



James D. Snyder, Esq.
501 West Broadway, Suite 600
San Diego, California 92101
(619) 400-8000
(619) 238-8707 Fax
jsnyder@klinedinstlaw.com

August 18, 2023

VIA ELECTRONIC MAIL

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines IA 50319
consumer@ag.iowa.gov

Re: Notice of Data Security Incident

Dear Attorney General:

Klinedinst PC represents Alogent in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with the data breach notification statute.

Nature of the incident

On Wednesday, May 31, 2023, at approximately 2 pm ET, Alogent received notification from an Alogent vendor, Progress Software, developers of MOVEit Transfer, that a vulnerability was being used actively on the Internet to exploit a portion of their applications' functionality.

Alogent was informed, like many other Progress Software customers, that the SQL Injection vulnerability (CVE-2023-34362) could permit unauthenticated users' capabilities to escalate privileges or otherwise gain access to the environment. Upon receipt of the vulnerability information, the Alogent Incident Response Team immediately triaged the vulnerability to determine if Alogent or its customers were at risk. Alogent immediately implemented the recommended mitigations from CISA and Progress Software, disabling any HTTP/HTTPS access to the device to ensure that the system was not vulnerable to the potential exploit.

A data inventory was performed of the MOVEit Transfer system and it was found that data relating to some Alogent customer organizations ("Impacted Organizations") was present within that environment and accessed.

Alogent notified all such Impacted Organizations as promptly as was possible due to the investigation results on June 12, 2023. Alogent continues to work with Impacted Organizations in an attempt to mitigate any potential exposure to such organizations or their end user customers. To date, only one Impacted Organizations, The Huntington National Bank ("Huntington"), has accepted Alogent's offer to have Alogent issue notices to individuals impacted by the vulnerability.

Office of the Attorney General of Iowa
Hoover State Office Building
Re: Notice of Data Security Incident
August 18, 2023
Page 2

Alogent is unable to issue notices to individuals within the state without its Impacted Organizations' consent and assistance due to contractual restrictions with the Impacted Organizations and a lack of complete impacted individuals' contact information, and continues to try to work with its Impacted Organizations in an effort to ensure all such notices are issued promptly.

Please note that Alogent has already implemented additional security measures designed to prevent a recurrence of such an attack, and to protect the privacy of Alogent's customer data.

Approximate number of affected state residents:

Approximately 900 Iowa residents were affected by the breach based on Alogent's investigation results. Of this total, 136 residents were Huntington customers and are receiving the attached notice.

Consumer notices:

Enclosed is a copy of the notice sent to Huntington impacted consumers. Said notices were sent on Monday, August 14, 2023, via regular mail. Alogent continues to make attempts to work with all of its other Impacted Organizations in an effort to ensure all such notices are issued promptly or have been issued.

Services being offering to affected residents:

Alogent is providing impacted Huntington consumers with identity protection services including, credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. These services are being provides for at least 12 months but up to 24 months in some cases. Alogent continues to make attempts to work with its other Impacted Organizations in an effort to offer the same services to impacted individuals in the state.

Steps Alogent has taken or plans to take relating to the breach of the security of a system:

Alogent has discontinued the use of the MOVEit Transfer software after the compromise was discovered and is working to establish a new solution with improved security measures designed to mitigate risk in the future.

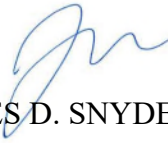
Contact information:

Alogent remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at jsnyder@klinedinstlaw.com or (619) 400-8000.

Office of the Attorney General of Iowa
Hoover State Office Building
Re: Notice of Data Security Incident
August 18, 2023
Page 3

Regards,

KLINEDINST PC

A handwritten signature in blue ink, appearing to read 'Jm', is positioned above the printed name.

JAMES D. SNYDER

Enclosure: Sample notice mailed to impacted consumer on August 14, 2023.

22994670.1

Logo/Client

<<Return Address>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call: [TFN] Or Visit: https://app.idx.us/account-creation/protect Enrollment Code: [XXXXXXXXXX]

To the Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

What Happened

This letter is written to inform you that between May 30, 2023 and June 1, 2023, Alogent Holdings, Inc. (“Alogent”), was victim of a zero-day vulnerability within one of their vendors software, Progress Software’s MOVEit Transfer application (CVE-2023-3462). A compromise of a server exposed data, which included account information, related to checks processed through Alogent’s customer, Huntington Bank.

What Information Was Involved

After reviewing the compromised files, it appears that some of your information may have been accessed by an unauthorized malicious third party. The data set included account and routing numbers, name, address, phone, check payee and remittance amount.

What Has Been Done

Alogent has discontinued the use of the MOVEit Transfer software after the compromise was discovered and is working to replace this solution, as well as to establish improved security measures to mitigate risk in the future.

What You Can Do

Alogent is offering identity theft protection services through IDX, A ZeroFox Company, a data breach and recovery services expert. IDX identity protection services include: 12 months (24 months where required by state regulations) of CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will work to help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling [TFN] or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Pacific Time. Please note, the deadline to enroll is [Enrollment Deadline].

Again, at this time, there is no evidence that your child’s information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives are fully versed on the incident and can answer questions or concerns you may have regarding protection of your child’s personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. You will need to reference the enrollment code at the top of this letter when calling or enrolling on online, so please do not discard this letter.

Please call [TFN] or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

Name
Client

(Enclosure)

DRAFT DO NOT DISTRIBUTE



Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Telephone. Contact IDX at [TFN] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

3. Watch for Suspicious Activity. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Security Freeze. You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below to place the freeze. 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. There is no cost to freeze or unfreeze your child's credit files.

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

DRAFT DO NOT DISTRIBUTE