October 20, 2015

Important: Unauthorized Use of Nomura Brand

Nomura takes its security very seriously and continuously monitors for email scams and other types of illegal activity purporting to be on behalf of Nomura and reports such activity immediately.

Nomura recommends you follow these simple steps to stay secure:

- Nomura does not engage in cold calling. If you have been approached by someone claiming to be a Nomura employee or representative that you do not already have a relationship with, take their details and contact our Fraud Risk Officer immediately.
- Do not reply to suspicious emails or text messages or contact the sender.
- Never click on suspicious website links or open attachments as this may lead to an attempt to infect your computer or mobile device with a virus.
- If you have opened a link in a suspicious email, do not input any personal or financial information on the web page that may appear.

Should you receive a suspicious Nomura branded email, text message or phone call from someone claiming to be a Nomura employee or representative, please contact our Fraud Risk Officer immediately to authenticate the content of such communication.