CHANNEL
YOUR PARTNER IN FUNDING

October 9, 2023

Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

RE: Data Security Event

Channel Partners Capital LLC ("Channel") is submitting this notice to provide your office with information regarding a cybersecurity event at one of its vendors that likely resulted in unauthorized access to consumer personal information ("PI"). Channel is a financial services company that provides small businesses with business capital loans and is headquartered in Minnetonka, Minnesota.

Channel contracts with CBIZ to provide data verification services related to its business capital loan service offering. Channel is required to verify the identities and other information of its clients in connection with its securitization transactions, and provides CBIZ with certain personal information related to the guarantors of business loans for that purpose. CBIZ, a leading vendor in this space, uses a software platform called MOVEit Transfer to securely transfer this personal information. On May 31, 2023, Progress Software, the provider of MOVEit Transfer software, publicly disclosed a zero-day vulnerability in their software that had been exploited by an unauthorized third party who was able to download files from MOVEit Transfer. On September 25, CBIZ informed Channel that the incident affected Channel personal information processed by CBIZ. Based on the information provided by CBIZ and an internal investigation by Channel, Channel determined that copies of driver's licenses for 11 individuals, including one individual in Maryland, were acquired by the third party. According to public and government sources, the unauthorized third party is a cybercriminal group called CL0P.

The incident was limited to the MOVEit Transfer portal used by CBIZ; Channel's internal networks and systems were not compromised. CBIZ is notifying all affected individuals, including Channel customers and guarantors, and providing 12 months of complimentary credit monitoring and identity theft protection through Kroll.

At this time, we consider the incident to be resolved.

Should you have any questions please do not hesitate to contact our outside counsel: Michael Bahar (MichaelBahar@eversheds-sutherland.com or +1.202.383.0882) or Alexander Sand (AlexanderSand@eversheds-sutherland.com or +1.512.721.2721).

Thank you,

Troy C. Kepler
Corporate Counsel
Channel Partners Capital LLC

[CBIZ Logo]

<<Return Mail Address>>

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>> <<Date>>

Dear <<Name 1>> <<Name 2>>,

CBIZ, Inc. is providing notice of a global data incident involving MOVEit Transfer software, which is used by many prominent organizations around the world. CBIZ and its customers, including <<DataOwner>>, used MOVEit Transfer to securely transfer files. <<DataOwner>>'s systems were not involved in this incident. This letter provides you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On May 31, 2023, Progress Software, the provider of MOVEit Transfer software, which is used by global organizations, disclosed a zero-day vulnerability in their software that had been exploited by an unauthorized third party who was able to download files from MOVEit Transfer. CBIZ and its customers utilize MOVEit Transfer in the regular course of business operations to securely transfer files. CBIZ promptly launched an investigation, with the assistance of cybersecurity professionals, into the nature and scope of the MOVEit Transfer vulnerability. That investigation determined that an unauthorized party exploited the vulnerability and downloaded files from CBIZ's MOVEit Transfer server.

What Information Was Involved? Our investigation determined that one or more files involved contained your <<DataElements>>.

What We Are Doing. CBIZ takes the responsibility of safeguarding your information very seriously. We have patched the identified vulnerability on our MOVEit Transfer server, and reviewed the protocols we have in place with our vendors to help prevent something like this from happening again.

As a precaution, we are offering you one year of free identity theft protection services through Kroll. You will not be billed for this service. The identity monitoring services we are making available to you include credit monitoring, fraud consultation and identity theft restoration. These services will expire at the conclusion of the complimentary period and will not automatically renew. For more information on identity theft prevention and Kroll Identity Monitoring, including instructions on how to activate your complimentary membership, please visit the below website and see the pages that follow this letter.

> Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.
> *You have until <<**Date**>> to activate your identity monitoring services.*
> Membership Number: <<**Member ID**>>

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the enclosed *Additional Steps You Can Take*, which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the free credit monitoring services that we are offering.

For More Information. If you have additional questions, you may call our toll-free assistance line at <<Call Center Number>> Monday through Friday from 9:00 am to 6:30 pm Eastern time (excluding U.S. holidays).

Sincerely,

CBIZ, Inc.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 over the next 12 to 24 months. 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 or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately 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. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

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.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

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 is because most creditors need to see your credit report before they approve a new account. If they cannot see your report, they may not extend the credit.

How do I place a freeze on my credit reports? 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. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com
- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com

You will need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the 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. 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.

The business address for CBIZ, Inc. is PO Box 31420, Independence, OH 44131, and CBIZ can be reached by telephone at (216) 447-9000.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

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, 518-474-8583 / 1-800-697-1220, http://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

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves [X] individuals in Rhode Island. Under Rhode Island 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: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of 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. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- 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” offers of credit and insurance you get 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.