



Baker&Hostetler LLP

1735 Market Street
Suite 3300
Philadelphia, PA 19103-7501

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

March 14, 2025

Sara M. Goldstein
direct dial: 215.564.1572
sgoldstein@bakerlaw.com

VIA EMAIL (IDTHEFT@OAG.STATE.MD.US)

Anthony G. Brown
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Data Security Incident

Dear Attorney General Brown:

We are writing on behalf of our clients, California Cryobank LLC and its affiliates (collectively “CCB”), to notify you of a data security incident.

CCB completed its investigation of an incident that involved unauthorized activity in its information technology (“IT”) environment. Upon identifying the activity, CCB isolated the computers from its IT network and launched an investigation. Through its investigation, CCB determined that an unauthorized party gained access to its IT environment and may have accessed and/or acquired files maintained on certain computer systems between April 20, 2024 and April 22, 2024. CCB undertook a comprehensive search and review of the files that may have been accessed and/or acquired as a result of the incident.

As part of its ongoing review of the files, CCB determined that certain files potentially accessed and/or acquired as a result of the incident contain information pertaining to certain customers. The information potentially involved varied by customer but included names and one or more of the following: Social Security numbers, bank account and routing numbers, payment card numbers, and/or health insurance information. On March 13, 2025, CCB determined that this incident may have involved information pertaining to 45 Maryland residents.

Beginning on March 14, 2025, CCB will mail notification letters via United States Postal Service First-Class mail to Maryland residents whose information may have been involved, in accordance with Md. Code Ann., Com. Law § 14-3504. A copy of the notification letter is enclosed. CCB is offering individuals whose Social Security numbers may have been involved in the incident complimentary one-year memberships to credit monitoring services through CyberScout. CCB has also established a dedicated, toll-free call center to answer questions that letter recipients may have.

March 14, 2025

Page 2

To help prevent something like this from happening again, CCB has implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor its systems.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in cursive script that reads "Sara Goldstein".

Sara M. Goldstein
Partner

Enclosure



0003471

CooperSurgical, Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS127

11 0003471



March 14, 2025

Dear [REDACTED]:

California Cryobank LLC and our affiliates (collectively “CCB”) are committed to protecting the confidentiality and security of the information we maintain. We are writing to inform you about a data security incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

What Happened?: CCB recently completed our investigation of an incident that involved unauthorized activity on certain computers in our information technology (“IT”) environment. Upon identifying the activity on April 21, 2024, CCB isolated the computers from our IT network and launched an investigation. Through our investigation, CCB determined that an unauthorized party gained access to our IT environment and may have accessed and/or acquired files maintained on certain computer systems between April 20, 2024 and April 22, 2024. Out of an abundance of caution, CCB undertook a comprehensive search and review of the files that may have been accessed and/or acquired as a result of the incident.

What Information was Involved?: As part of our ongoing review of the files CCB determined that certain files that were potentially accessed and/or acquired as a result of the incident contain some of your information, including your name Social Security number, driver's license number, financial account number and health insurance information.

What We Are Doing?: To help prevent something like this from happening again, we have implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor our systems. As a precaution, we are offering you a complimentary twelve (12) months membership to identity protection services through TransUnion. The services include access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to any of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud.

What You Can Do?: For more information on Cyberscout, a TransUnion company specializing in fraud assistance and remediation services, including instructions on how to activate your complimentary twelve (12) months membership and additional steps you can take, please see the pages that follow this letter.

For More Information: We deeply regret any inconvenience or concern this incident may cause and take this matter seriously. If you have any questions about this incident, please call **833-998-5854**, Monday through Friday, between 8:00 a.m. – 8:00 p.m., Eastern Time.

Sincerely,

California Cryobank LLC



Enrollment Instructions:

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided.

When prompted please provide the following unique code to receive services: [REDACTED].

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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, 1-888-378-4329

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-833-799-5355

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.

CCB's mailing address is 11915 La Grange Avenue, Los Angeles, California 90025 and its phone number is 866-927-9622.

Connecticut Residents: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia Residents: You may contact and obtain information from your attorney general at: *Office of the Attorney General for the District of Columbia*, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland Residents: 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.marylandattorneygeneral.gov

New York Residents: 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 Residents: 19 Rhode Island residents have been notified of this incident. 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 Residents: 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.