DocuSign Envelope ID: 7C238DDD-9D75-4615-BA74-F50B2274E23C

Shell USA, Inc.
James Cowan
Global Litigation
150 Dairy Ashford
Houston, TX 77079
Phone: 832- 337-2676
Email: james.cowan@shell.com

July 25, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Data Security Event

Shell USA, Inc. ("Shell USA") is submitting this notice to provide the Attorney General with information regarding a cybersecurity event involving affiliates of Shell that has resulted in unauthorized access to the personal information of one (1) Maryland resident.

On **May 31, 2023**, an affiliate of Shell USA discovered that some of its data had been impacted by the MOVEit Transfer vulnerability. The attack targeted the MOVEit Transfer software, a file transfer system offered by Progress Software. The attack exploited a vulnerability within the software (CVE-2023-34362) that allowed an attacker to escalate privileges and gain unauthorized access to MOVEit databases. Shell was one of many organizations that was affected by the mass exploitation of the MOVEit vulnerability. The attackers did not access Shell's network outside of the MOVEit Transfer portal.

Upon learning of the existence of a vulnerability in the MOVEit Transfer software, Shell's cyber defense team immediately began an investigation to determine if the software was in use and if it had been compromised. Upon verification of a compromise, Shell initiated a process to understand what data may have been accessed without authorization. Shell subsequently learned that personal data belonging to the employees of the BG Group, a company previously acquired by Shell, had been compromised and downloaded by a hacker group called CL0P. While the data was encrypted at rest on Shell's server, the nature of the vulnerability allowed the attackers to bypass the encryption in place on the MOVEit portal and obtain the data in plaintext. Shell patched the vulnerability to prevent further unauthorized access from this incident on **June 1**, the same day the compromise was verified.

Following a detailed investigation into the impacted data, Shell confirmed that some personal information related to employees of the BG Group had been accessed without authorization. Shell's initial investigation indicated that name, address, date of birth, marital status (in the form of a numerical key), number of children, employee personnel number, postal code, telephone number, bank account number (but without any additional information that would allow access to that account), and annual salary had been impacted. However, as the investigation progressed, on **June 30**, Shell discovered that Social Security numbers were also impacted, including the Social Security number of one (1) Maryland resident, which prompted this notification.

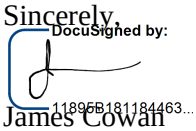
Shell sent a preliminary email notification to impacted individuals for whom we had a valid email address on July 5 and will be mailing formal notifications to all impacted Maryland residents on or about July 27, 2023. For U.S. residents, Shell will be providing individuals with a complimentary 24 month membership

DocuSign Envelope ID: 7C238DDD-9D75-4615-BA74-F50B2274E23C

to Experian's IdentityWorks fraud detection tools and credit monitoring. In total, approximately 16,200 individuals were impacted globally. However, this number may be over-inclusive as Shell is still working to identify duplicates within this data set for employees who have changed jurisdictions and may have been double-counted.

Should you have any questions please do not hesitate to contact our outside counsel, Michael Bahar, at MichaelBahar@eversheds-sutherland.com or 1 (202) 383-0882.

Sincerely,



James Cowan
Associate General Counsel Global Litigation
Head of Legal US

Shell Privacy Office
Email Central-HR-Incident-Support@shell.com
Internet https://www.shell.com/employeedata.html

ToName of Affected Individual
ToAddress of Affected Individual
Address second Line
Address third line

X July 2023

Subject: Important information about your personal data

Dear Name,

We are contacting you in relation to a cyber security incident which has impacted your personal data.

What happened?

You may have seen in the news that a number of organizations globally have been affected by a cyber security attack on software from Progress Software called MOVEit Transfer. The MOVEit software is currently used by a small number of companies within the Shell group of companies ('Shell').

On May 31, 2023, Shell discovered that we were impacted by this cyber-attack. Shell contained the vulnerability to prevent further unauthorized access from this incident on June 1, the same day the compromise was verified. The cyber-attack did not target Shell directly but was directed at all users of the MOVEit Transfer software.

What information was involved?

The personal data that has been subject to unauthorized access and exfiltration includes your Social Security number, as well as potentially your name, address, telephone number, date of birth, emergency contact name, number of children, annual salary, and bank account numbers. The data is from 2013 and while it may be out of date, there is a risk of identity theft and being targeted by phishing campaigns.

What we are doing:

Shell takes this incident and the security of information in our care seriously. Immediately upon verifying the compromise, Shell took steps to successfully contain the vulnerability to prevent further unauthorized access from this incident.

What you can do:

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please

also review the enclosed *Steps You Can Take to Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the credit monitoring services that we are offering.

The main issue is to be aware of the possibility of identity theft and targeted email campaigns. In particular:

- Be alert and aware of suspicious emails, SMS or telephone calls requesting your personal information.
- Change your account passwords and never use the same passwords for different accounts.
- Alert financial institutions you have accounts with so they can implement additional monitoring and security protocols on your account.
- Closely monitor financial statements for unauthorised transaction.

Experian IdentityWorks℠

To help protect your identity we are offering complimentary access to Experian IdentityWorks℠ for 24 months. This includes identity restoration and fraud detection.

Identity Restoration

If you believe there was or may have been fraudulent use of your information as a result of this incident, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). Identity Restoration does not require any activation. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

Fraud Detection

We also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24 month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Contact Central-HR-Incident-Support@shell.com to receive a unique activation code.
- Ensure that you enroll by 31 October 2023 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Enter the details of your activation code.

If you have any questions or need assistance with Identity Restoration or Fraud Detection please contact Experian's customer care team at 1-

877-890-9332. Be prepared to provide engagement number B098258 as proof of eligibility for the Identity Restoration services by Experian.

Additional details regarding your 24-month Experian IdentityWorks Membership

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- Credit Monitoring: Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARETM: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

For more information:

We regret the concern and inconvenience this may cause. We take cyber security seriously and are committed to ensuring we have the appropriate controls in place to protect personal data. Shell's cyber defence team continues to proactively monitor external and internal sources for any additional developments related to this incident. You can find further information regarding your rights here: https://www.shell.us/privacy/ex-employee-notice.html. If you require further information, please contact Central-HR-Incident-Support@shell.com or call +1 (866) 514-7135.

Yours sincerely,

Shell Data Privacy Office

ATTN: HR Operations (E-6)
150 N Dairy Ashford Road
Woodcreek Campus E-0674
Houston, TX 77079

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Steps You May Take to Help Protect Yourself Against Potential Misuse of Information

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. We recommend that you 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 obtain 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: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports. We also recommend that you promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission (FTC). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft

should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

Fraud Alerts: Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com

Experian: 1-888-397-3742, www.experian.com

TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Placing, lifting, and/or removing a credit freeze from your account is completely free and will not affect your credit score. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. Please contact the three national credit reporting agencies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com

TransUnion: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the three national credit reporting agencies listed above.

The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when

freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day, and year); current address and previous addresses for the past 5 years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state, or military ID card, and a copy of a utility bill, bank, or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

For residents of the District of Columbia: You may also obtain information about steps to take to avoid identity theft from the District of Columbia Attorney General: District of Columbia Attorney General, 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of New York: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: 1-800-771-7755, http://www.ag.ny.gov/home.html and the New York Department of State Division of Consumer Protection: 1-800-697-1220, https://dos.nysits.acsitefactory.com/consumer-protection.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.