GT GreenbergTraurig

July 10, 2023

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
attorneygeneral@doj.nh.gov

Re: Notification of Security Incident

Dear Attorney General Formella:

We are writing to inform you that our client, Accelya Topco Limited ("Accelya") is notifying 1 individual who resides in New Hampshire of a data security incident that may have impacted some of their personal information.

On May 31, 2023, Progress Software announced a previously unknown (Zero-Day) vulnerability affecting its MOVEit Transfer application, which is utilized by thousands of companies worldwide. Alight, a vendor supporting Accelya in its HR software migration, utilizes this application for managed file transfers and other business purposes. This Zero-Day vulnerability has impacted thousands of organizations across all industries and in many geographies around the world. Importantly, Accelya does not itself utilize MOVEit, and its corporate systems remain unaffected by this issue. Alight has advised that its forensic investigation was unable to conclusively determine if Accelya's data was affected by this incident; accordingly, Accelya is notifying employees in an abundance of caution.

The U.S. Accelya employees' personal information potentially accessed could include some or all of the following: ,
other demographic information, and certain job and salary information.

Accelya initially provided notice via email to all potentially affected individuals on June 14, 2023. Additionally, Accelya is mailing the attached notification letter in **Schedule A** to all potentially affected individuals on July 10, 2023.

Accelya currently has no indication that employee personal information faces an imminent risk of misuse, but they are providing all employees based in the U.S. with of complimentary identity protection services. These services provide enrollees with alerts for from the

date of enrollment when changes occur to any of one of their Experian, Equifax or TransUnion credit files. This notification is sent to them the same day that the change or update takes place with the bureau. Cyber monitoring will look out for their personal data on the dark web and alert them if their personally identifiable information is found online. In addition, Accelya is providing enrollees with proactive fraud assistance to help with any questions that they might have or in event that they become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. Please contact me for any additional information.

Best Regards,

Jena Valdetero
Shareholder

JMV:

Schedule A

Individual Notification Letter

Accelya Global Ltd
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07587

[Name]
[ADDRESS]
[ADDRESS]
[CITY, STATE,ZIP]

July 10, 2023

Dear [Name],

We are writing to follow up on our prior communications concerning the data security incident involving the MOVEit Transfer application (SecureFT) that may have impacted some of your personal information. We take the security of your information and any concern this incident may cause very seriously and are writing to provide additional information and resources to support you.

On May 31, 2023, Progress Software announced a previously unknown (Zero-Day) vulnerability affecting its MOVEit Transfer application, which is utilized by thousands of companies worldwide. Alight, a vendor supporting Accelya in our HR software migration, utilizes this application for managed file transfers and other business purposes. This Zero-Day vulnerability has impacted thousands of organizations across all industries and in many geographies around the world. Importantly, our corporate systems remain unaffected by this issue.

Alight has advised that it could not definitely determine if Accelya's data was removed from the MOVEit platform. Accordingly, out of an abundance of caution, we are notifying you and providing you with credit monitoring and identity theft protection services.

WHAT HAPPENED: After Progress Software's announcement on May 31st, Alight immediately began investigating to determine if it was among one of the thousands of Progress Software customers affected. Accelya followed suit, initiating a data review to determine what Accelya information may have been contained in the MOVEit files.

WHAT INFORMATION WAS INVOLVED: Our review determined that the MOVEit files contained

,

.

WHAT WE ARE DOING: Alight has assured us that, upon notification of Progress Software's Zero-Day vulnerability, they immediately took the application offline and applied the available patches issued by Progress Software to fix the vulnerability.

We currently have no indication that employee personal information faces an imminent risk of misuse, but we are providing all employees based in the U.S. with access to **Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score/Cyber Monitoring** services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

WHAT YOU CAN DO: To enroll in Credit Monitoring services at no charge, please log on to and follow the instructions provided. When prompted,

please input your unique code: In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

You may consider additional steps to help protect your information. It is advisable to review your credit reports and account statements over the next and notify your financial institution of any unauthorized transactions or incidents of suspected identity theft. If you identify any unauthorized activity on your account statements, you should immediately report those charges to your personal bank. You may also decide to freeze your credit or place a fraud alert on your credit profile. To initiate a credit freeze, contact each of the three national credit reporting agencies listed on the following page. Additional information is available at . Refer to the enclosed "Important Additional Information" for other precautions you can take.

FOR MORE INFORMATION: The security of our employees' personal information is a responsibility we take seriously. If you have any questions about this incident, please reach out to .

We deeply regret any concern or inconvenience this incident may cause you. Thank you for your continued commitment and understanding.

Sincerely,

Robert Wilson, Head of Legal
Funda Saltuk, Chief Human Resources Officer

Important Additional Information

For residents of *Iowa*: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:
You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

DC Attorney General	**Maryland Office of Attorney General**	**New York Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
400 6th Street NW	200 St. Paul Pl	120 Broadway, 3rd Fl	9001 Mail Service Ctr	150 South Main St
Washington, DC 20001	Baltimore, MD 21202	New York, NY 10271	Raleigh, NC 27699	Providence, RI 02903
1-202-727-3400	1-888-743-0023	1-800-771-7755	1-877-566-7226	1-401-274-4400
www.oag.dc.gov	https://www.marylandattorneygeneral.gov/	www.ag.ny.gov	https://ncdoj.gov/	www riag ri.gov

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

***Massachusetts and Rhode Island residents*:** You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies and have information relating to fraudulent transactions deleted. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or

password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
http://www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800