



December 23, 2020

Name  
Address  
Address

## NOTICE OF SECURITY INCIDENT

Dear [NAME] / [INVESTOR]:

We write to advise you of a cybersecurity incident (the “Incident”) that NetGain Technology (“NetGain”), a third party vendor that our fund administrator PKF O’Connor Davies (“ODA”) uses to host its servers discovered in December 2020. This Incident, which we recently learned about, impacted servers that store 747 Capital data for our funds and individual investors. We take the privacy and security of our investors very seriously and regret having to advise you that this Incident occurred. The Incident and the measures you can take to protect your information, are described in more detail below and in the attachment to this letter.

### What Happened?

NetGain is a cloud storage and data hosting provider headquartered in St. Cloud, Minnesota. 747’s fund administrator, ODA, utilizes NetGain’s hosting services to store 747’s data. In November, NetGain was the victim of a cyber incident that impacted its systems. To contain the impact and possible spread of infection, NetGain took its systems offline, which caused a temporary disruption to ODA’s business operations.

NetGain has engaged a leading cybersecurity firm to assist with its remediation efforts and to conduct a forensics investigation to determine the nature and scope of the Incident. Based on the investigation, it appears the threat actor initially gained access to ODA’s hosted environment on November 8, 2020. Between November 10 and November 23, 2020, the threat actor deployed various tools associated with the exfiltration of data, and on December 3, 2020, the threat actor began encrypting files.

### What Information Was Accessed?

ODA has advised that data hosted on behalf of 747 Capital (including data related to individual investors) may have been accessed in an ODA work environment by the attackers. It appears that this data may include personal information contained in Subscription Documents (e.g., individual’s name, address, bank account information, Social Security Numbers, and/or tax documents including W-9s).

The cybersecurity firms engaged by ODA and NetGain are continuously monitoring the Dark Web for any such information. To date, there is no indication that any data accessible by the threat actor has been published on the Dark Web or elsewhere, and we are unaware of any misuse of any individual investors’ personal information.

### What Are We Doing?

Since the initial notice of the Incident, 747 has been in contact with ODA to uncover more information about the Incident and its impact on you and our other investors. ODA and NetGain have been in continuous communications with cybersecurity professionals to mitigate the risk of harm to their systems and minimize the compromise of any client data. ODA has engaged its own cybersecurity firm to aid in these remediation measures. ODA has also assured 747 Capital that remedial measures, such as deploying threat-detecting tools across its environment and rotating all user credentials, have been undertaken.

Based on the information provided by ODA, it is our understanding at this time that 747 Capital’s Investor Portal (which is managed by ODA and hosted by NetGain) was not breached as a result of this cybersecurity incident. However, investor information may have been present in a separate ODA work environment that may have been accessed as part of this Incident. Thus, out of an abundance of caution, we have instructed ODA to reset every

880 Third Avenue, 17<sup>th</sup> Floor  
New York, NY 10022, USA  
[www.747capital.com](http://www.747capital.com)  
Tel: +1 212 747 7474

investor's password for the Portal. Upon learning of the Incident, 747 Capital immediately engaged Greenberg Traurig to assist with handling 747's obligations in relation to the Incident.

### **What Can You Do?**

We encourage you to be vigilant by regularly reviewing your account statements and online activity. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.

- Use Tools From Credit Providers. Carefully review your financial reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police.
- Reset Your Password. We have also required all affected users to reset their passwords. If you have not done so, please reset your password information as soon as possible.

Attached to this letter is more information about additional steps you can take to protect against the misuse of your personal information.

### **Free Credit Monitoring.**

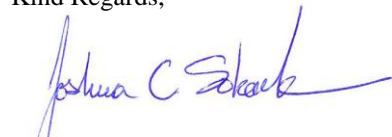
747 Capital is offering you 24 months of free credit monitoring and \$1,000,000 in identity theft insurance through Equifax. With Equifax ID Patrol, you will be provided with daily credit monitoring of your Equifax, Experian, and TransUnion credit files, daily access to your Equifax Credit Report, and an annual 3-in-1 Credit Report with your credit history as reported by the three major credit reporting agencies. **You must activate the Equifax ID Patrol by 11:59 p.m. ET on April 30, 2021, in order for it to be effective.** To activate, go to [www.myservices.equifax.com/patrol](http://www.myservices.equifax.com/patrol) and enter your activation code: **<Enter Activation Code>**. There is a 4-step enrollment process, which includes identity authentication. You will be asked a series of questions regarding your credit file that you must answer accurately to activate the product.

### **For More Information.**

You may contact us with questions and concerns about the potential unauthorized access of your personal information. You may email [Joshua@747capital.com](mailto:Joshua@747capital.com) for any questions you may have, or you may contact us at 1-212-747-7474.

We take our role in safeguarding all investor personal information very seriously, and we apologize for any inconvenience this may have caused you. Should you have any questions regarding this notice or if you would like more information, please do not hesitate to contact us.

Kind Regards,



Joshua C Sobek  
Partner, The 747 Capital Team

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

### Fraud Alerts and Credit or Security Freezes

**Fraud Alerts:** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

**Credit or Security Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company (Experian, TransUnion, and Equifax). After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password.

- Experian Security Freeze, PO Box 9554, Allen, TX 75013 | 1-888-397-3742 | <https://www.experian.com/freeze/center.html>
- TransUnion Security Freeze, P.O. Box 160, Woodlyn, PA 19094 | 1-888-909-8872 | <https://www.transunion.com/credit-freeze>
- Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348 | 1-800-349-9960 | <https://www.equifax.com/personal/credit-report-services/>

**How to Request a Security Freeze:** To request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail: (1) 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, the addresses where you have lived over the prior five years; (5) proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed; (6) a legible photocopy of a government issued identification card, such as a state driver's license or ID card, military identification, etc.; (7) social security card, pay stub, or W2; and (8) if you are a victim of identity theft, include a copy of either your police report, investigative report, or complaint to a law enforcement agency.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

**How do I lift a freeze?** A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. You will need your PIN to lift the freeze. If the request is made online or by phone, a credit bureau must

lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

### **Your Rights Under the Fair Credit Reporting Act**

The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below:

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit “prescreened” credit and insurance offers based on information in your credit report.
- You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

### **Additional Information for Residents of the Following States:**

**Connecticut:** You may contact and obtain information from your state attorney general at: Connecticut Attorney General’s Office, 165 Capitol Ave., Hartford, CT 06106 | 1-860-808-5318 | [www.ct.gov/ag](http://www.ct.gov/ag)

**Maine:** You may contact the Maine Attorney General Consumer Protection Division by phone at: 207-626-8849, or online at: [consumer.mediation@maine.gov](mailto:consumer.mediation@maine.gov).

**Maryland:** You may contact the Maryland Attorney General’s Office using the following methods: By U.S. Mail at: Office of the Attorney General, Attn: Security Breach Notification, 200 St. Paul Place, Baltimore, MD 21202 | By Fax to Attn: Security Breach Notification, 1-410-576-6566 | By Email: [ldtheft@oag.state.md.us](mailto:ldtheft@oag.state.md.us)

**Massachusetts:** Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Attorney General, Consumer Advocacy & Response Division, One Ashburton Place, 18th Floor, Boston, MA 02108 | 1-617-727- 8400 | [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html)

**New Jersey:** The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) is the state’s one-stop shop for cybersecurity information sharing, threat intelligence, and incident reporting. For general inquiries or to speak with an analyst, call us at 1-833-4-NJCCIC or send an email to [njccic@cyber.nj.gov](mailto:njccic@cyber.nj.gov)

**New York:** You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001 | 1-518-474-8583 | 1-800-697-1220 | <https://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341 | 1-800-771-7755 | <https://ag.ny.gov>