credit monitoring and identity theft protection services through Experian. Timios is providing a telephone number for potentially affected individuals to call with any questions they may have about the incident.

To help prevent this type of incident from happening again, Timios is implementing additional measures to further enhance already exiting security protocols and is providing continued education and training to all employees.

[1] This report is not, and does not constitute, a waiver of Timios' objection that Maine lacks personal jurisdiction over the company related to this matter.

TIMIOS

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Timios, Inc. is committed to maintaining the integrity and the security of the data that we receive and maintain. We are writing to notify you of a recent cybersecurity incident that may involve some of your data. This letter contains a description of the incident, measures we have taken in response, information on what personal information of yours may be involved, and steps you may consider taking in response. We take this situation seriously and sincerely regret any concern that this may cause.

What Happened?

We detected unauthorized access to certain devices in our network that resulted in the encryption of some of our systems. We immediately activated our incident response plan, took measures to stop the unauthorized access, and launched an investigation. A cybersecurity firm was engaged to assist with the investigation and determine the nature and scope of the incident. Through the investigation, we identified unauthorized access to Timios' systems between July 19-25, 2021. On July 30, 2021, the investigation determined that personal information related to some individuals may have been accessed or acquired by an unauthorized actor during that time, but was unable to determine whether the unauthorized actor actually viewed any of the information. Out of an abundance of caution, we are notifying all individuals whose data may have been accessed. We reviewed the files that may have been accessed or acquired and determined on September 7, 2021 that your information may have been involved.

What Information Was Involved?

The information accessed or acquired may include your name and one or more of the following: Social Security number, driver's license or state-issued identification number, passport number, tax identification number, military identification number, financial account number, payment card number and/or date of birth.

What We Are Doing:

We notified law enforcement and are fully cooperating with their investigation. We are also taking a number of steps to help prevent something like this from occurring again. We implemented additional measures to further enhance our security protocols and are providing continued education and training to our employees.

As a precaution, we are offering a complimentary one-year membership to Experian's® IdentityWorks Credit 3B. This product helps detect possible misuse of your personal credit information and provides you with identity protection services focused on identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate the complimentary membership, please see the additional information provided with this letter.

What You Can Do:

It is a best practice to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. As always, you should remain vigilant for incidents of fraud that may attempt to trick you into providing passwords or other information about yourself. We also encourage you to enroll in Experian IdentityWorks.

For More Information:

For more information on identity theft prevention and your complimentary services, as well as some additional steps you can take to protect your personal information, please see the additional information enclosed with this letter.

If you have any questions, please call (855) 551-1703, Monday through Friday from 8:00 am to 5:30 pm Central Time.

Sincerely,

Ray Davison

Ray Davison
Chief Executive Officer
Timios, Inc.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **<<b2b_text_1(Enrollment Deadline)>>** **(**Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: **<<Activation Code s_n>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877.890.9332**. Be prepared to provide engagement number **<<b2b_text_2(Engagement Number)>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit or call 877.890.9332 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **877.890.9332**.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 over the next 12 to 24 months. 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 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, 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.

Timios is located at 5716 Corsa Ave # 102, Westlake Village, CA 91362 and may be reached by telephone at (818) 706-6400.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection*; and *New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov*

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 109 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

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.