MUFG Bank, Ltd.
Singapore Branch
(Incorporated in Japan with limited liability)
7 Straits View
#23-01 Marina One East Tower
Singapore 018936
Tel: 6538-3388
Fax: 6538-8083
Registration No. (UEN) S73FC2287H

24th September 2019

Subject: Protect Yourself Against Business Email Compromise Frauds

Dear Valued Customer,

As part of MUFG's vision to be the world's most trusted financial group, we are committed to the security of your financial information, and protect you against increasingly sophisticated fraud schemes, including Business Email Compromise (BEC) frauds.

BEC fraud is just one prominent type of payment fraud. There are many others. Fraudsters are using increasingly sophisticated techniques that include voice impersonation and other social engineering tricks to get you to share account security credentials and related details or otherwise exploit vulnerabilities in your systems or procedures to accomplish their crimes.

Fraud prevention is a shared responsibility. We would like to share some guidelines on how to identify and avoid becoming a victim to BEC fraud in the next page.

If you suspect any fraudulent activity in connection with your MUFG accounts, please contact us immediately and notify the relevant authorities.

Sincerely,

Takuya Tanaka
Managing Director
Country Head of Singapore
MUFG Bank, Ltd.

MUFG Bank, Ltd.
Singapore Branch
(Incorporated in Japan with limited liability)
7 Straits View
#23-01 Marina One East Tower
Singapore 018936
Tel: 6538-3388
Fax: 6538-8083
Registration No. (UEN) S73FC2287H

About Business Email Compromise (BEC) Frauds:

A BEC fraud involves a fraudster hacking into an email account and impersonating its owner — your CEO, CFO, lawyer, or business counterparty — to request authorised staff members (e.g. your finance department) to transfer your funds to the fraudster's account. The fraudster will typically use a format and language similar to genuine requests to make them appear credible.

If successful, the fraudulent transfer will be completed, and it is often very difficult or impossible to retrieve those funds as they are immediately moved elsewhere with little or no audit trail or other trace of their ultimate destination.

Indications of an attempted BEC fraud include:

- A request to transfer funds urgently.
- Pressure not to follow usual procedures.
- Instructions to keep the transfer confidential or secret.
- Transfers to bank accounts that have not previously received funds from your account.
- Changes in the receiving bank account's details from prior transactions.
- Transfers to bank accounts in countries to which you have not usually sent funds.
- Transfers in currencies that are unusual for the transaction type, recipient's presumed location or country.

How to Protect Against BEC Frauds:

I) Review your security measures

- Regularly check your internal information security environment. Keep your antivirus software up to date and never open a link in an unexpected email or text.
- Communicate via secure methods (such as encrypted attachments and electronic signatures).

II) Confirm and consult

- Confirm requests received by email using an alternative communication method if at all possible (e.g. telephone using contact details you had on file prior to the email or otherwise known to be correct). Never use new contact details that come in the email requesting a transfer.
- When replying by email, do not use an automatic "reply" function. Manually re-enter an email address you know to be correct (previously had on file) in a new email thread. Fraudsters often use email addresses that appear identical but differ slightly from the correct one.
  Consult colleagues or your internal, regional cybersecurity professionals if you have any doubts about whether a transfer request is genuine, particularly in cases where the request is described as being confidential or urgent.

III) Review your internal approvals framework

- Check that your internal procedures for authorising, sending and executing fund transfer requests you receive are as strong as they can be.
- Review your list of authorised staff to make sure the number is sufficient to accommodate when some staff are absent from the office.