Link to the web learning course
"3-minute animation for protecting yourself from BEC"

Please be cautious when making an urgent remittance to a new account. There have been an increasing number of business email compromise (BEC) frauds worldwide, where fraudsters impersonated their target companies' business partners, CEOs, etc. using spoof emails, fax messages, or phone calls to instruct the companies to make remittances. Please take a look at the web learning course as it introduces recent cases of fraud and countermeasures.

Trends in Remittance Fraud through BEC Based on Recent Cases

- Requests for wire payments via emails
- Slight differences in senders' email addresses (e.g. "Yanada" instead of "Yamada")
- Urgent requests
- Requests for wire payments to new beneficiary accounts
- Grammatical errors in remittance requests
- Fraudsters attempt to slip through signature verification by cutting out the true customers' signatures and attaching them to remittance request forms
- Domain names seem plausible at first sight (i.e. "@corporate-unionbank.com" instead of "@unionbank.com")
- Free webmail domain names instead of corporate domain names
- Remittances to banks in countries to which remittances have never been made before
- Attacks called deepfakes, which use AI to make phone calls that imitate the voices of target companies' CEOs, etc. to deceive their employees, have been reported
- Recently, there have also been cases where fraudsters exchanged emails over one to two months to make the targets trust them more before committing actual frauds

Effective Countermeasures against Remittance Fraud (BEC)

- Suspect strong requests for confidentiality (M&A) or prompt handling (urgent).
- Companies that show their contact information on their websites or social media sites

are more likely to be targeted by fraudsters.

- We strongly recommend that all remittance request emails be checked with the assumed email senders with no exception. (Use means other than email. Phone calls are very effective.) It is also useful to check the header information of emails.
- Make phone calls to numbers already registered in customer information files, instead of numbers written in emails. Fraudsters may intercept such calls (they may be forwarded), so ask one or two questions, whose answers only customers or their staff in charge know.
- If you receive an email from a sender in a foreign country (e.g. a vendor) and you cannot call them due to the difference in time zones and/or language, confirm the authenticity of the message by using a fax or phone number left in past outgoing communication records, instead of email. Ask the requestor to reply via fax or a phone call, instead of email (which could be compromised). If you cannot confirm the authenticity, consider delaying the remittance by a day to ensure authenticity is ensured.
- If you have any questions, please do not hesitate to contact your RM immediately.