

## **Appendix**

On February 1, 2023, Veracyte, Inc. (“Veracyte”) learned that an email spear-phishing incident targeting one of its employees involved some sensitive information. The incident occurred on January 27, 2023, when an employee was tricked into believing they were responding to a request for information from another employee, but they were conversing with an unknown individual. In response, Veracyte took immediate steps to prevent further disclosure and initiated an investigation of the incident. The investigation determined that certain spreadsheets were inadvertently disclosed to the unauthorized individual via email and that the spreadsheets contained some information related to paying Veracyte vendors. Importantly, Veracyte’s email system, Veracyte’s network, and the employee’s email account, were NOT accessed without authorization or otherwise involved in the incident.

Veracyte’s review of the spreadsheets determined that they contained the name and Social Security number of one Maine resident.

Beginning on March 3, 2023, a notification letter will be mailed to the Maine resident in accordance with Me. Rev. Stat. Tit. 10, §1348 via United States First-Class mail. A copy of the notification letter is enclosed. The Maine resident is being offered one year of access to a credit monitoring and identity theft protection solution.

To help prevent something like this from happening again, Veracyte has enhanced its internal processes and security safeguards to further protect and monitor the information they maintain.



<<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>>,

Veracyte, Inc. (“Veracyte”) is committed to protecting the security and privacy of the information we maintain. We are writing to notify you about an incident that may have involved some of your information. This notice explains the incident, measures we have taken in response, and additional steps you can take to protect your information.

**What Happened?** On February 1, 2023, we determined that some of your information was involved in an email spear-phishing incident targeting one of our employees. The incident occurred on January 27, 2023, when an employee was tricked into believing they were responding to a request for information from another employee, but they were conversing with an unknown individual. In response, we took immediate steps to prevent further disclosure and initiated an investigation of the incident. The investigation determined that certain spreadsheets were inadvertently disclosed to the unauthorized individual via email and that the spreadsheets contained some information related to paying our vendors. Importantly, Veracyte’s email system, Veracyte’s network, and the employee’s email account, were NOT accessed without authorization or otherwise involved in the incident.

**What Information Was Involved?** Our analysis of the spreadsheets involved determined that one spreadsheet contained your name and Social Security number.

**What We Are Doing.** To help prevent something like this from happening again, we have enhanced our internal processes and security safeguards to further protect and monitor the information we maintain. In addition, as a precaution, we are offering you a complimentary 12-month membership of Experian’s® IdentityWorks<sup>SM</sup>. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks, including instructions on how to activate your complimentary membership, please see the pages that follow this letter.**

**What You Can Do.** We want to assure you that we take this incident very seriously. For information about additional steps you can take in response to the incident, please see the pages that follow this letter. We also encourage you to enroll in the complimentary credit monitoring services we are offering you.

**For More Information.** We deeply regret any concern this incident may cause you. If you have any questions, please contact (866) 674-7985, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Doug Curwin  
Privacy Officer  
Veracyte, Inc.

To help protect your identity, we are offering a **complimentary** one-year membership to Experian IdentityWorks<sup>SM</sup>. This product 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 IdentityWorks In Three Easy Steps

1. ENROLL by: <<b2b\_text\_6(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 that arose as a result of this incident 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\_1(engagement number)>> as proof of eligibility for the identity restoration services by Experian.

### ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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

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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** 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](http://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. 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](http://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](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://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.identitytheft.gov](http://www.identitytheft.gov)

**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](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://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.

Veracyte is located at 6000 Shoreline Court, Suite 300, South San Francisco, CA 94080 and can be reached via telephone at 650.243.6300.

**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](http://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](http://www.ncdoj.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.