Key:
[Data driven variable text inserts]
[Text to be added]

Name, Surname of Data Subject
Address
Date, ……
Letter ID: **[INSERT unique random number]**

Dear [salutation]

We are writing to let you know about an incident that we recently understood concerns your personal information held by Credit Suisse. While we have not identified evidence showing that your data has been subject to misuse, we wanted to share details and offer support as a result. From Credit Suisse's perspective there is no further action required by you at this time but please note the section 'What can I do' below.

What happened?
An individual employee, who has since left the firm and had legitimate access to your personal data at the time for their daily work, inappropriately copied this information without Credit Suisse's authorisation onto their personal device. Once this incident was discovered, we immediately took actions to contain and protect your data. We have not identified evidence showing that your data has been subject to misuse.

Credit Suisse continues to take all appropriate steps – including legal remedies – in response to this situation. Credit Suisse has robust technical and organizational practices in place, including data loss measures, policies, procedures and training which we actively and continually enhance.

What data is involved?
The following personal information about you was accessed:

- **[If Basic Employment Flag = Yes]** Basic employment information such as employee ID, gender, address, civil status or date of birth
- **[If Enhanced Employment Flag = Yes]** Employment information such as National / Social Security ID and , contact information
- **[If Aged Salary Flag = Yes]** Aged compensation information (salary and bonus) for the period of 2013-15
- **[If Bank Account information flag = yes]** Bank account information as used by Credit Suisse to make payments to you.

What can I do?
As noted above, we have not identified evidence showing that your personal information has or is intended to be misused to cause harm to you. Nevertheless, and as a matter of general precaution, we encourage you to:

- Be especially aware of email, telephone and postal mail contact that asks for personal or sensitive information
- Remain vigilant, review your account statements, and monitor any available credit reports.

If you prefer help in monitoring signs of potential identity theft or misuse of your personal data, you may obtain a [**US:** 24 month / **OTHER LOCATIONS:** 12 month] identity monitoring service via Experian, an expert provider engaged by Credit Suisse, at no cost to yourself. In case you wish to sign up to this service please visit [**UK:** https://identity.experian.co.uk/get-started/protection / **US:** [EXPERIAN TO PROVIDE] / **Rest of World:** www.globalidworks.com/identity1] by 31 May 2023 using activation code [EXPERIAN: Code].

Who can I contact for further information?
Further information, including on the Experian service and notifications in different languages, are available at www.credit-suisse.com/ch/en/legal/data-incident.html. Credit Suisse also has opened a helpline for any questions relating to this matter available on [INSERT COUNTRY CONTACT NUMBERS]

We regret any inconvenience or concern that this may cause you and remain available for any questions you might have.

Your sincerely,

Nita Patel Chief Compliance Officer	Markus Diethelm General Counsel