INTL · FCStone®

INTL FCSTONE INC.
NASDAQ: INTL
www.intlfcstone.com

2 Perimeter Park South
Suite 100W
Birmingham, Alabama 35243
205-414-3313
andrew.chambless@intlfcstone.com

December 10, 2019

The Honorable Gordon MacDonald
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Ladies and Gentlemen:

I write on behalf of INTL FCStone, Inc. to inform you of a data security incident involving the personal information of certain current and former employees and clients, including approximately 28 residents of the State of New Hampshire.

On May 8, 2019, INTL FCStone detected that the email account of an email administrator was accessed by an unauthorized person. We immediately engaged leading data security firms to conduct a thorough investigation, and we believe the unauthorized activity is attributable to phishing emails received in April and May 2019. Working with these consultants, we successfully terminated the unauthorized person's access to our system on May 14. The consultants concluded that the incident implicated no systems beyond certain of INTL FCStone's email accounts and that the unauthorized person did not gain access to any account management or online customer database or server or other INTL FCStone system.

The investigation could not, however, conclusively rule out that information was accessed or removed from the affected email accounts. We thus immediately began working with a leading forensic firm to analyze the scope of any implicated information. This review and analysis took a substantial amount of time due to the unstructured nature and combined volume of items in the affected email accounts. Given this, the forensic firm did not provide us their report until late October, at which point we immediately began our analysis of the forensic firm's findings, which included supplementing their analysis with residency information. We completed this analysis on December 6th, 2019.

While, as noted above, we are unable to conclusively determine whether any information about the potentially implicated individuals was actually accessed or removed from the affected email accounts, we nonetheless decided, out of an abundance of caution, that it was appropriate to notify them that their personal information may have been implicated by the incident. This personal information may have included an individual's name, address, date of birth, Social Security number, driver's license number, passport number, INTL FCStone account number, and other information we collect or use in the ordinary course of our business.

At this time, all indications are that the unauthorized person has no further access to our email system. As always, we've been working with leading experts to enhance our security. We continue to monitor our systems for unauthorized access and have introduced additional security measures since the incident including, among other things, implementing multi-factor authentication for our email system. We have also coordinated with the Federal Bureau of Investigation to investigate the incident.

INTL FCStone expects to begin informing potentially affected individuals by U.S. mail on or about December 18th. A sample of that communication is enclosed. In addition to alerting these individuals, INTL FCStone is offering free credit monitoring services from ID Experts for 12 months.

If you have any questions about this incident, please do not hesitate to contact me at (205) 414-3313.

Yours truly,

Andrew R. Chambless
Counsel

Logo/INTL FCStone Inc.
C/O ID Experts
<<Return Address>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
[TFN]
Or Visit:
https://ide.myidcare.com/customending
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Breach

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

I am writing to let you know about a data security incident that may have affected certain information in our possession. We have no evidence that your personal information has been acquired or misused, but we are notifying you out of an abundance of caution to explain the circumstances as we understand them and to make you aware of the steps we have taken in response to the incident and the resources we are making available to you.

What Happened?

On or about May 8, 2019, we detected that the email account of an email administrator was accessed by an unauthorized person. We immediately engaged leading data security firms to conduct a thorough investigation, and we believe the unauthorized activity is attributable to phishing emails received in April and May 2019. Our investigation concluded that the incident implicated no systems beyond certain of the Company's email accounts and that the unauthorized person did not gain access to any account management or online customer database or server or other INTL FCStone systems. However, the investigation could not conclusively rule out that information was accessed or removed from the affected email accounts, and we thus immediately began working with a leading forensic firm to analyze the scope of any implicated information. The forensic firm delivered us their report on the incident in late October, and we completed our analysis of this report on December 6th, 2019.

Based on this investigation, we were unable to determine whether any information about you was actually accessed. Nonetheless, INTL FCStone has decided out of an abundance of caution that it is appropriate to notify you that information about you might have been affected.

What Information May Have Been Involved?

As noted above, we were unable to determine whether any information about you was actually accessed, but we have also not been able to rule out that your information was affected by this incident. Information that might have been implicated includes your name, address, date of birth, Social Security number, driver's license number, passport number, INTL FCStone account number, and other information we collect or use in the ordinary course of our business.

What We Are Doing

The safety of your personal information is of utmost importance to us. That's why, as soon as we discovered this incident, we took steps to understand its nature and scope and brought in external forensic consultants that specialize in cyber attacks. Working with these forensic consultants, we terminated the unauthorized person's access to our system on May 14, and all indications are that the unauthorized person has no further access to our email system. As always, we've been working with leading experts to enhance our security. We continue to monitor our systems for unauthorized access, have introduced additional security measures, and have coordinated with law enforcement to investigate the incident.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling [TFN] or going to https://ide.myidcare.com/customending and using the Enrollment Code provided above. **The Credit monitoring included in your membership must be activated to be effective.** MyIDCare experts are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is TBD.

In addition to enrolling in MyIDCare services and activating credit monitoring, we encourage you to review and monitor your account for suspicious activity. Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and report any suspected incidents of fraud to us or the relevant financial institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information.

Please refer to the enclosure entitled "Additional Ways to Protect Your Identity" for additional actions you should consider taking to protect yourself against fraud and identity theft.

For More Information

We take the security of your information very seriously and sincerely regret any inconvenience or concern. Our customers have always been our first concern and highest priority, and we are committed to protecting your information and maintaining your trust and confidence. Should you have questions or concerns, please do not hesitate to contact us at [TFN].

Sincerely,

(enclosure)

Important Notice

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some we suggest you consider:

Reviewing Your Accounts and Credit Reports

Federal regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax 1-800-525-6285 Equifax.com	**Experian** 1-888-397-3742 Experian.com	**TransUnion** 1-800-680-7289 Transunion.com

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report 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. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

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. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT

(438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft: A Recovery Plan*, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Special Information for Residents of Iowa, Maryland, Massachusetts, New Mexico, North Carolina, Oregon, Rhode Island, and Vermont

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.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with 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 its honoring your request.

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 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. 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.