April 2, 2018

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).

Request to our <customers>

Has there been any changes to the remittance destination account so far? (If there was a sudden change in remittance destination account just before the payment due date, please take precautions as there may be risks that such accounts may be designated for financial crime purposes!) Once funds are wired to a fraudulent account, refund will not be possible. Therefore, prior to arranging remittances, please confirm by directly inquiring not only to your accountant but also to the Marketing Personnel (Supplying, Purchasing and Overseas Section) that receives Business (Negotiation) E-Mails. Damages can be prevented through fact confirmation by Marketing Personnel.

For details, please see the attached file.

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

Caution Notice to Corporate Customer using our Remittance Service

There are repeatedly detected incidents of BEC (Business Email Compromise) frauds i.e. victims' email is hacked, fraudulently requested to arrange remittance of funds by identity thief's business email, and defrauded of funds.
If such remittance has been completed, it is very hard to get refund of the fund because, in many cases, fraudsters had already withdrawn or transferred it.
In order not to fall victim to the crime, BEC frauds, please be informed of the explanation as follows.

1. Methods of BEC frauds

Type 1: Identity Thief pretending to be your Business Partner

A fraudster becomes an identity thief pretending your business partner, sends email(s) that notice you of "Changing Bank Detail (e.g. Bank's name, Country's name where the bank is located, Payee's name, etc.)" and instruct you to complete arrangement of foreign remittance to the bank account noticed.

<Case Study>

Company A (A, hereinafter), a wholesaler handling steel related parts, purchases raw materials e.g. iron ore from Company C (C, hereinafter) in Asia. One day, late at night, A's accountant firstly received an email seeming to be sent by C. It said, "Our email address had been changed", "Our bank account that we have been occasionally using for receiving payment from our customers had been suspended for some reason", and "New bank details are to be informed". Next morning, the accountant received second email saying "New bank details are written as follows (Note: Bank name in Europe and its account number was mentioned there). Please complete your remittance of payment for the concerned contract very urgently". At once within the day, the accountant applied for foreign remittance. Then, the fund transfer had been completed. One week later, the genuine C inquired A about the payment of the concerned contract. At the time, A had detected possibility of fraud for the first time. Although A tried to retrieve the fund as rapidly as possible, the fund had already been withdrawn by the fake C, the fraudster.

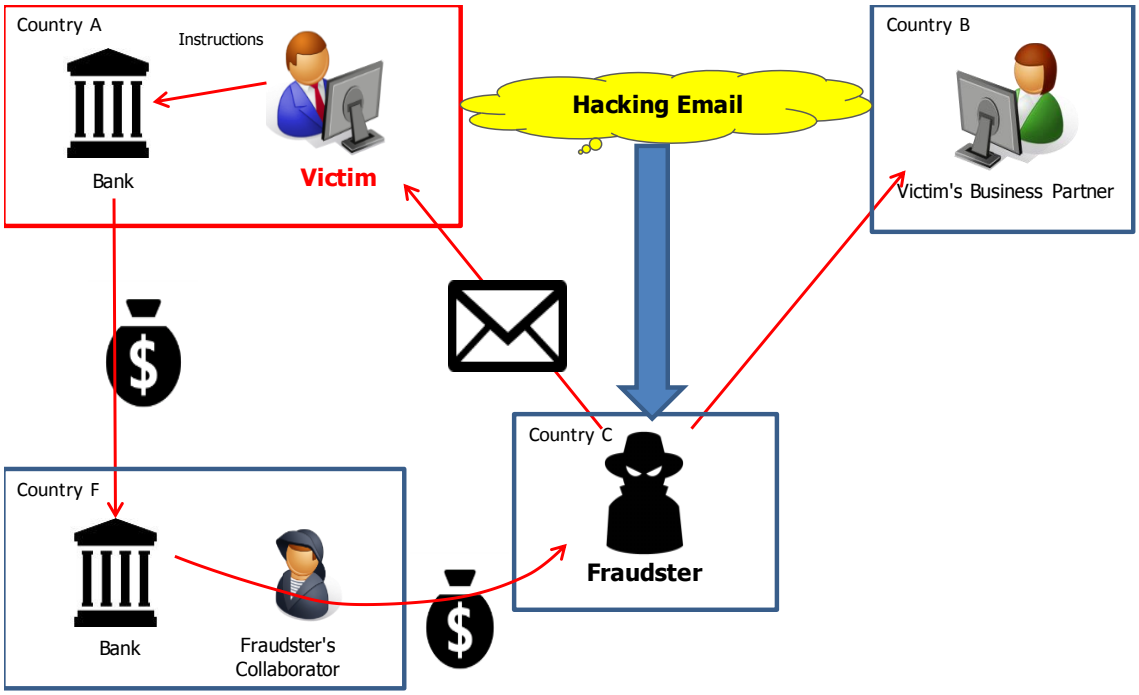
Type 2: Identity Thief pretending to be your company's executive or corporate lawyer

A fraudster becomes an identity thief pretending your company's executive or corporate lawyer. When the genuine executive or the lawyer is away from the office, a fraudulent email instructs you to complete arrangement of foreign remittance to the bank account noticed. In many cases, such instruction emphasizes that the remittance is "very urgent" and/or "strictly confidential".

<Case Study>

Company B (B, hereinafter) is a trader. One day, while Mr.T, B's CEO, had been away from the office on business trip since last Monday, B's accountant received an email. It said, "This is your company's corporate lawyer appointed by Mr. T, your CEO. At the moment, a certain M&A is being studied confidentially, and to be closed. Please send funds for acquisitions urgently. This matter must be handled secretly." The accountant, seriously following the "lawyer's" instructions, applied for foreign remittance without sharing the matter with anyone in B. Then, the fund had been transferred. One week later, when Mr. T, B's CEO came back to the office from business trip, he told that he did not have any recognition about the M&A. At the time,B detected possibility of fraud for the first time. After all,B had huge amount of funds stolen and damaged.

Caution Notice to Corporate Customer using our Remittance Service



What is BEC (Business Email Compromise) crime?
<Answer>
Fraudster(s) hack its/their target's email communication and comprehend relationship and background around the target, next become identity thief(s) pretending concerned party(s) e.g. business partner(s), defraud the funds of the target(s) by means of fraudulent email(s) i.e. Business Email Compromise.

2. Preventive measures against BEC crime
In many cases of BEC incidents, victims had their PCs or systems had been infected and hacked.

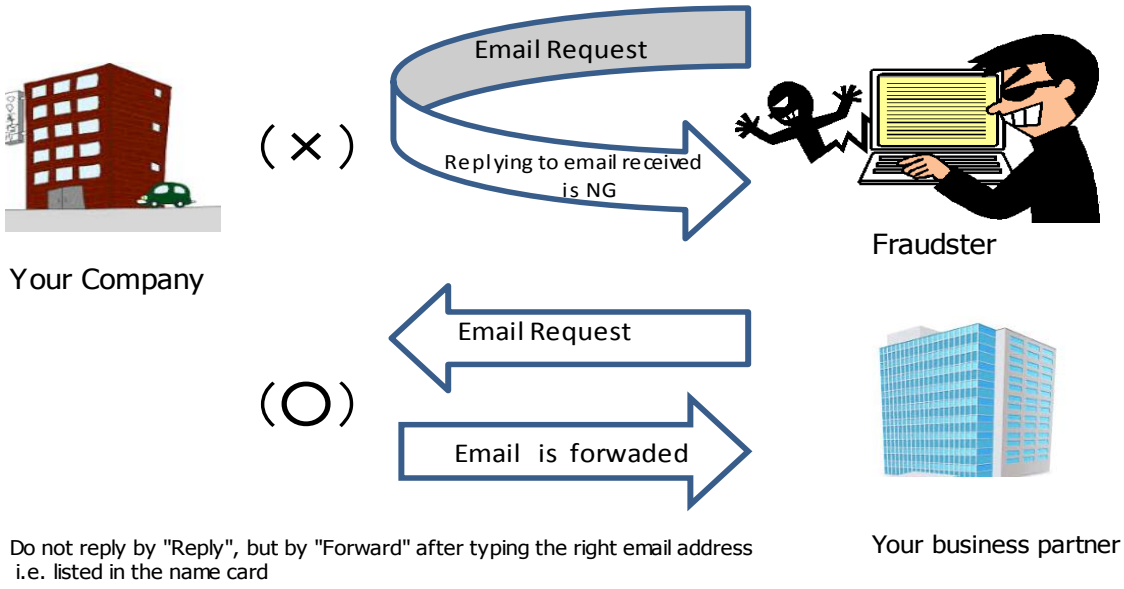
1. Reviewing your security measure
   a. To check your internal information security environment including PCs, network, various communication tools, etc.
   b. To communicate with your business partners via more secure methods, such as using encoded attachments, using electronic signatures, etc.

2. Ensuring confirmation with your concerned party(s)
   a. To make direct communication e.g. telephone, if noticed by email of "The change of Bank Details"
   b. It is better to reply by "Forward" than by "Reply", when you cannot help making confirmation by email.
   c. To avoid a staff's independent judge, if given instructions of "Confidential" or "Urgent" remittance.

3. Reviewing your fund management framework
   a. To review fund management authorities for situations when the representative is absent.
   b. To establish an internal check framework such as requiring two persons' signature.

<What is emphasized, in order not to be defrauded>

When you make confirmation, it is recommended to avoid email. Direct communication e.g. telephone is safe way to confirm.
If you cannot help using email, it is better to reply by "Forward" than by "Reply".



3. What to be checked before applying for remittance

If anything applicable of the checklist below, you are recommended to suspend the remittance. Anything suspicious is to be clarified whether it is absence or presence of problems.

<Checklist>

a. Did you receive an email requesting you to transfer funds soon with indicating "Urgent" etc.?
b. Were you instructed to transfer funds to the bank account where you had not sent?
(For example, the bank is located in the country and/or region that seemed to be strange.)
c. Do you find the fact the currency is not the home currency of the country to be remitted?
(For example, you are instructed to remit funds in USD to a bank in UK.)
d. Are you still in the stage you have not directly contacted with your beneficiary by telephone, etc. other than email?
e. Are you still in the stage you have not anyone check details of the invoice related to the fund transfer you are going to apply for.
f. When you reply to an email from someone, do you do so by hitting the reply button?
g. Are you still in the stage you have not consulted nor shared information with anyone within your company including another staff of different department?
h. Are you still in the stage you have not conducted antivirus measures on your PC, etc.?

If you detect that you are (possibly) defrauded by the crime, please contact our bank or your local police.