

# Morgan Lewis

**Gregory T. Parks**

Partner  
215.963.5170  
gregory.parks@morganlewis.com

June 12, 2024

**VIA EMAIL**

Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place, 25th Floor  
Baltimore, MD 21202  
Email: [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us)

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

This Firm represents Council for Relationships, Inc. ("CFR"), a non-profit organization that provides low-fee therapy services and professional education. We are representing CFR *pro bono* without charge. We are writing to notify your office about the nature and circumstances of a recent data security incident at CFR.

CFR recently discovered suspicious activity on one of its servers that has since been confirmed to be a data security incident. Investigation revealed that an unauthorized third-party gained access to the server. CFR does not know whether any information was taken from the server. But out of an abundance of caution, CFR is assuming that any information on the server may have been taken. On May 6, 2024, CFR confirmed the identity of individuals whose personal information was present on the servers.

The nature of the information involved varied by person. For current and former employees, the information included name, address, social security number, banking information for direct deposit, and information related to employee benefit programs. For some current and former students, the information included name, address, and social security number. For donors, the information included name, credit card details, and amount of any donation(s). For clients, the information included name, address, and session dates. For a smaller number of clients, the information included notes taken by a counselor during counseling sessions. For individuals whose social security numbers were involved, CFR is offering two years of credit monitoring.

Since learning of this incident, CFR has been engaged in an investigation and recovery effort with the assistance of cyber experts and law enforcement. Determining what information was on the server so that we could notify potentially affected individuals was a top priority of this effort. CFR is also making increased efforts to improve its information security to prevent incidents like this from occurring in the future.

**Morgan, Lewis & Bockius LLP**

2222 Market Street  
Philadelphia, PA 19103-3007  
United States

 +1.215.963.5000  
 +1.215.963.5001

Office of the Attorney General  
June 12, 2024  
Page 2

Further information about what mitigations have been completed to date and what further mitigations are recommended to the individuals in question can be found in the enclosed notification that CFR is sending to 53 Maryland residents via mail on June 12, 2024.

If you have any questions, please feel free to contact me.

Regards,

A handwritten signature in blue ink, appearing to read "G. T. Parks", with a stylized flourish at the end.

Gregory T. Parks

Enclosure



Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

June 12, 2024



L4246-L03-0000001 T00001 P001 \*\*\*\*\*SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L03 FORMER STAFF

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



Re: Notice of Information Security Incident

Dear Sample A. Sample:

You are receiving this letter as a former staff member at Council for Relationships (“CFR”).

We are writing to notify you that a recent data security incident affecting CFR’s operations may have involved your personal information. This letter is being sent to provide you with information and to advise you of services that CFR is offering at no charge to you, to help you at this time. We outline below what happened, what information was potentially involved, what we have done, and what you can do to protect your continued privacy.

### What Happened?

CFR discovered suspicious activity on one of its servers that we have since confirmed to be a data security incident. Our investigation revealed that an unauthorized third-party gained access to the server. We do not know whether any information was taken from our systems. But out of an abundance of caution, we are assuming that any information on the server may have been taken.

### What Information Was Involved?

The server in question included personal information about our current and former staff members, including name, address, social security number, payroll information, bank account details for direct deposit, and details of your current or past participation in CFR’s benefit programs.

### What We Are Doing

Immediately upon learning of this incident, we launched an investigation and recovery effort with the assistance of cyber experts and law enforcement. Determining whether information was compromised in any way was one of the top priorities of this effort, so that we could notify potentially affected individuals. Rest assured, we are also making increased efforts to improve our information security to prevent incidents like this from occurring in the future.

**To help protect your identity, we have arranged to offer a complimentary one-year subscription to Experian IdentityWorks<sup>SM</sup> credit monitoring and identity theft protection. To activate your membership, and to start monitoring your credit and the use of your personal information:**

- Ensure that you **enroll by** August 30, 2024 (Your code will not work after this date).
- **Visit** the Experian IdentityWorks<sup>SM</sup> website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**



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 1-877-890-9332 by August 30, 2024. Be prepared to provide engagement number B123644 as proof of eligibility for the Identity Restoration services by Experian.

### What You Can Do

To help protect your personal information, we strongly recommend you take the following steps:

- Carefully review statements sent to you by your bank, credit card company, or other financial institutions as well as government institutions like the Internal Revenue Service (IRS). Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.
- Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and social security number to establish credit and to block that credit from being established if you were not the one who initiated it.
- The attached **Reference Guide** describes additional steps that you can take and provides resources for additional information. We encourage you to read and follow these steps as well.

### For More Information

If you have questions or concerns or learn of any suspicious activity that you believe may be related to this incident, please call me at 215-382-6680 ext 3228.

Please know that CFR takes this matter very seriously, and we apologize for any concern and inconvenience this may cause you.

Sincerely,



Howard Cohen  
Chief Financial Officer  
Council for Relationships

## **REFERENCE GUIDE**

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

**Order Your Free Credit Report.** To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at [www.ftc.gov](http://www.ftc.gov) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or [www.ftc.gov](http://www.ftc.gov).

**Place a Fraud Alert on Your Credit File.** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

|            |                                                                                  |                |                                                            |
|------------|----------------------------------------------------------------------------------|----------------|------------------------------------------------------------|
| Equifax    | P.O. Box 740241<br>Atlanta, Georgia 30374-0241                                   | 1-800-525-6285 | <a href="http://www.equifax.com">www.equifax.com</a>       |
| Experian   | P.O. Box 9532<br>Allen, Texas 75013                                              | 1-888-397-3742 | <a href="http://www.experian.com">www.experian.com</a>     |
| TransUnion | Fraud Victim Assistance Division<br>P.O. Box 2000<br>Chester, Pennsylvania 19016 | 1-800-680-7289 | <a href="http://www.transunion.com">www.transunion.com</a> |

**Place a Security Freeze on Your Credit File.** You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

|            |                                                                                  |                                                            |
|------------|----------------------------------------------------------------------------------|------------------------------------------------------------|
| Equifax    | P.O. Box 740241<br>Atlanta, Georgia 30374-0241                                   | <a href="http://www.equifax.com">www.equifax.com</a>       |
| Experian   | P.O. Box 9554<br>Allen, Texas 75013                                              | <a href="http://www.experian.com">www.experian.com</a>     |
| TransUnion | Fraud Victim Assistance Division<br>P.O. Box 2000<br>Chester, Pennsylvania 19016 | <a href="http://www.transunion.com">www.transunion.com</a> |



The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years.
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

**Contact the U.S. Federal Trade Commission.** If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

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

**For District of Columbia Residents:** You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, [www.oag.dc.gov](http://www.oag.dc.gov)

**For Maryland Residents:** You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us)

**For New York Residents:** You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

|                                                                                                     |                                                                                                   |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| New York Attorney General's Office                                                                  | NYS Department of State's Division of                                                             |
| Bureau of Internet and Technology                                                                   | Consumer Protection                                                                               |
| (212) 416-8433                                                                                      | (800) 697-1220                                                                                    |
| <a href="https://ag.ny.gov/internet/resource-center">https://ag.ny.gov/internet/resource-center</a> | <a href="https://www.dos.ny.gov/consumerprotection">https://www.dos.ny.gov/consumerprotection</a> |

**For North Carolina Residents:** You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)