Corridor Capital

12400 Wilshire Boulevard · Suite 645 · Los Angeles, CA 90025 · www.corridorcapital.com

May 14, 2022

[redacted]

Re: Notice of Dynamo Software Data Security Incident

Dear [redacted],

Protecting the personal and financial information of our limited partners is a priority at Corridor Capital ("Corridor"). In this regard, we are writing to inform you of a recent incident which took place at Dynamo Software ("Dynamo"), a third-party vendor engaged by Corridor for its cloud-based customer relationship management (CRM) services. Dynamo, founded in 1998 and backed by Francisco Partners, is a SOC 1 and SOC 2 compliant, leading provider of cloud-based CRM services for alternative asset managers. Although we have no evidence that your personal information has been misused, we are writing to make you aware of this security incident so that you may take any necessary precautions.

What Happened?

Corridor learned of a data security incident at Dynamo on April 28, 2022. We understand that on April 27, 2022, Dynamo detected suspicious activity on its US-based servers which was determined to be a ransomware attack. In a ransomware attack, a cybercriminal typically encrypts a victim business' data and demands payment of a ransom in order to make the data once again available to the business.

Upon noticing the suspicious activity on its servers Dynamo states that it took its systems offline while the suspicious activity was investigated, and systems were restored. Dynamo informed Corridor the company engaged leading cybersecurity consultants and reported the incident to law enforcement. This notification was not delayed as a result of the law enforcement investigation. Dynamo shared that it was contacted by the bad actors and upon receiving proof of the data in their possession, including data allegedly associated with Corridor, paid the ransom. Thereafter, the bad actors allegedly informed Dynamo they had deleted the misappropriated data.

Dynamo informed Corridor that the company has also engaged another third-party service which is searching the dark web for any data taken from the security incident and have stated to date they have not found such data on the dark web. An independent investigation into the incident is reported to be currently underway.

Dynamo continues to be operational and has stated that it has implemented enhanced security measures in response to the incident, including:

- Engaging leading cybersecurity partners and new vendors to mitigate vulnerability areas;
- Modifying perimeter entry security settings;
- Strengthening access control and authentication protocols;
- Expanding the deployment of interior network traffic monitoring and alerting tools;
- Enabling 24×7 monitoring service via a leading third-party cybersecurity company;
- Initiating multiple exterior and interior scanning processes using different tools to provide overlapping coverage; and
- Enhancing supervision of security operations using internal and partner resources.

What Information Was Involved?

The personal information potentially accessed through Dynamo appears to include information contained in certain old fund K-1s which consists of name, address and Social Security number or Employer

Identification number. The potential access also appears to involve certain fund subscription agreements which consist of name, address, Social Security number or Employer Identification number, email address, phone number, bank account number and bank routing number.

However, as noted, there is no evidence or confirmation that any personal information was actually misused. Nevertheless, as a precautionary measure, we wanted to notify you so that you can take steps to protect your information.

What We Are Doing

Corridor acted promptly to respond to the security incident when we were notified by Dynamo and continues to coordinate with Dynamo regarding its response to the attack. Corridor conducted a search of its data stored in the CRM and is removing all documents containing personal information.

Months before the security incident, Corridor engaged Drawbridge Partners ("Drawbridge"), a provider of cybersecurity services and risk assessments, and IQ-EQ formerly known as Greyline Partners, a compliance consultant. Based on Drawbridge and IQ-EQ advice, Corridor had already put in place enhanced cybersecurity policies and measures. Under these advisors' guidance, Corridor continues to actively work on enhancing cybersecurity protocols particularly surrounding the privacy processes, security due diligence and contractual requirements Corridor imposes on its vendors to prevent cybersecurity incidents.

As a courtesy, Dynamo is providing Corridor limited partners with identity protection services, at no cost to Corridor limited partners, through IDX, a data breach and recovery services expert. IDX identity protection services include **12-months** of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

If you have questions about these services, please call Kerry-Anne Dinwoodie at Corridor.

We encourage you to enroll in free IDX identity protection services by going to https://app.idx.us/account-creation/protect or calling 1-800-939-4170 and using the Enrollment Code **P5WZ2DJ7H5**. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is September 12, 2022.

What You Can Do

Because in some cases personal information that was compromised could be utilized to submit a fraudulent capital call, please exercise caution in responding to capital call requests. Corridor does not send capital calls in the form of a PDF but rather an email presented with a link to AltaReturn, a password protected portal. The link has been and will continue to be https://corridorcapital.altareturn.com/. Should you receive a suspicious capital call request, please reach out to Kerry-Anne Dinwoodie.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports periodically. You also may want to consider placing a security freeze on your credit files. A freeze prevents an unauthorized person from using your personal identifying information to open new accounts or borrow money in your name.

Regardless of whether you take advantage of the complimentary identity theft protection and credit monitoring services that Dynamo is offering, we encourage you to consider these additional measures to monitor and protect your personal information and to remain vigilant for potential incidents of fraud and identity theft:

- Obtain a free credit report from each of the three national consumer credit reporting companies (Equifax, Experian, and TransUnion) by calling (877) 322-8228 or by logging on to www.annualcreditreport.com.

- Consider placing a "fraud alert" on your credit file to ask creditors to contact you before they open any new accounts or change your existing accounts. This request, which can be made from any of the three national consumer credit reporting companies, can help detect any possible misuse of your personal information. The initial fraud alert is active for 90 days and can be renewed.

- Consider placing a "security freeze" on your credit files. A freeze prevents an authorized person from using your personal identifying information to open new accounts or borrow money in your name. You will need to contact the three national consumer credit reporting companies at the toll-free telephone numbers or websites listed below. Under Section 301(a)(2) of the Economic Growth, Regulatory Relief, and Consumer Protection Act, you have the right to place (and remove) a security freeze on your credit report free of charge. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

  Equifax
  P.O. Box 105069
  Atlanta, GA 30348
  (800) 525-6285
  www.equifax.com

  Experian
  P.O. Box 4500
  Allen, TX 75013
  (888) 397-3742
  www.experian.com

  TransUnion
  P.O. Box 105281
  Atlanta, GA 30348
  (800) 680-7289
  www.transunion.com

- Regularly monitor your financial accounts and, if you see any unfamiliar activity, promptly contact your financial institution.

- The FTC website has further information regarding preventing fraud and identity theft, including additional information about "fraud alerts" and "security freezes," and about how to monitor and protect your credit and finances:

  Federal Trade Commission
  600 Pennsylvania Avenue, NW
  Washington, D.C. 20580
  (202) 326-2222
  1-877-382-4357
  www.consumer.ftc.gov/features/feature-0014-identity-theft
  www.IdentityTheft.gov

- If you have not already filed your most recent tax return, consider filing your tax return electronically at the earliest convenience. If your electronic return has already been filed, that may dissuade perpetrators from attempting to file a fraudulent return in your name.

- The Internal Revenue Service provides information in the event that tax-related identity theft may be suspected: https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft

- In addition, the Internal Revenue Service offers victim assistance at: https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works

- If you believe you have been the victim of identity theft, you should report the identity theft to local law enforcement, including your local police office, the state Attorney General, and/or the FTC.

- If you are a resident of North Carolina, you should also consider obtaining information from the North Carolina Attorney General about preventing identity theft:

Josh Stein
North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
1-877-566-7226
www.ncdoj.gov

- If you are a resident of Maryland, you may contact the Office of the Maryland Attorney General for more information about how you can protect your personal information.

  Maryland Office of the Attorney General
  Attn: Security Breach Notification
  200 St. Paul Place
  Baltimore, MD 21202
  (410) 576-6574
  https://www.marylandattorneygeneral.gov

For More Information

We understand that this incident may pose an inconvenience to you, and we sincerely regret that this situation has occurred. Corridor is committed to protecting the privacy and security of your personal and financial information, and we want to assure you that we have implemented appropriate measures to safeguard that information.

If you have any questions regarding this incident or if you desire further information or assistance, please contact us at craig@corridorcap.com / (310) 442-7001 or kerry-anne@corridorcap.com / (310) 442-7000 ext. 7015.

Sincerely,

Craig Enenstein
Chief Executive Officer

Kerry-Anne Dinwoodie
Chief Compliance Officer