December 6, 2016

Please be vigilant to BEC(Business E-mail Compromise) or fraudulent e-mails instructing foreign remittance from imposters posing as trusted sources (foreign remittance fraud).

There have been a limited number of cases reported where a fraudulent email appearing to be from a trusted internal/external source has requested a foreign remittance instruction be made. The request is in fact a manipulated e-mail sent by a fraudster. The funds have then been stolen by the fraudster upon receipt.

*** This is a different scenario to infection of a computer by a virus or a crime in which a remittance is made illegally from a customer's account using an illegally acquired PIN.**

If you discover that your organization has been a victim of fraud, please contact and consult with the bank and/or the police.

Beware of fraudulent e-mails and phone calls attempting to defraud funds through domestic or foreign remittances.

✧ **When you receive e-mails that inform you of payment information (including payee's name ,bank name,bank account number,etc.)changed, please perform fact checking over telephones within your company. Please share information within your company.**
(e.g.purchasing person,person in charge of overseas business, accounting person in charge,etc.)

✧ **Please pay attention to your internal fund management framework (including your overseas subsidiaries) and security management framework for computers and other communication devices.**
(e.g.preventive measures against hacking activities)

■ Actual cases of fraud and preventive measures

Case 1 (Fraud that frequently occurs by typical tricks)

Funds were defrauded through the execution of a foreign remittance based on a request sent by e-mail from a person pretending to be a business partner such as a supplier (e.g. instructions to amend the deposit account) or an invoice attached to an e-mail.

[Preventive measures] Confirm facts by means other than e-mail (phone call, fax, etc.) whenever possible.

Case 2 (Fraud that occurs by artful tricks and causes high-value damage)

Funds were defrauded through the execution of a foreign remittance based on an e-mail or phone call from a person pretending to be the parent company's CEO or CFO, or urgent remittance instructions (e.g. for a confidential M&A deal) sent by e-mail from a person pretending to be a lawyer, etc.

[Preventive measures] Do not handle the issue alone. Share information within the company and determine the authenticity of the request by means such as confirming it with your head office.

■ Security measures, etc. for computers and means of communication

It has been confirmed that in many cases of fraud, computers were infected with viruses, internal e-mails were hacked, etc.

<Preventive measures>

- ✓ Reconfirm your internal information security environment (including overseas subsidiaries).
- ✓ Communicate with your business partners via more secure methods, such as using encoded attachments, using electronic signatures, etc.

■ Fund management framework

Cases of fraud where a staff member independently responded to a fraudulent e-mail while the person with the authority to execute banking transactions (e.g. a representative of an overseas subsidiary) was away on a business trip, etc. have been reported.

<Preventive measures>

- ✓ Review fund management authorities for situations when the representative is absent, and establish an internal check framework such as requiring two signatures.

MUFG Bank of Tokyo-Mitsubishi UFJ