straumanngroup

CONFIDENTIAL
Re: Important notification about a data breach; request to be careful about phishing attempts

Dear [redacted]

We are writing to inform you of a cybersecurity incident and resulting data breach that affected a legacy system and which may affect your personal information. We take the protection of your data seriously and want to explain what has happened, what we are doing, and what steps you can take.

Your name appeared in the records of our local Straumann Group subsidiary in connection with the period during which the system was used by Straumann Group. However, at this stage, there is no indication that your data has been misused.

What happened
We recently identified unauthorised access to a legacy system used in connection with certain internal control processes from 2021 to 2024. Following detection, we immediately took steps to contain the incident and launched an investigation with the support of external cybersecurity specialists.
The affected system is separate from our core IT infrastructure and has been shut down and is being permanently decommissioned. Other customer-facing and internal systems, as well as the company's operations, products, and services, are not affected. Straumann Group remains focused on serving its customers without disruption. The incident has been reported to the relevant data protection authorities, and our investigation is ongoing. We are also taking appropriate steps with law enforcement authorities.

What information may be affected
Based on our current findings, the data involved may include your contact and identification details (such as name, email address, postal address, telephone number, and copies of signatures included in documents), certain employment-related information (for example contract details and employment dates), limited personal identifiers (such as Social Security Numbers), and limited) financial information (such as bank details (bank names/account numbers only – no PINs or passwords were impacted) or salary-related data).
The exact data involved may vary between individuals.

What this means for you
There is no indication at this stage that your data has been misused. However, your information may have been accessed by unauthorized third parties. As a result, you may receive unsolicited communication or phishing attempts, and in some cases, there is a risk of attempted identity or financial fraud. We recognize this may be concerning and are treating the matter with the utmost seriousness.

What we are doing
We have taken immediate steps to contain and address the incident and to reduce any potential impact, including:

- shutting down and isolating the affected system, which is not connected to the rest of our network
- engaging independent cybersecurity specialists to investigate the incident and support remediation
- ensuring that the replacement system operates within a strengthened and secure environment
- reviewing and strengthening our procedures and security measures
- In addition, we are offering you complimentary identity theft and credit monitoring services through Experian to help safeguard your personal information. To activate your membership and begin monitoring, please follow the instructions provided in the attached pages below.

ENGAGE# [redacted]

straumanngroup

What you should do

As a precaution, we recommend that you:

- remain vigilant for any unexpected emails, calls or messages requesting personal information
- do not click on suspicious links or open attachments from unknown sources
- do not share personal or financial information in response to unsolicited requests
- monitor your bank accounts and other relevant accounts for unusual activity and report any concerns promptly
- verify any unexpected communication claiming to be from Straumann through official channels

Contact

You have rights under data protection laws in relation to your personal data. You also have the right to lodge a complaint with your local data protection authority.

If you have questions or concerns, including questions about the cybersecurity incident, please contact [redacted] where dedicated team members are available to assist you.

If have questions on the enrollment process, or you prefer not to enroll online, you may call 1-833-931-7577 toll-free, Monday through Friday from 9 a.m. to 9 p.m. Eastern Time, excluding major U.S. holidays. Please have your engagement number [redacted] available.

We sincerely apologize for any inconvenience caused and will keep you informed of any significant developments.

Yours sincerely,

Straumann Group

Activate IdentityWorks Credit 1B Now in Three Easy Steps

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, 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).

Please note that Identity Restoration 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.

ENGAGE# [redacted]

While identity restoration assistance is immediately available to you, 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:

- Ensure that you **enroll by July 31, 2026**, by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/1Bcredit
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by July 31, 2026, at 1-833-931-7577 Monday – Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide engagement number [redacted] 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 file for indicators of fraud.
- **Security Freeze:** A freeze prevents unauthorized access to your Experian credit file, giving you peace of mind and protection against fraud.
- **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.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* 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.

ENGAGE# [redacted]