Dear Sir/Madam,

In these unprecedented circumstances, which first responders, patients, families and businesses face with courage, we strongly recommend that you do not lower your guard against **fraud and cyber threats**. Fraudsters and hackers are increasingly active; seeing opportunities to attack fragile businesses and organisations, exploiting the on-going crisis to carry out fraudulent attacks.

- Beware of **new 'fake CEO' scam schemes**: Scammers will exploit the crisis, using it as a justification to request the urgent transfer of funds to other banks.
- Make your employees particularly aware of **the risk of ransomware**: Hackers have already exploited the theme of the coronavirus to spread malware, by email, attachments and via malicious websites – treat every email with added suspicion before taking any action.
- Stay protected against **'fake vendor' scams**: Ensure you verify any changes via a known contact using your existing contact details, via skype, Facetime or telephone; we recommend dual verification prior to making any changes to vendors bank account details internally.
- Be careful when **purchasing masks, hydroalcoholic gel or other coronavirus related products**: we are informed of numerous scams (products are not delivered or are bogus).
- Check the identity of anyone claiming to be part of BNP Paribas teams: We see **'fake technician'** scam attempts.
- If possible, **use electronic transfers** and avoid transfer orders and validation by fax and email; it is easy for fraudsters to get signature samples.
- In all cases, pay particular attention to **'email spoofing'**: Fraudsters can use an email address that very closely resembles that of your president, supplier, client, bank, auditor, etc. In some case fraudsters have infiltrated the address/server so the email appears completely genuine.

Raise your employees' awareness of fraud and cyber risks, be particularly vigilant with new joiners and temporary/contract employees. To assist you, please find attached the updated version of our **fraud and cyber risk awareness kit**. This kit of thirteen pages is aimed at operational staff, but is useful for everyone. It contains examples of frauds, warning signs that should alert them, videos and articles to learn more, as well as concrete tips to protect against fraud and cyber-attacks.

As your Cash Management Officer **I stand ready to support you through this challenging period**. Please feel free to contact me directly by phone or e-mail.