

**Asia Pacific**

Bangkok  
Beijing  
Hanoi  
Ho Chi Minh City  
Hong Kong  
Jakarta\*  
Kuala Lumpur\*  
Manila\*  
Melbourne  
Seoul  
Shanghai  
Singapore  
Sydney  
Taipei  
Tokyo

**Europe, Middle East  
& Africa**

Abu Dhabi  
Almaty  
Amsterdam  
Antwerp  
Bahrain  
Baku  
Barcelona  
Berlin  
Brussels  
Budapest  
Cairo  
Casablanca  
Doha  
Dubai  
Dusseldorf  
Frankfurt/Main  
Geneva  
Istanbul  
Johannesburg  
Kyiv  
London  
Luxembourg  
Madrid  
Milan  
Moscow  
Munich  
Paris  
Prague  
Riyadh  
Rome  
St. Petersburg  
Stockholm  
Vienna  
Warsaw  
Zurich

**Latin America**

Bogota  
Brasilia\*  
Buenos Aires  
Caracas  
Guadalajara  
Juarez  
Lima  
Mexico City  
Monterrey  
Porto Alegre\*  
Rio de Janeiro\*  
Santiago  
Sao Paulo\*  
Tijuana  
Valencia

**North America**

Chicago  
Dallas  
Houston  
Miami  
New York  
Palo Alto  
San Francisco

April 6, 2021

**Via Email: attorneygeneral@doj.nh.gov**  
Office of the Attorney General  
33 Capitol Street  
Concord, New Hampshire 03302

Brian Hengesbaugh  
Tel: +1 312 861 3077  
brian.hengesbaugh@bakermckenzie.com

**RE: Data Breach Reporting**

Dear New Hampshire Attorney General:

I am writing on behalf of Credit Suisse Securities (USA) LLC ("Credit Suisse") to notify you of a data incident. Specifically, Credit Suisse recently became aware that an email containing personal information about a small number of former employees was sent without authorization on or around March 20, 2021 to a limited set of former employees and other recipients. Upon learning of this incident on March 23, 2021, we immediately initiated an investigation to determine the scope of the incident. Although we are still investigating, we have now confirmed that personal information relating to 65 of our former employees was included in the unsolicited email, approximately 1 of which are New Hampshire residents.

Credit Suisse provided notice to affected former employees on April 2, 2021 via email address where available, and is following up with a postal mail notification as soon as possible, informing them about the incident, and encouraging them to take security precautions regarding their personal information. Credit Suisse is also providing affected individuals with 24 months of credit monitoring services.

Former employees affected by this intrusion may contact Credit Suisse at (212) 325-3467 if they have any questions and to clarify any concerns regarding this matter. Attached is a copy of the sample individual notice.

Please feel free to contact me with any questions at [brian.hengesbaugh@bakermckenzie.com](mailto:brian.hengesbaugh@bakermckenzie.com) or 312-861-3077.

Best regards,



Brian Hengesbaugh

April 2, 2021

## **NOTICE OF DATA BREACH**

We recently learned of a security incident that involved your personal information. We take the protection of your information seriously. We are contacting you now to explain what happened and the steps you can take to protect yourself.

### **WHAT HAPPENED?**

We recently became aware that an email containing personal information about a small number of former employees was sent without authorization on or around March 20, 2021 to a limited set of former employees and other recipients. Although this email purported to come from our CEO, we can confirm that it was actually sent by an unauthorized individual. Upon learning of the incident on March 23, 2021, we immediately initiated an investigation to determine the scope of the incident.

### **WHAT INFORMATION WAS INVOLVED?**

The personal information at issue may have included your name, social security number, bank account number, and date of birth.

### **WHAT ARE WE DOING?**

We have been working diligently to investigate and contain the incident, and to prevent this type of incident in the future. We continue to review our security measures to assure protection of our systems.

### **WHAT CAN YOU DO?**

At this point, we have no evidence that your personal information has been used to commit identity fraud. Nonetheless, we encourage you to be especially aware of email, telephone, and postal mail scams that ask for personal or sensitive information. Credit Suisse will not contact you in any way, including by email, asking for your social security number, bank account information, or other sensitive personal information. If you are asked for this information, you can be confident Credit Suisse is not the entity asking. Credit Suisse encourages you to remain vigilant, review your account statements, and monitor your credit reports where available.

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior 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 June 30, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [www.experianidworks.com/3bcredit](http://www.experianidworks.com/3bcredit)
- Provide your activation code: [REDACTED]

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 **(877) 890-9332** by **June 30, 2021**. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

## WHAT IS OTHER IMPORTANT INFORMATION?

The following additional information could also be useful:

- You may wish to visit the website of the U.S. Federal Trade Commission at <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> or reach the FTC at 877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC.
- North Carolina Residents: You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina) (919) 716-6400, [www.ncdoj.gov](http://www.ncdoj.gov).
- You may have the right to obtain any police report filed related to this intrusion, and to file a police report and obtain a copy of it if you are the victim of identity theft.
- U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free 877-322-8228.
- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus listed below. At no charge, if you are a U.S. resident, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit, mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies and you may be required to provide information such as your: (1) name; (2) Social Security number; (3) date of birth; (4) current address; (5) addresses over the past five years; (6) proof of current address; (7) copy of government identification; and (8) any police/investigative report or complaint. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.
  - Experian: 888-397-3742; [www.experian.com](http://www.experian.com); P.O. Box 9554, Allen, TX 75013
  - Equifax: 800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 105788, Atlanta, GA 30348
  - TransUnion: 800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000

Please note that although Credit Suisse is offering to provide the IdentityWorks product at no charge to you, the consumer reporting agencies listed above may require fees for their services.

If you have further questions or concerns, please call (212) 325-3467 during regular business hours or email us at: [us.data-protection@credit-suisse.com](mailto:us.data-protection@credit-suisse.com).

Credit Suisse values our employees, and protecting your personal information is a top priority. We apologize sincerely for any concern this incident may have caused.

Yours Sincerely,

James Keenan