





## MG Stover - Security incident notification

  
  
  
 1 attachments (33 KB)

Preventing Identity Theft and Fraud.pdf;

September 29, 2023

RE: Notice of Data Incident

Dear Investor,

We want to inform you of a security incident impacting MG Stover, fund administrator for Off the Chain LP. Retool, a managed service provider used by MG Stover, was recently the victim of a security incident where an unauthorized party gained access to MG Stover's account/system within Retool's managed service. Retool is used by MG Stover to develop internal business applications and integrate data originating from their fund accounting applications.

### What Happened?

On Wednesday September 20, 2023, MG Stover learned that the unauthorized party had gained unauthorized access to administrator account at Retool, which enabled the unauthorized party gain access to all Retool managed service customers' systems. Retool demonstrated to MG Stover that they successfully contained the incident and terminated all unauthorized access. MG Stover's company network was not affected and has not been compromised. On Friday September 22, 2023, MG Stover discovered that the attacker was able to query data from the customer systems connected to Retool which contained sensitive data.

### What Information Was Involved?

The potentially exposed information may have included your name, mailing address, email address, phone number, date of birth, and social security number and/or tax identification number.

### What We Are Doing

Upon being notified of the breach, MG Stover immediately began an internal investigation and took actions to 1) review all Retool user accounts and 2) assess the impact of the event. Retool demonstrated to MG Stover that they had successfully contained the incident and terminated all unauthorized access.

Retool took actions to terminate the relationship with the third-party contractor for whom the breached individual support person worked. In addition, they changed the process to add devices to the VPN to require a human-in-the loop manual review with administrator approval and synchronous verification of the employee's government ID. Further, Retool disabled user-level updates that enable support flow and implemented database-level constraints for updating critical user-level properties, restricting even the support team from performing these actions. Retool has also added requirement for hardware keys in order to access any admin-level tooling, regardless of location. Vendors must meet this requirement.

MG Stover has rotated the credentials of the breached user, enabled MFA for all users, reviewed all user activity logs within Retool, reviewed other managed services with sensitive data access, and initiated review of data access to ensure minimal sensitive data exposure to Retool. Finally, MG

Stover has initiated evaluation of alternative service providers to Retool.

MG Stover ensured that its company network and other 3rd party applications were not affected and have not been compromised.

#### What You Can Do

While it cannot be proven from the Retool logs that any MG Stover data was exported, we must assume that an attacker of this sophistication was able to successfully exfiltrate the data. As such, you should be on heightened alert and aware of any suspicious activity, including phishing emails.

MG Stover will be providing all affected investors and interested parties whose information may have been compromised with identity monitoring services. Arrangements for the services are still being completed and we will be sending a follow up notification with detailed instructions on how to activate your complementary identify monitoring. Please continue to be vigilant about the security of your personal accounts and monitor them for unauthorized activity. Please report any suspicious activity to appropriate law enforcement or your state Attorney General.

#### For More Information

Please review the enclosed attachment called Preventing Identity Theft and Fraud for more information about how to protect your personal information.

Again, we take your privacy seriously and regret any concern or inconvenience this incident may cause you. If you have additional questions, please contact us at: [ir-notifications@mgstover.com](mailto:ir-notifications@mgstover.com)

Sincerely,  
MG Stover Information Security

## *Preventing Identity Theft and Fraud*

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Immediately report any suspicious activity to your bank or credit union. If you do find suspicious activity on your credit reports or other statements, call your local police or sheriff's office, or state Attorney General and file a report of identity theft. You have a right to a copy of the police report, and you may need to give copies of the police report to creditors to clear up your records and access some services free to identity theft victims.

Under the U.S. Fair Credit Reporting Act and other laws, you have certain rights that can help protect yourself from identity theft. Many of these are explained in this letter and at [www.identitytheft.gov/#/Know-Your-Rights](http://www.identitytheft.gov/#/Know-Your-Rights). For example, you are entitled to one free credit report annually from each of the three major credit reporting agencies. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free at 1-877-322-8228. You may also contact the three major credit reporting agencies directly to request a free copy of your credit report.

In addition, at no charge, you can have these credit bureaus place a short-term or an extended "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because a fraud alert tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. Once one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. If you wish to place a fraud alert or have any questions regarding your credit report, please contact any one of the agencies listed below. Please note no one except you is allowed to place a fraud alert on your credit report.

General contact information for each agency:

Equifax P.O. Box 105069 Atlanta, GA 30348-5069 1-866-349-5191 <a href="http://www.equifax.com">www.equifax.com</a>	Experian P.O. Box 9554 Allen, TX 75013 888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	TransUnion P.O. Box 2000 Chester, PA 19016-2000 800-888-4213 <a href="http://www.transunion.com">www.transunion.com</a>
--	--	---

To add a fraud alert:

Equifax	(888) 202-4025, Option 6 or	<a href="https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/">https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/</a>
Experian	(714) 830-7000, Option 2 or	<a href="https://www.experian.com/fraud/center.html">https://www.experian.com/fraud/center.html</a>
TransUnion	(800) 916-8800, Option 0 or	<a href="https://www.transunion.com/fraud-alerts">https://www.transunion.com/fraud-alerts</a>

You may also place a security freeze on your credit reports, free of charge. A security freeze, also known as a "credit freeze," prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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. Unlike a fraud alert, you must place a security freeze separately on your credit file at each bureau. You can use the following addresses and contact information to place a security freeze with each major credit bureau:

**Equifax Security Freeze.** 1-888-298-0045. P.O. Box 1057881, Atlanta, GA 30348-0241.  
[www.equifax.com/personal/credit-report-services/credit-freeze](http://www.equifax.com/personal/credit-report-services/credit-freeze);

**Experian Security Freeze.** 1-888-EXPERIAN or 1-888-397-3742. P.O. Box 9554, Allen, TX 75013.  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html); or

**TransUnion.** 1-800-680-7289. Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19016-2000.  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

The Federal Trade Commission also provides additional information about credit freezes here:  
<https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

In order to request a security freeze, you may need to supply your full name (including middle initial, as well as Jr., Sr., II, III, etc.), date of birth, Social Security number, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or another statement to show proof of your current address. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning your identity theft.

The credit reporting agencies must place a security freeze on your credit report within one (1) business day after receiving a request by phone or secure electronic means and within (3) business days after receiving your request by mail. The credit bureaus must then send written confirmation to you within five (5) business days of placing the security freeze, along with information about how to remove or lift the security freeze in the future.

You can further educate yourself regarding identity theft, fraud alerts, freezes, and the steps you can take to protect yourself by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission encourages those who discover their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement or your state Attorney General.

The Federal Trade Commission can be reached at:

Federal Trade Commission  
Consumer Resource Center  
600 Pennsylvania Avenue NW  
Washington, DC 20580  
1-877-ID-THEFT (1-877-438-4338)  
TTY: 1-866-653-4261  
[www.identitytheft.gov](http://www.identitytheft.gov) or [www.ftc.gov](http://www.ftc.gov)

## **OTHER IMPORTANT INFORMATION**

You may obtain information about avoiding identity theft from the relevant regulators of your state of residence, including:

### **California residents:**

You can visit the California Attorney General's site ([www.oag.ca.gov/idtheft](http://www.oag.ca.gov/idtheft)) for information on protection against identity theft.

### **Maryland residents:**

You may obtain information about avoiding identity theft at: Office of the State of Maryland Attorney General, 200 St. Paul Place Baltimore, MD 21202; phone: 1-888-743-0023; [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov).

### **New York residents:**

The Office of the Attorney General may be reached at The Capitol, Albany, NY 12224-0341; phone: 1-800-771-7755; [ag.ny.gov](http://ag.ny.gov)

### **North Carolina residents:**

You may obtain information about avoiding identity theft at: North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001; phone: 919-716-6400; [ncdoj.gov](http://ncdoj.gov)

### **Colorado, Georgia, Maine, Maryland, Massachusetts, and New Jersey residents:**

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).