

UPDATE ON 2017 DATA BREACH – REGULATORY NOTICE

ABOUT THE DATA PRIVACY EVENT

Clarkson PLC (“Clarksons”) has 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	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19106
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	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	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/	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/ff/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.