Email Title: Important: Incident update

Email Copy:

Dear <Customer Name>,

We are writing to notify you of a data security incident involving your personal information.

We believe in being transparent, so we want to explain what happened and what action we have taken to ensure you are protected.

What happened:

On 3 November 2025, we detected unauthorized access attempts to our file system that resulted in certain customer information being downloaded. Our teams responded immediately by restricting the unauthorized party from accessing our file system.

After blocking the unauthorized access, we conducted a detailed investigation, identified dependencies across internal application services, and reset the affected accounts. We then performed a comprehensive review of the impacted files and the associated file system, which is primarily used for storing technical system logs and not personal information. Through this analysis, we identified a limited number of files that contained personal data.

What information that accessed:

Based on our investigation, an old file from 2022 was accessed, which includes:

- Your name
- Email address
- Physical address
- Phone number
- Social Security Number
- Date of Birth

Additional preventive measures we have taken to safeguard your information:

- We have strengthened our monitoring to immediately detect and flag any such access attempts.
- We have implemented additional security controls to further restrict and protect our file system.
- As part of our continuous security improvements, we are planning to migrate to a new technology stack, which will further mitigate such risks in the future.

While there is no impact to your account, do keep a close watch for the following attempts:

- **Watch out for phishing attempts.** Personal data can sometimes be used to create phishing messages that appear more legitimate. These may:
    - Ask you to click on a link to "verify" your account
    - Pretend to be from a trusted organization
    - Use your name or partial details to seem credible

  Note that Instarem will never ask for your password, one-time passwords (OTPs), or financial information via email, SMS, or phone.

- **Be alert to impersonation scams.** In some cases, scammers may use your personal information to pose as you when attempting to contact others, for example, by pretending to be you in messages or online accounts.

We are here to help:

We understand this information may raise questions. Our team is committed to resolving any concerns you may have, fully and transparently. If you have questions regarding this incident or would like to subscribe to a complimentary credit monitoring service we are offering, please contact us at help@instarem.com. This email address has been created specifically for this incident and is closely monitored by senior management.

We sincerely apologize for this incident. Protecting your data is our highest priority.

Thank you for your trust and continued support.

Team Instarem