Dear [_____],

Cyber attack: important information about your personal data

I am very sorry to inform you that Southern Water has been the target of an illegal cyber attack, which has unfortunately affected the security of some of your personal data, as one of our customers.

We are currently conducting an intensive investigation into this, supported by industry experts and following guidance from our regulators together with the National Cyber Security Centre. Our operations and services have not been impacted and your water supply is unaffected.

As a result of this investigation, we have reason to believe that the data compromised which relates to you may include:

- Basic personal details for administering your account and identifying you, such as your name and contact details. This may include your national insurance number and date of birth if you have provided these details to us.

What we are doing to reduce the risk to you

Southern Water takes its data protection and information security responsibilities to you seriously, and so we are bringing this to your attention as soon as we can. We are working closely with the regulatory authorities. We have notified the Information Commissioner's Office and are in regular contact with the National Cyber Security Centre. In addition, we have taken further steps, with support from independent cybersecurity experts, to enhance the security monitoring of our IT infrastructure.

We have also engaged a reputable third party to monitor the dark web on our behalf. They report that, since we were named on the cyber criminals' site on 22 January 2024, they have found no new evidence of data potentially compromised by this cyber incident being published online. They will continue to carry out these checks for as long as necessary.

To ensure that we're doing everything we can to look after you, we are offering you a 12-month, free-of-charge, enhanced Experian credit monitoring membership. This service provides identity monitoring and helps detect possible misuse of your personal information. It also supports identification and resolution of identity theft incidents.

What you should do next: activating your Experian Identity Plus membership

1) Please ensure that you sign up for the service within 2 months of the date of this letter (your code expires after this date).

2) Visit the Identity Plus website to get started: https://identity.experian.co.uk/get-started/protection

3) Validate your activation code: [xxxxx].

4) Enter your details to complete the registration

Once your membership is activated, you will have access to the following features:

- Unlimited access to your Experian Fraud Report.
- Credit Alerting – an email or SMS to let you know when certain changes happen on your Experian Credit Report, such as the addition of a new credit search.
- Access to Experian's CreditLock feature, allowing you to lock your Experian Credit Report when you're not applying for credit, and block any bogus claims.
- Web monitoring **–** an alert by email or SMS which confirms that personal information has been found on the dark web.
- Access to Experian's Victims of Fraud service if you do become a victim of fraud, who will support you in resolving fraud that has occurred.
- If you are at higher risk of fraud, Experian can add protective Cifas registration to your Credit Report which can help prevent credit being taken in your name.

If you have any questions regarding this service, then please contact Experian's Customer Support Centre on Tel. 03444 818182. They are open Monday to Friday, 8am to 6pm.

What is the background?

On 22 January 2024 we became aware that a cyber criminal organisation was claiming on its website to have stolen data from some of our IT systems.

We had previously detected suspicious activity and launched an investigation, as well as enhanced monitoring and other precautionary measures. Our independent cyber security specialists continue to investigate.

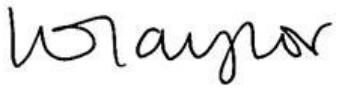
What happens next?

The information we have provided is based on what we know at this time. Our investigation remains active, and should we receive any additional material information, we will contact you.

Once again, I am very sorry that this has happened and for any inconvenience this illegal breach of data may cause you. We are working closely with the authorities and industry experts, to do everything possible to manage the situation and support you at this time.

Please call our dedicated customer service team on 0330 303 0025 if you have any questions.

Yours sincerely,



Katy Taylor

Chief Customer Officer

FURTHER INFORMATION

The National Cyber Security Centre, the Financial Conduct Authority and the Information Commissioners Office all provide helpful information to help protect your data and prevent fraud. This is summarised below with some useful links.

- Stay alert against any suspicious calls, texts or emails which could be a scam. If you receive any suspicious messages or calls, **do not hand over any information such as your bank account details**. Instead, hang up, or delete any worrying texts or emails and then contact your bank to report the suspicious activity. The FCA has some useful information on how to spot the warning signs of financial scams at www.fca.org.uk/consumers/protect-yourself-scams.

- Cyber criminals commonly use a scam technique called "**phishing**", which is mostly email-based but can also be via telephone calls, to lure victims under false pretences to websites which appear legitimate to get them to provide information including bank account and credit card details. These emails/phone calls appear to be from recognisable sources such as banks but actually link to fraudulent websites. To help prevent phishing:

    - Protect your email with a **strong password.**
    - **Do not share your password** with anyone.
    - **Install the latest security updates** to your browser software and personal computing devices.
    - If in doubt, **do not open emails from senders you do not recognise**.
    - **Check links** look correct before you click on them.
    - **Be suspicious** of anyone who asks for your bank account or credit card details.
    - If the email contains **spelling mistakes**, this can be a sign that this is a phishing scam. Do not open the email or attachments.

- More helpful information on how to protect your data can be found on the **National Cyber Security Centre**'s website - www.ncsc.gov.uk/guidance/data-breaches and the **Information Commissioner's Office** website – www.ico.org.uk/for-the-public/identity-theft and www.ico.org.uk/for-the-public/online