SIDLEY

SIDLEY AUSTIN LLP
1501 K STREET, N.W.
WASHINGTON, D.C. 20005
+1 202 736 8000
+1 202 736 8711 FAX

AMERICA • ASIA PACIFIC • EUROPE

EMCNICHOLAS@SIDLEY.COM
+1 202 736 8010

June 25, 2018

By FedEx and Email

The Honorable Gordon J. Macdonald
Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Data Security Incident

Dear Attorney General Macdonald:

On behalf of our client, Capital Integration Systems LLC ("CAIS" or the "Company"), we are writing to notify you about a data security incident involving personal information maintained by CAIS. CAIS initially provided notice to known affected individuals and the relevant state regulators on March 22, 2018. Since then, CAIS continued its investigation and learned additional information about the scope of the incident.

The incident stems from one CAIS employee being the victim of an email phishing attack. The phishing attack appears to have taken place on or about February 1, 2018. Upon discovering this incident on March 15, 2018, CAIS conducted a forensic investigation and confirmed that no other company systems were affected. The phishing attack compromised a single Office 365 email account and did not compromise the integrity of the CAIS platform.

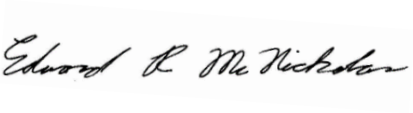
Through further investigation, CAIS has now identified approximately 19 New Hampshire residents who may have had their personal information available through the affected account. On June 22, 2018, CAIS began notifying these individuals. In total, approximately 2,321 individuals were determined to be potentially affected by this incident. As a precautionary measure, CAIS is also providing one year of credit monitoring and identity theft protection services to potentially affected individuals through AllClear ID, as described in the attached sample notice letter.

At this time, there continues to be no indication of financial fraud with any CAIS accounts. However, information that may have been available through the impacted employee credentials includes employee names, contact information, tax identification numbers, financial account information, and other information connected with CAIS financial services.

SIDLEY

CAIS will continue to provide regular reminders and annual training for employees on how to spot and avoid being victimized by phishing emails in the future. If you have any questions, please do not hesitate to contact me.

Respectfully submitted,



Edward R. McNicholas

CAIS

527 MADISON AVE., 2nd FLOOR, NEW YORK, NY 10022 +1 212 300 9350 CAISGROUP.COM

June 22, 2018

Notice Regarding Email Phishing

We are writing to share important information with you about an email phishing incident that may have affected your personal information, as well as steps we have taken in response to the incident and recommended actions you may wish to take.

A phishing attack is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal sensitive information, such as passwords or credit card numbers.

This phishing attack solely compromised a single CAIS employee's Office 365 email account and in no way compromised the integrity of the CAIS platform, which successfully undergoes rigorous annual auditing by the information security teams of Fortune 500 clients as well as penetration testing by an outside security firm retained by CAIS.

We should emphasize that we have no evidence confirming that this phishing incident has compromised any of your Personally Identifiable Information, however we are communicating with you as a precautionary measure in compliance with best practices.

What Happened?

An email account at a trusted vendor of CAIS was the subject of a phishing attack. On February 1, 2018, a CAIS employee received an email from the compromised account at the trusted vendor which appeared legitimate, thereby deceiving the CAIS employee and compromising the email account of such CAIS employee. Based on our forensic review of the incident, we believe that the attacker was able to access this employee's email account on February 19 via a web interface, as well as download email via an email client. The compromised email account was detected on February 22 by the CAIS Security Team.

Upon detection of the compromised email account, the following plan was put into action:

- The password on the compromised email account was changed immediately by the CAIS Security Team.
- Microsoft Office 365 Support was engaged immediately by the CAIS Security Team to assist in gathering details of the attack and to contain any further activity.
- Counsel and forensic experts at Navigant were retained to comprehensively understand the scope of the intrusion.

CAIS

527 MADISON AVE., 2nd FLOOR, NEW YORK, NY 10022 +1 212 300 9350 CAISGROUP.COM

- CAIS has implemented several new policies, procedures and security measures with respect to email access and handling of personally identifiable information in order to prevent any further exploits of this nature.

Data security is of paramount importance to CAIS. Our information security policies and practices meet and exceed those best practices and guidelines recommended for the wealth management industry. All CAIS personnel receive thorough annual security training including the identification and avoidance of phishing attacks, however, regrettably, the human element is not perfect and hence remains the weakest link in any security program. Industry analysis reports of phishing attempts in 2018 suggest the volume of phishing attacks has grown 65% in the last year and that 76% of businesses reported being a victim of a phishing attack in the last year.

What Information Was Involved?

It has been determined that the compromised email account contained certain elements of your Personally Identifiable Information. We should emphasize that while the CAIS employee's email account was compromised, we have no evidence confirming that the unauthorized individual has accessed any messages containing Personally Identifiable Information. For purposes of this communication, "Personally Identifiable Information" includes individual names, tax identification numbers, social security numbers, postal addresses and email addresses.

What We Are Doing.

Upon discovery of the incident, we blocked the intruder's access and conducted a forensic investigation. We are offering all affected individuals credit monitoring services at no charge. We have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice, and you can use them at any time during the next 12 months.

- AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-866-979-2595 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

- AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. In the event that you wish to avail yourself of this service, please contact inquiries@caisgroup.com in order to receive a redemption code and sign up online at **enroll.allclearid.com**.

CAIS

527 MADISON AVE., 2nd FLOOR, NEW YORK, NY 10022 +1 212 300 9350 CAISGROUP.COM

- Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may be required in order to activate your monitoring options.

What You Can Do.

We encourage you to regularly review your financial accounts and credit reports. You should remember to report any suspected incidents of fraud to us or the relevant financial institution.

We also have included an attachment listing additional steps you may wish to consider taking at any time if you ever suspect that you may have been the victim of identity theft. We offer this out of an abundance of caution so that you have information that may be helpful to you.

We take the security of your information very seriously. We truly regret any inconvenience this incident may cause you. If you have any questions and concerns, please do not hesitate to contact CAIS at inquiries@caisgroup.com.

Thank you for your patience and understanding.

Sincerely,

CAIS Executive Committee

CAIS

527 MADISON AVE., 2nd FLOOR, NEW YORK, NY 10022 +1 212 300 9350 CAISGROUP.COM

Important Identity Theft Information: Additional Steps You Can Take to Protect Your Identity

The following are additional steps you may wish to take to protect your identity.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies.

You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

- Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com
- Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742. www.experian.com
- TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. www.transunion.com

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud	1.888.766.0008
Experian:	Report Fraud	1.888.397.3742
TransUnion:	Report Fraud	1.800.916.8800

Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00, (or in certain states such as Massachusetts, no more than $5.00), each to place, temporarily lift, or permanently remove a security freeze.

CAIS

527 MADISON AVE., 2nd FLOOR, NEW YORK, NY 10022 +1 212 300 9350 CAISGROUP.COM

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the following addresses:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348
- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013
- TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Don't send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five 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.

To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include (1) proper identification (name, address, and Social Security number), (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze all together, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze.

The credit bureaus have three business days after receiving your request to remove the security freeze.

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 www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Suggestions If You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1.877.IDTHEFT (1.877.438.4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.
- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Take Steps to Avoid Identity Theft

Further information can be obtained from the FTC about steps to take to avoid identity theft through the following paths: http://www.ftc.gov/idtheft; call 1.877.IDTHEFT (1.877.438.4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at http://www.oag.state.md.us/idtheft/index.htm, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

CAIS

527 MADISON AVE., 2nd FLOOR, NEW YORK, NY 10022 +1 212 300 9350 CAISGROUP.COM

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a small fee to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at http://www.atg.state.vt.us.