LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS AT LAW

550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

RECEIVED
15 AUG 11 AM 10: 15
CONSUMER PROTECTION DIV.

JENNIFER A. COUGHLIN
DIRECT DIAL: 215.977.4081
JENNIFER.COUGHLIN@LEWISBRISBOIS.COM

August 7, 2015

Via First Class US Mail
Iowa Attorney General
Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319

Re: Notice of Data Event

Dear Sir/Madame:

In follow up to our July 31, 2015 communication, our office continues to represent SterlingBackcheck, 1 State Street Plaza, 24th Floor, New York, New York 10004. SterlingBackcheck provides background screening services to clients throughout the world, including to clients that request screening services be conducted on certain Iowa residents. We are providing notice to your office of an event that may impact the security of personal information relating to nine hundred and fifty-two (952) Iowa residents for whom SterlingBackcheck performed a screening service at the request or direction of a SterlingBackcheck client. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SterlingBackcheck does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

Background

SterlingBackcheck provides background screening services to clients located in, among other geographic areas, the United States, seeking background information relating to job applicants, volunteers, or professional affiliates ("candidates"). During provision of these services, SterlingBackcheck receives personally identifiable information of candidates, either directly from the candidates themselves or from the SterlingBackcheck clients to which the candidate is affiliated.

On May 29, 2015, a laptop used by a SterlingBackcheck employee was stolen from the employee's vehicle. SterlingBackcheck learned of the incident on May 30, 2015, notified law enforcement, and launched an investigation to determine the types of information that may have been stored on the laptop at the time of the theft and to whom this information relates.

While SterlingBackcheck's investigation into this event is ongoing, it has determined an Excel file containing the names, Social Security numbers, and dates of birth of certain candidates may have been stored

on the laptop at the time of the theft. SterlingBackcheck is unaware of any actual or attempted misuse of the personally identifiable information contained in this Excel file.

Notice to Iowa Residents

The names, Social Security numbers, and dates of birth of nine hundred and fifty-two (952) Iowa residents may have been stored on the laptop at the time of the theft. On or about the week of July 27, 2015, SterlingBackcheck provided notice of this event to its potentially impacted clients. Unless directed by the client to refrain from doing so, SterlingBackcheck began mailing written notice of this incident to these nine hundred and fifty-two (952) potentially impacted Iowa residents on or about August 5, 2015, in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

SterlingBackcheck's investigation into this incident is ongoing. SterlingBackcheck is offering those individuals impacted by this incident and to whom it is legally obligated or permitted to notify with access to two free years of credit monitoring and identity restoration services with AllClear ID and is providing these individuals with helpful information on how to better protect against identity theft and fraud. SterlingBackcheck is taking steps to mitigate the risk that an event like this happens again by, among other things, reviewing data security, privacy, technology, and asset inventory procedures, retraining its employees on data security and privacy protocols, and installing encryption and remote deletion software on mobile devices. In addition to providing notice of this incident to your office, SterlingBackcheck is providing notice of this incident to other regulators and consumer reporting agencies where required.

Contact Information

Should you have any questions regarding this notification or other aspects of this event, please contact us at 215-977-4081.

Very truly yours,

Jennifer A. Coughlin of
LEWIS BRISBOIS BISGAARD & SMITH LLP

JAC:sn

EXHIBIT A

SterlingBackcheck

Processing Center • P.O. BOX 141578 • Austin, TX 78714

00003
ACD1234
01153
John Q. Sample
1234 Main Street
Anytown US 12345-6789

August 7, 2015

Dear John Sample,

SterlingBackcheck provides background screening services to clients throughout the world, including to a client with which you recently applied for employment. As part of your application process, we received personal information relating to you, including your name, Social Security number, and date of birth. We recently discovered an incident that may affect the security of this personal information. While we are unaware of any actual or attempted misuse of this information, we are writing to provide you with information regarding the incident, steps we've taken since discovering the incident, and information on what you can do to better protect against identity theft and fraud should you feel it is appropriate to do so.

What Happened? On May 29, 2015, a password-protected laptop was stolen from a SterlingBackcheck employee's vehicle. The employee reported the theft to our office, and we launched an investigation to determine what information may have been stored on the laptop at the time of the theft. While our investigation is ongoing, we've determined a file containing your name, Social Security number, and date of birth may have been stored on the laptop at the time of the theft. **We are unaware of any actual or attempted misuse of this information, and there is no indication the data that may have been stored on the laptop was the target of the theft.**

What is SterlingBackcheck Doing? We take the security of your personal information seriously. In addition to launching the ongoing investigation into this incident, we have implemented additional measures to mitigate against the risk that an incident like this will happen again by updating our encryption and audit procedures, revising our equipment custody protocols, retraining employees on privacy and data security, and installing remote-wipe software on portable devices.

In addition to the steps above, we've provided notice of this incident to our potentially impacted clients and are coordinating with these clients to disclose this incident to its potentially impacted candidates and provide potentially impacted candidates with complimentary access to 24 months of free credit monitoring and identity restoration services with AllClear ID. The enclosed Privacy Safeguards Information contains instructions on how to enroll and receive these complimentary services, as well as additional information that can be used to better protect against identity theft and fraud. We are also providing notice of this incident to certain state regulators and consumer reporting agencies, as required.

What Can You Do? You can review the enclosed Privacy Safeguards Information. You can also enroll to receive the complimentary access to 24 free months of credit monitoring and identity restoration services. You can also contact the confidential inquiry line we've established relating to this incident. This confidential inquiry line is staffed with professionals familiar with this incident and knowledgeable

on what you can do to better protect against misuse of your information. This confidential inquiry line is available Monday through Saturday, 8:00 am – 8:00 pm Central Time, at 1-855-227-9823.

SterlingBackcheck takes your privacy and the security of your information seriously and sincerely regrets any inconvenience or concern this incident has caused you.

Sincerely,

Clare Hart

Clare Hart
CEO, SterlingBackcheck

PRIVACY SAFEGUARDS INFORMATION

To help detect the possible misuse of your information, we have arranged to have AllClear ID protect your identity for 24 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 24 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-227-9823 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-227-9823 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts.

You may also take action directly to further protect against possible identity theft or other financial loss. We encourage you to remain vigilant for incidents of fraud and identity theft by reviewing your account statements regularly and monitoring your credit reports for suspicious activity. Under U.S law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any question regarding your credit report, please contact any one of the agencies listed below:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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 bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files.

To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Fraud Victim Assistance
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834
1-800-685-1111	1-888-397-3742	Fraud Division
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	800-680-7289
www.equifax.com/help/credit-freeze/en_cp		www.transunion.com/freeze

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. **For Iowa residents**: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164; and online at http://www.iowaattorneygeneral.gov/. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. Instances of known or suspected identity theft should also be reported to law enforcement.