Return Mail Processing
P.O. Box 1330
Columbus, MT 59019

[NAME]
[ADDRESS]
[CITY, ST ZIP]

Sibanye Stillwater Limited
Reg. 2014/243852/06

Registered Address:
Constantia Office Park
Bridgeview House • Building 11 • Ground Floor
Cnr 14th Avenue & Hendrik Potgieter Road
Weltevreden Park • 1709

Postal Address:
Private Bag X5 • Westonaria • 1780

Tel +27 11 278 9600 • Fax +27 11 278 9863

September 9, 2024

RE: NOTICE OF SECURITY INCIDENT

Please read this entire letter.

Dear [NAME]:

We are contacting you about a recent data security incident involving the Sibanye-Stillwater group ("we" or the "Company"). You are receiving this notice as a current or former employee of Stillwater Mining Company, a group company. This notice serves to inform you that certain of your personal information may have been impacted as a result of the incident.

What Happened? On or around July 8, 2024, we discovered that certain Sibanye-Stillwater information and communications technology ("ICT") systems within our global network had been compromised. We quickly took steps to contain and remediate the incident. Upon discovery, we initiated the Incident Response plan we maintain, and we engaged external cybersecurity experts and forensic firms to assist our ICT team to investigate the incident. The investigation remains ongoing, and in August 2024, the forensic investigation identified that certain U.S. systems storing personal information were impacted by the incident. We have notified relevant law enforcement agencies and continue to work closely with them to identify and hold accountable those responsible for this attack; this notification was not delayed as a result of a law enforcement investigation.

What Information Was Involved? Our U.S. investigation has revealed that the personal information you provided the Company and/or that you may have stored on the Company's ICT infrastructure during the course of your employment relationship may have been impacted. Not all types of personal information were impacted for each person receiving this letter, so this full list may not apply to you. The types of personal information we have identified as impacted consist of employee files containing records of personal information, such as: names; contact details; government ID and/or passport number; Social Security number; tax ID number; date of birth; marriage or birth certificate; financial information, such as a bank account number (but no passcodes or PINs); and medical information, such as a health plan number.

What We Are Doing. The incident has been contained, but we remain vigilant and are closely monitoring all systems. To reduce the risks of data security incidents in the future, we have and are implementing further measures to enhance the security of our network, systems and data, including refining password policies and further investing in enhancing our end-point detection, real-time monitoring and response capabilities. We are committed to continuous improvement and will continue to evaluate and implement additional available steps to further refine the security of our environment. While we are unaware of instances of identity fraud or theft as a result of this event, as a precaution, we are offering you access to free identity and credit monitoring services through Experian to help protect your identity. Further details and instructions for activating these services are explained below.

What You Can Do. We encourage you to be proactive and remain vigilant against identity theft and fraud by reviewing your account statements and monitoring credit reports, including for any suspicious activity or errors, and reporting any unusual activity to your financial institution. You can review the below additional ***Steps You Can Take to Help Protect Your Personal Information***. You can also activate the free identity and credit monitoring services we are offering.

Other Important Information.

How to Activate Experian's IdentityWorks℠. This complimentary 24-month membership of Experian's® IdentityWorks℠ product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by: December 31, 2024 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/plus
- Provide your activation code: [##########]

For further information about Experian IdentityWorks membership, please review ***Additional Details Regarding Your 24-Month Experian IdentityWorks Membership*** below.

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-931-5666 by December 31, 2024. Be prepared to provide engagement number B130505 as proof of eligibility for the identity restoration services by Experian.

For More Information. Should you have questions or concerns regarding this matter, please do not hesitate to call our toll-free assistance line at 1-833-931-5666, Monday through Friday from 8:00 am to 8:00 pm Central time (excluding U.S. holidays). You may also contact Stillwater Mining Company at P.O. Box 1330, Columbus, MT 59019, or for a quicker response, email us at ictservicedesk@sibanyestillwater.com.

At Sibanye-Stillwater, we take the privacy and security of our current and former employees' data seriously, and we regret any impacts that may result or have resulted from this incident.

Yours sincerely,

Neal Froneman

NEAL FRONEMAN
CHIEF ENABLING OFFICER
SIBANYE-STILLWATER

****

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 file for indicators of fraud.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration**: Identity Restoration specialists are immediately available to help you address credit and non-credit-related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-833-931-5666. 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 (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).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

** 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 CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Please be aware that access to personal information can create a heightened risk of criminals attempting to impersonate you or trick you into disclosing further information about yourself or your organization. This could potentially be used by third parties in various ways to commit fraudulent scams, digital profile hacks, identity theft or to intercept your communications. As a precaution, we also advise following these security guidelines as good practice to protect yourself:

- Remain vigilant against any suspected unauthorized use of your personal information
- Be cautious of any unsolicited communications that ask for your personal information or refer you to a web page asking for personal information: fraudsters often pose as officials from trusted authorities like the police or banks
- Change your passwords regularly and never share these with anyone else
- Avoid clicking on links or downloading attachments from suspicious emails
- Monitor your accounts, as described below

Monitor Your Accounts

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. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" (sometimes called a “security freeze”) on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report.

To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued ID card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding, and obtain information about, identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission (their main website is www.ftc.gov) 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, the Federal Trade Commission, and the relevant state attorney general.

The Massachusetts Attorney General may be reached at: One Ashburton Place, Boston, MA 02108; www.mass.gov/orgs/office-of-the-attorney-general; and 1-617-727-2200 (Mass relay users can also dial 7-1-1 and connect via the Attorney General's main number). Under Massachusetts law: (i) residents have the right to obtain any police report filed in regard to this event; and (ii) there shall be no charge for a security freeze.