



21830

July 6, 2021

Re: Notice of Data Breach

Dear Our Valued Team Member,

We write to inform you about a recent data security incident that involves some of your personal information. We take the protection of your information very seriously, and we are contacting you directly to explain the circumstances of the incident, the steps we are taking in response, and the resources we will make available to you. Please know that the safety and security of your personal information is our utmost priority in resolving this matter.

What Happened?

On Tuesday, June 29, 2021, we discovered that certain company files were accessed without authorization in a cyberattack. Upon discovering this incident, we began an investigation to understand the scope of the incident, secured the Company's information technology systems, and contacted law enforcement. While we know the files were compromised, as of this time, we do not have any evidence that the information in those files has been made public or that any identify theft fraud has been committed to date.

What Information Was Involved?

We are still working to determine the exact scope and nature of this incident. As of now, we believe the affected information that may have been obtained without authorization included employee names, contact information, Social Security Numbers, dates of birth, bank account numbers, bank routing numbers, dates of employment, salary information, benefits election, insurance policy and dependent information, and other related information maintained for HR purposes.

What We Are Doing.

Please be assured that we have taken numerous steps to address the incident. Upon discovery of the breach, our cybersecurity team immediately took a series of actions, including a forensic investigation to confirm that no other company systems were impacted and to better understand the nature of the event.

Protecting your personal information is of utmost concern to us. We will provide identity theft protection and credit monitoring services offered by Experian at no cost to you (as well as your dependents in our benefits plan) for the next two years. You will hear directly from us in a separate communication that will detail how to activate your Experian membership and start monitoring your personal information.



We also will make available free internal consulting services to assist you in protecting your information. Additionally, we will continue to implement security measures and team member education to protect against the recurrence of a similar incident.

What You Can Do.

We want to make sure you are aware of the steps you may take to guard against potential identity theft or fraud.

As we all know, cyberattacks increasingly threaten the security of information at work and at home. You should remain vigilant by reviewing account statements and monitoring free credit reports. We also encourage you to take advantage of the identity theft protection and credit monitoring services offered by Experian being provided at no cost to you. Please see the attachment for further steps you can take to protect your personal information as well as additional important information. We also ask you to remain vigilant against any attack and to report any suspicious computer-related activity.

For More Information:

As noted, please see the attachment for further steps you can take to protect your personal information as well as additional important information.

To address any questions you may have, we will be hosting a virtual Town Hall meeting via Zoom on Tuesday, July 6 at 11:30 a.m. for remote team members, and an in-person Town Hall meeting on July 6 at 1:30 p.m. for those located in our facility. A calendar invite with details on the Town Hall meetings will follow shortly.

If you have further questions or concerns about this incident, please contact LaurieMcMullin@acesurgical.com or (781) 534-5279. Please know that we sincerely regret any inconvenience caused by this incident and that we are working diligently to protect against future events of this kind.

Thank you for your patience and understanding.

Regards,



ATTACHMENT

What You Can Do:

- Be on the alert for suspicious activity related to your accounts, credit report and financial products. We cannot exclude the possibility that third parties may attempt to use some of your personal information for financial gain.
- If you suspect an incident of identity theft has occurred, find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report and/or contact a major credit bureau, other local law enforcement, your state attorney general or the Federal Trade Commission. Get a copy of any report as you may need it to clear up any fraudulent debts.
- Call one of the major credit bureaus listed below to place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days. You can obtain further information about fraud alerts and security freezes from the credit bureaus.
- You may also place a security freeze on your credit reports, free of charge. A security freeze generally requires submitting to the credit bureau your full name, address (including past addresses within the last five years), proof of current address, a legible photocopy of a government issued identification card, social security number, and date of birth. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

- Equifax, P.O. Box 740241, Atlanta, GA 30348: equifax.com or 1-800-525-6285
 - Experian, P.O. Box 4500, Allen, TX 75013: experian.com or 1-888-397-3742
 - TransUnion, P.O. Box 2000 Chester, PA 19022: transunion.com or 1-800-680-7289
- We also recommend you periodically request that credit reports from all available major credit bureaus be sent to you, free of charge, for your review. Checking your credit reports periodically can help you spot problems and address them quickly. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.
 - You can obtain additional information about preventing identify theft, fraud alerts and security freezes from the Federal Trade Commission ("FTC"), 600 Pennsylvania Avenue, NW, Washington, DC 20580: 877-382-4357, <https://www.consumer.ftc.gov/topics/identity-theft>. You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA at <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.
 - For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.
 - For New York Residents: Further information about security breach response and identity theft prevention and protection can be obtained from New York's Office of the Attorney General, The Capitol, Albany, NY 12224-0341: 1 (800) 771-7755 or <https://ag.ny.gov/internet/privacy-and-identity-theft>.
 - For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.
 - For Maryland Residents: Further information about security breach response and identity theft prevention and protection can be obtained from Maryland's Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202: 410-576-6300 or <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>.
 - For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.



1034 Pearl Street
Brockton, MA 02301

[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

RE: Important Security Notification
Please read this entire letter.

Dear [Insert recipient's name]:

On July 6, 2021, we notified you that we discovered on June 29, 2021 that certain company files were accessed without authorization in a cyberattack. Today, we are contacting you regarding the identify theft protection and credit monitoring services that will be offered by Experian at no cost to you. Enclosed is a copy of the July 6 communication explaining the circumstances of the incident and steps you can take to guard against identity theft or fraud.

Protecting your personal information is of utmost concern to us. While we know the files were compromised, as of this time, we do not have any evidence that the information in those files has been made public or that any identify theft fraud has been committed to date. As of now, we believe the affected information that may have been obtained without authorization included employee names, contact information, Social Security Numbers, dates of birth, bank account numbers, bank routing numbers, dates of employment, salary information, benefits election, insurance policy and dependent information, and other related information maintained for HR purposes.

What we are doing to protect your information:

To help protect your identity, we have worked with Experian, one of the leading credit and identity monitoring companies, to provide a complimentary 24-month membership in Experian's® IdentityWorksSM. This product provides you with identity theft detection and resolution tools. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: October 31, 2021**. Your **activation code** will not work after this date.
- **Visit** the Experian IdentityWorks website to enroll: [URL]
- Provide your **activation code**: [code]
Please note that any dependent or beneficiary whose information may have been involved in this incident will receive a personalized letter from Experian with a dedicated activation code.

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 [customer service

number] by October 31, 2021. Be prepared to provide engagement number [engagement #] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [customer service number]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration support is available as part of the membership being provided by the Company at no cost to you and is effective from the date of this letter. Registration is not required to access the service provided by Experian's Identity Restoration Specialists. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please contact LaurieMcMullin@acesurgical.com or (781) 534-5279.

Sincerely,

Michael Mancini
General Manager and Chief Operating Officer

Enclosure

* 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.