



510 Madison Ave
9th Floor
New York, NY 10022
Tel: 646-874-5400

January 29, 2024

Via E-Mail

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Capula Investment Management LLP – Notice of Data Event

Dear Sir or Madam:

We represent Capula Investment US LP (“CIUS”) and are writing to notify your Office of a recent event that may affect the security of certain personal information relating to one (1) Maryland resident.

Please note this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, CIUS does not waive any rights or defenses, including regarding the applicability of Maryland law, the applicability of the Maryland data breach notification statute, or personal jurisdiction.

On May 31, 2023, a payroll service provider, Paycor, Inc. (“Paycor”), used by CIUS became aware that the MOVEit Transfer software of Paycor’s software service provider, Progress Software, experienced a “zero-day” cyber vulnerability between May 29 and May 30, 2023. MOVEit Transfer is a secure file transfer protocol that is used by governments and organizations worldwide to send and receive certain data securely. Paycor discovered that an unauthorized third party exploited the cyber vulnerability on the MOVEit Transfer software platform to obtain certain files, including personal information, transferred through the platform.

We understand that Paycor immediately took steps to address the issue, including conducting a forensic analysis with the assistance of outside experts. According to Paycor, the analysis showed the incident’s scope was limited to the third-party MOVEit Transfer platform and did not impact Paycor’s own software.

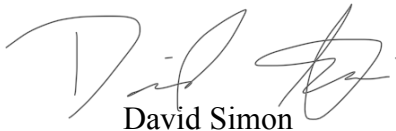
On November 30, 2023, Paycor notified CIUS of this data breach and the findings of its forensic analysis, specifically noting that certain personal information of CIUS personnel was compromised, including their date of birth and Social Security number.

CIUS maintains a robust information and cyber security program and takes very seriously its responsibility to protect all data entrusted to us. This breach was limited to the third-party software provider of our payroll provider, Paycor, and did not impact the systems or software of CIUS or its affiliates.

CIUS takes very seriously its responsibility to protect data entrusted to us, and promptly notified affected individuals – a copy of the notification is enclosed. As part of our ongoing commitment to the privacy of personal information in our care, we reviewed our existing procedures, and are continuously working to implement additional safeguards to further secure our information systems.

Should you have any questions regarding this notification or other aspects of the data security event, please contact me at (202) 371-7120.

Sincerely,

A handwritten signature in black ink, appearing to read "David Simon", with a stylized flourish at the end.

David Simon

[Insert Recipient's Name]

[Insert Address]

[Insert City, State, Zip]

[Date]

RE: Important Security Notification. Please read this entire letter.

Dear [First Name] [Last Name]:

Independent Dialysis Foundation (IDF) recently discovered an incident that may affect the security of your personal information. We want to provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so.

On January 10, 2024, Independent Dialysis Foundation became aware of a breach of your personal information. On January 3, 2024, information containing your name, address, phone number, social security number, date of birth, and treatment information was received by an unauthorized party as the result of a misdirected fax. We have been in contact with the unintended recipient of your information who has assured us that the information has been destroyed.

We are notifying you now so you can take action to reduce or eliminate potential harm.

We advise you to immediately take the following steps:

- Call the toll-free numbers of any of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three bureaus will provide you a copy of your credit report free of charge.

Equifax: 888-766-0008; 800-685-1111

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Experian: 888-397-3742

<https://www.experian.com/fraud/center.html>

TransUnion: 800-680-7289; 888-909-8872

<http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page>

- Order your credit reports. You can order your reports from the three credit reporting agencies for free by calling 1-877-322-8228 or going to www.annualcreditreport.com. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours. If you find anything suspicious, call the credit reporting agency at the phone number on the report.

- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.
- Review the explanation of benefits (EOB) statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement.
- Information about Identity Theft and steps to avoid identity theft are available at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Telephone: (202) 326-2222
FTC identity theft hotline: 877-438-4338
Website: <https://www.ftc.gov/idtheft>

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
Telephone: 410-576-6300 / En español 410-230-1712 / toll-free: 1-888-743-0023
Website: <https://www.marylandattorneygeneral.gov/>

To help ensure that your information is not used inappropriately and to lessen the harm this may cause you, IDF is providing you with access to complimentary identity protection services. Information about this service is enclosed with this letter.

As required by law, IDF will provide notice of the breach to the Office of Civil Rights and the Maryland Office of the Attorney General.

IDF sincerely apologizes for the inconvenience and concern this incident causes you. Your information privacy is very important to us and we will continue to do everything we can to improve protections for you and others.

You may contact us with questions and concerns by calling our Privacy Officer at (410) 468-0900 x 318 between the hours of 9 a.m. and 5 p.m., Monday to Friday; sending an e-mail message to csimon@idfdn.org; or, addressing a letter to our postal address:

IDF-Parkview Center
Attn: Privacy Officer
840 Hollins Street
Baltimore MD 21201

Sincerely,

Christopher Simon
Privacy Officer
410-468-0900 x318

Information about complimentary identity protection services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [##] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 is available to you for [##] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [##]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** [Enrollment End Date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code**: [Activation Code]

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 [Enrollment End Date]. Be prepared to provide engagement number [B#####] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [##]-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, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** 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.

* 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.