



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

AUG 03 2018

CONSUMER PROTECTION

Sian M. Schafle
Office: 267-930-4799
Fax: 267-930-4771
Email: sschafle@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

July 30, 2018

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

We represent Clarkson PLC, as well as its subsidiaries Clarksons Platou Futures Ltd., Genchem Holdings Limited, Clarkson Research Services Limited, Clarkson Port Services Limited, Clarkson Valuations Limited, Trustee(s) of the Clarkson PLC Pension Scheme, H Clarkson & Company Limited, and Clarkson Cloud Limited, (together, "Clarksons"), and write to notify your office of an incident that may affect the security of personal information relating to approximately three (3) New Hampshire residents. 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, Clarksons does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On November 7, 2017, Clarksons learned that it was the subject of a cyber security incident in which an unauthorized third party accessed certain Clarksons' computer systems in the UK, copied data, and demanded a ransom for its safe return. As soon as the incident was discovered, Clarksons took steps to respond to and manage the incident, including launching an immediate investigation into the nature and scope of the event, notifying regulators, working with third party forensic investigators, and informing law enforcement.

Through the forensic investigation, Clarksons quickly learned that the unauthorized third party had gained access to its system from May 31, 2017 until November 4, 2017. Clarksons learned that the unauthorized access was gained via a single and isolated user account. Upon discovering this access, Clarksons immediately disabled this account.

Through the investigation and legal measures, Clarksons were then able to successfully trace and recover the copy of the data that was illegally copied from its systems. While Clarksons were able to successfully trace and recover the copy of the data that was illegally copied from its systems, as a precautionary measure, Clarksons have also been working diligently, in cooperation with law enforcement and forensic investigators, to determine what data may have been involved. In an abundance of caution, Clarksons are notifying potentially affected individuals.

While the potentially affected personal information varies by individual, this data may include: name, date of birth, Social Security number, and address information.

Notice to New Hampshire Residents

On or around November 29, 2017, Clarksons provided preliminary notice of this incident to its employees globally, providing dedicated consultation for employees who had further questions. Additionally, on November 29, 2017, Clarksons provided notice of this incident to the Regulatory News Service in the United Kingdom.

On July 30, 2018, Clarksons will begin mailing written notice of this incident to potentially affected individuals, which includes approximately three (3) New Hampshire residents. Written notice will be provided in substantially the same form as the letter attached here as *Exhibit A*. Clarksons will also by posting notice of this event on its website, as well as issuing a national press release on or around July 30, 2018. These notices will appear in substantially the same form as the communications attached hereto as *Exhibits B* and *C*.

Other Steps Taken and To Be Taken

Upon discovering this incident, Clarksons immediately launched an investigation to determine the nature and scope of the event, as well as determine what data may potentially be affected and take steps to recover and/or delete any data acquired without authorization. The investigation included working with third-party forensic experts, as well as regulators and law enforcement. Clarksons is mailing written notice to those individuals whose data was present on the systems impacted by the event for whom it has address information. This notice will include guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Clarksons has and will continue to provide notice of this event to other state, federal, and international regulators as required by law.

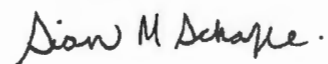
Clarksons has security measures in place to protect data in its care and is working diligently to enhance these protections and ensure the ongoing security of its networks. This has included putting in place additional security measures to best protect against a similar incident happening in the future and escalating certain planned enhancements as part of its wider cybersecurity review, which had already begun last year.

Office of Attorney General Gordon J. MacDonald
July 30, 2018
Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please do not hesitate to contact me at 267-930-4799

Very truly yours,



Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/mab
Enclosure

EXHIBIT A



Clarksons Platou

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Cyber Security Incident

Dear <<Name 1>>:

Clarkson PLC (“Clarksons” or “we”) write to inform you of a cyber security incident that may affect the security of some of your personal information. Clarksons take issues of IT security extremely seriously and by this letter is providing you with information and access to resources so that you can take further steps to best protect your personal information, should you feel it is appropriate to do so.

What Happened?

On November 7, 2017, Clarksons learned that it was the subject of a cyber security incident in which an unauthorized third party accessed certain Clarksons’ computer systems in the UK, copied data, and demanded a ransom for its safe return. As soon as the incident was discovered, Clarksons took steps to respond to and manage the incident, including launching an immediate investigation into the nature and scope of the event, notifying regulators, working with third party forensic investigators, and informing law enforcement.

Through the forensic investigation, Clarksons quickly learned that the unauthorized third party had gained access to its system from May 31, 2017 until November 4, 2017. We learned that the unauthorized access was gained via a single and isolated user account and we immediately disabled this account.

Through the investigation and legal measures, Clarksons were then able to successfully trace and recover the copy of the data that was illegally copied from its systems.

What Information Was Involved?

While Clarksons were able to successfully trace and recover the copy of the data that was illegally copied from its systems, as a precautionary measure, Clarksons have also been working diligently, in cooperation with law enforcement and forensic investigators, to determine what data may have been involved. In an abundance of caution, Clarksons are notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so.

Our investigation has determined that certain personal information was included in the data that was illegally copied from our computer systems. This may include your: <<Variable Data Text>>.

What We Are Doing.

We are sending you this letter because we take the security of your personal information very seriously. While we have enhanced security measures in place to protect data in our care and while we have notified the necessary regulatory and law enforcement bodies across the relevant jurisdictions, as a precautionary measure, we are also providing you with information about this event and about the further steps you can take to best protect your personal information, should you feel it appropriate to do so.

As an added precaution, we are also offering you access to one (1) year of identity protection services. These services are being offered at no cost to you and will be paid for by Clarksons. Should you wish to take further steps to protect your personal information, we would encourage you to enroll in these services by calling the number at the bottom of this letter. We are not able to enroll on your behalf.

What You Can Do.

Please review the enclosed "Steps You Can Take to Protect Your Information." You can also enroll to receive the identity protection services that we are offering at no cost to you.

For More Information.

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 888-785-1475, Monday through Friday, 9 a.m. to 9 p.m. Eastern Time, except holidays.

As part of our response to the incident, we have also published a statement on the news section of our website which is available at <https://www.clarksons.com/news/notice-of-cyber-security-incident-ckn/>.

Again, Clarksons take the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident may have caused you.

Sincerely,



Sandra Rosignoli
Group General Counsel | Clarkson PLC

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

We are offering you access to one (1) year of identity protection services. These services are being offered at no cost to you and will be paid for by Clarksons. Should you wish to enroll in these services please call our dedicated assistance line at 888-785-1475, Monday through Friday, 9 a.m. to 9 p.m. Eastern Time, except holidays. Our operators will be able to advise you as to the most appropriate service depending on the jurisdiction where you live.

Monitor Your Accounts

Personal Accounts. Where your financial or card related data may have been affected, we suggest that you consider monitoring any relevant accounts that you may have, including reviewing your personal account statements for any unusual or suspicious activity. If you do notice any suspicious activity, contact your account provider immediately.

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your personal account statements and monitoring your free credit reports for suspicious activity and to detect errors. 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. Contact information for the credit reporting agencies can be found below.

Fraud Alerts. At no charge, you can also have the three major 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 questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
800-680-7289
www.transunion.com

Security Freeze. 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, lift, 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. Fees vary based on where you live, but commonly range from \$3 to \$15. 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. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
[www.transunion.com/
credit-freeze/place-credit-freeze](http://www.transunion.com/credit-freeze/place-credit-freeze)

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General, as well as the credit reporting agencies listed above. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Maryland 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. Clarksons is located at Commodity Quay, St Katharine Docks, London, United Kingdom, E1W 1BF.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; by phone toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of seven Rhode Island residents are potentially impacted by this incident. You have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you may be asked to provide some kind of proof that you have been a victim.

For 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. We encourage you to 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 to the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

EXHIBIT B

NOTICE OF DATA BREACH

ABOUT THE DATA PRIVACY EVENT

Clarkson PLC ("Clarksons") recently discovered a cyber security incident that may affect the security of certain of personal information. Clarksons take issues of IT security extremely seriously and is working to provide potentially affected individuals with information and access to resources so that they may take steps to best protect their personal information.

FREQUENTLY ASKED QUESTIONS

Q. What Happened? On November 7, 2017, Clarksons learned that it was the subject of a cyber security incident in which an unauthorized third party accessed certain Clarksons' computer systems in the UK, copied data, and demanded a ransom for its safe return. As soon as the incident was discovered, Clarksons took steps to respond to and manage the incident, including launching an immediate investigation into the nature and scope of the event, notifying regulators, working with third party forensic investigators, and informing law enforcement.

Through the forensic investigation, Clarksons quickly learned that the unauthorized third party had gained access to its system from May 31, 2017 until November 4, 2017. Clarksons learned that the unauthorized access was gained via a single and isolated user account. Upon discovering this access, Clarksons immediately disabled this account.

Through the investigation and legal measures, Clarksons were then able to successfully trace and recover the copy of the data that was illegally copied from its systems.

Q. What Information Was Involved? While Clarksons were able to successfully trace and recover the copy of the data that was illegally copied from its systems, as a precautionary measure, Clarksons have also been working diligently, in cooperation with law enforcement and forensic investigators, to determine what data may have been involved. In an abundance of caution, Clarksons are notifying potentially affected individuals.

While the potentially affected personal information varies by individual, this data may include a date of birth, contact information, criminal conviction information, ethnicity, medical information, religion, login information, signature, tax information, insurance information, informal reference, national insurance number, passport information, social security number, visa/travel information, CV / resume, driver's license/vehicle identification information, seafarer information, bank account information, payment card information, financial information, address information and/or information concerning minors.

Q. What is Clarksons Doing to Respond? Clarksons take the security of personal information very seriously. While Clarksons has enhanced security measures in place to protect data in its care and while Clarksons has notified the necessary regulatory and law enforcement bodies across the relevant jurisdictions, as a precautionary measure, Clarksons is also providing potentially affected individuals with information about this event and about the further steps individuals may take to best protect their personal information.

Q. What Can I Do to Protect My Information? Clarksons encourage those potentially affected by this incident to review the information below on steps an individual can take to protect personal information.

For all potentially affected individuals:

1. Remain vigilant against incidents of identity theft and fraud by reviewing personal account statements for suspicious activity and to detect errors.
2. Contact the account provider immediately if any suspicious activity is detected.

For potentially affected individuals residing in the U.S.:

Monitor Your Accounts

Credit Reports. Clarksons encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your personal account statements and monitoring your free credit reports for suspicious activity and to detect errors. 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. Contact information for the credit reporting agencies can be found below.

Fraud Alerts. At no charge, you can also have the three major 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 questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. 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, lift, 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. Fees vary based on where you live, but commonly range from \$3 to \$15. 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. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a legible copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
freeze.transunion.com

Additional Information

You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General, as well as the credit reporting agencies listed above. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal

Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Maryland 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 North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; by phone toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 7 Rhode Island residents are potentially impacted by this incident. You have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you may be asked to provide some kind of proof that you have been a victim.

For 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. We encourage you to 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 to the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Massachusetts residents, you have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you may be asked to provide some kind of proof that you have been a victim. If you have been the victim of identity theft, and you provide a 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 up to \$5 to place, temporarily lift, or permanently remove a security freeze. The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit file report. The credit bureaus must also send written confirmation to you within five (5) 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 security freeze in order 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 proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze, as well as 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. To remove the security freeze, 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 (3) business days after receiving your request to remove the security freeze.

Q. Where Can I Find More Information? If you have additional questions, please call one of our dedicated assistance lines:

1. For callers in the U.S.: 888-785-1475, Monday through Friday, 9 a.m. to 9 p.m. Eastern Time, except holidays.
2. For callers in the U.K.: 0800 310 0190, Monday through Friday, 9 a.m. to 5 p.m. British Time. For callers outside the U.K., please call 0141 265 0007.

EXHIBIT C

FOR IMMEDIATE RELEASE

RE: Clarkson PLC (“Clarksons”), Notice of Data Breach

London, United Kingdom (July 30, 2018) – Clarkson PLC (“Clarksons”) discovered a cyber security incident that may affect the security of certain of personal information. Clarksons take issues of IT security extremely seriously and is working to provide potentially affected individuals with information and access to resources so that they may take steps to best protect their personal information.

What Happened? On November 7, 2017, Clarksons learned that it was the subject of a cyber security incident in which an unauthorized third party accessed certain Clarksons' computer systems in the UK, copied data, and demanded a ransom for its safe return. As soon as the incident was discovered, Clarksons took steps to respond to and manage the incident, including launching an immediate investigation into the nature and scope of the event, notifying regulators, working with third party forensic investigators, and informing law enforcement.

Through the forensic investigation, Clarksons quickly learned that the unauthorized third party had gained access to its system from May 31, 2017 until November 4, 2017. Clarksons learned that the unauthorized access was gained via a single and isolated user account. Upon discovering this access, Clarksons immediately disabled this account.

Through the investigation and legal measures, Clarksons were then able to successfully trace and recover the copy of the data that was illegally copied from its systems.

What Information Was Involved? While Clarksons were able to successfully trace and recover the copy of the data that was illegally copied from its systems, as a precautionary measure, Clarksons have also been working diligently, in cooperation with law enforcement and forensic investigators, to determine what data may have been involved. In an abundance of caution, Clarksons are notifying potentially affected individuals.

While the potentially affected personal information varies by individual, this data may include: date of birth, contact information, medical information, tax information, insurance information, Social Security number, CV / resume, driver's license/vehicle information, bank account information, passport information, payment card information, ethnicity, digital signature, visa/travel information, financial information, criminal conviction information, login information, seafarer information, and address information

What We Are Doing. Clarksons take the security of personal information very seriously. While Clarksons has enhanced security measures in place to protect data in its care and while Clarksons has notified the necessary regulatory and law enforcement bodies across the relevant jurisdictions, as a precautionary measure, Clarksons is also providing potentially affected individuals with information about this event and about the further steps individuals may take to best protect their personal information.

As an added precaution, Clarksons is offering potentially affected individuals access to one (1) year of identity protection services. This service is being offered at no cost and will be paid for by Clarksons.

What You Can Do. You can review the information Clarksons is providing on steps individuals can take to protect their information.

For More Information. If you have additional questions, please call our dedicated assistance line at 888-785-1475, Monday through Friday, 9 a.m. to 9 p.m. Eastern Time, except holidays.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your personal account statements and monitoring your free credit reports for suspicious activity and to detect errors. 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. Contact information for the credit reporting agencies can be found below.

Fraud Alerts. At no charge, you can also have the three major 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 questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. 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, lift, 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. Fees vary based on where you live, but commonly range from \$3 to \$15. 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. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a legible copy of your state identification card or driver’s license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. 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). Do not send cash through the mail. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
freeze.transunion.com

Additional Information

You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General, as well as the credit reporting agencies listed above. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Maryland 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 North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; by phone toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. There are currently no known Rhode Island residents potentially impacted by this incident. You have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you may be asked to provide some kind of proof that you have been a victim.

For 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. We encourage you to 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 to the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Massachusetts residents, you have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you may be asked to provide some kind of proof that you have been a victim. If you have been the victim of identity theft, and you provide a 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 up to \$5 to place, temporarily lift, or permanently remove a security freeze. The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit file report. The credit bureaus must also send written confirmation to you within five (5) 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 security freeze in order 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 proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze, as well as 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. To remove the security freeze, 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 (3) business days after receiving your request to remove the security freeze.