March 2020

**Subject: Cybersecurity Awareness**

Dear Corporate Clients,

At BNP Paribas, we are aware that cyber-crime is an ever present threat to unsuspecting individuals, companies and institutions. As such, we would like to reassure you that we maintain secure systems that are constantly updated to counter potential threats.

Nevertheless, it is important to remain extremely vigilant in your day to day activities. We would therefore like to highlight some of the current methods being deployed by cyber criminals. They include:

* Hacking into company emails and issuing out fraudulent communications to the company’s buyers/counterparts. Such communications tend to notify stakeholders of a change in bank account details, and request buyers/counterparts to make future payments into the hacker’s fraudulent account.
* Hacking into company emails and issuing fraudulent instructions to the company’s bank, requesting a fund transfer to a counterpart. The email instructions and the payment instructions are fraudulent (this includes forging an e-mail address, letter heads and authorised signatories signatures etc.)
* Phone calls from an individual claiming to be part of your company’s Senior Management, requesting an urgent and confidential transfer of a large sum of money for very secretive reasons (e.g. a take-over, tax reasons or a large confidential transaction). The caller puts enormous pressure on you to act immediately, so that you can’t verify the truth of the call. Frequently, these calls are carried out just before, or during holiday periods.

In order to minimise the risks of such incidents, we would recommend the following actions:

* Never disclose your account number, card number, CVV, OTN/PIN received from the bank to anyone over the phone or through any means.
* Always call back and verify any new instructions that you receive relating to a change in details, especially if the instructions relate to fund transfers. Use the number that is known to you, and not the one provided in the suspicious correspondence (if different).
* Never use email to communicate payment instructions to your bank. Always send payment instructions through secure channels, e.g. e-banking tools such as Connexis.
* Ensure that your clients/counterparts are aware that you will never request a change in bank account details or personal information via email
* Regularly check your account movements using the secure online reporting platforms provided by your bank. Immediately alert your bank if you notice any suspicious entries.
* Always keep your bank account details and passwords confidential and do not share them via email or any other unsecure channel.
* Ensure that your email system security features are updated regularly.

Please note: This notification does not constitute advice on how to secure your business and/or banking activities. It is solely intended to alert you to potential risks and remind you to take any necessary steps to combat fraud.

Thank you,

BNP Paribas