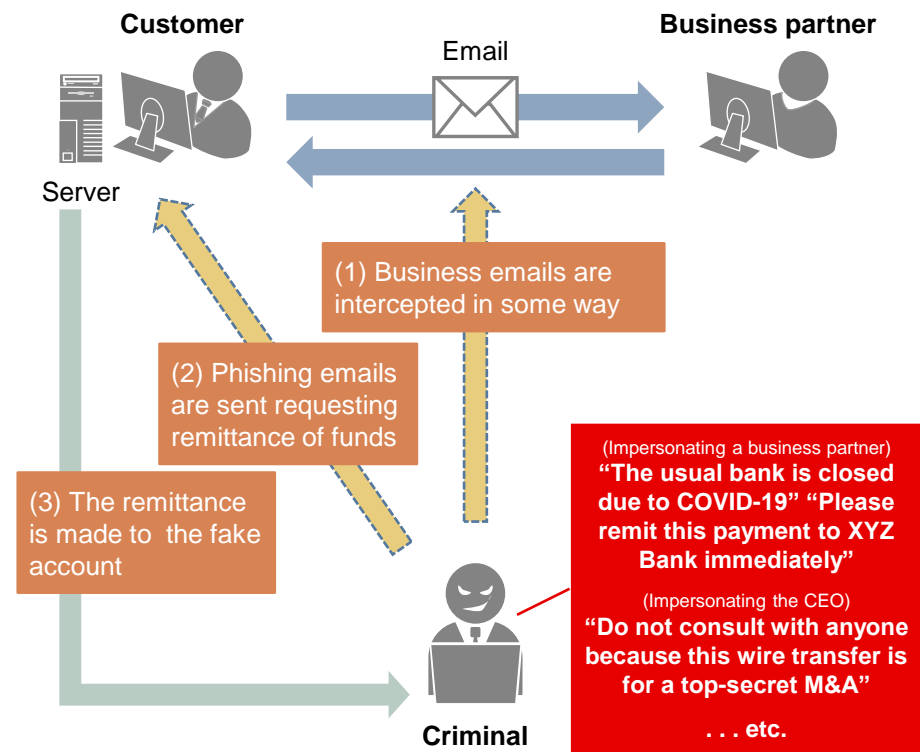


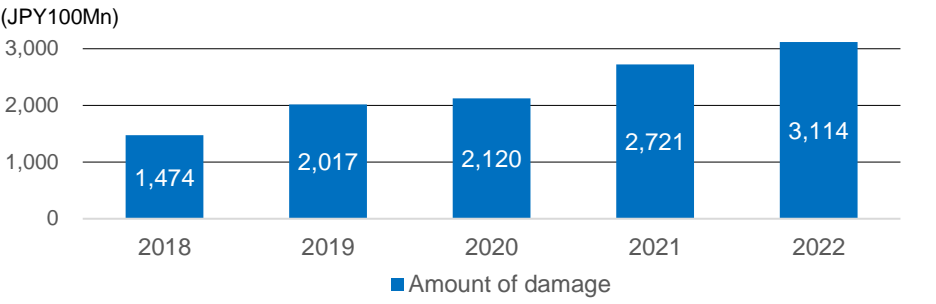
# What is Business Email Compromise (BEC)? – Beware of Foreign Remittance Fraud

**What is Business Email Compromise (BEC)?**  
Japanese companies (including overseas subsidiaries) are suffering frequent damages

**Business E-mail Compromise (BEC):**  
A type of fraud in which criminals swindle funds from customers by skillfully impersonating persons known to the victim, such as a business partner, and get them to send money to a fake account, etc. Recently, targeting methods other than email are increasing and become more sophisticated.



**Trends in the amount of BEC damage**  
(created based on FBI data on BEC damages / trends in amount of damage in the U.S.)



The above figures show the amount of BEC damages in the U.S. compiled by the FBI. In addition to the U.S., damages from BEC have been frequently reported in other countries including Japan, and subsidiaries of Japanese companies have suffered losses.

[Source] FBI Inter Crime Report, converted into JPY for 2018-2021 (calculated with a 5-year average TTM of JPY114)

## Main examples of BEC damage

- Vendor fraud (pretending to be a business partner)**
  - The scammer impersonates a business partner and requests changes to the bank account money is sent to, such as the account number or the name it is under.
  - They will provide some sort of plausible reason to convince you to change the account details.
    - ✓ “Please wire the money this time to the account of one of our group companies.”
    - ✓ “The name on the account has changed because of a merger.”
    - ✓ “The usual account cannot be used because of an audit.”
    - ✓ “The usual account is frozen due to a regulatory tax inspection.”
- CEO fraud (pretending to be the parent company president)**
  - The scammer impersonates the CEO of your company or your parent company and asks you to make a remittance, instructing you in the email to keep the information under control so that the scam goes unnoticed by anyone in your company.
    - ✓ “This matter is confidential. Keep it secret and between us only.”
    - ✓ “This remittance must be handled urgently, only involving the CEO and certain selected staff members.”


Extreme caution is needed, as the patterns of impersonation are increasingly complex, for example not only claiming to be a business partner or CEO, but also an authoritative third party such as a lawyer.




# Measures to Prevent Damage from BEC

## Measures to prevent damage from BEC

### Cases to be aware of

<b>“Deep-fake” voice phishing</b>	<ul style="list-style-type: none"> <li>■ This is a case in which a scammer uses an AI-generated voice to make phone calls that closely resemble the voice and intonation of the CEO or another person.</li> <li>■ Caution is required as in some cases, the customer is successfully duped by the voice on the phone, and may be pressured into hurriedly executing a money transfer.</li> </ul>
<b>Fraud in which multiple related parties are impersonated</b>	<ul style="list-style-type: none"> <li>■ This is a case in which e-mails related to a series of transactions are stolen and forged into multiple parties, including suppliers, customers, parent/subsidiary companies, and banks.</li> <li>■ Scammers send fake emails to each of the multiple parties involved and continue to communicate with them in order to buy time until the fraud is detected.</li> </ul>
<b>Fraud Cases Using Business Matching (Reference)</b>	<ul style="list-style-type: none"> <li>■ This is a case of fraud victims as a result of the commencement of transactions with new suppliers and customers in an attempt to develop a commercial distribution using business matching sites, SNS, etc.</li> <li>■ Caution is required as it is difficult to perceive the true identity of the counterparty or to confirm their soundness.</li> </ul>
 <b>Key points</b>	<ul style="list-style-type: none"> <li>■ It is first important to understand about the existence and tactics of BEC scams that target organizations and companies.</li> </ul>

### Specific measures

<b>1 Internal security countermeasures</b> <b>Systems</b>	<ul style="list-style-type: none"> <li>■ Double-check the information security environment.</li> <li>■ Apply multi-factor authentication.</li> <li>■ Establish a structure to detect unauthorized logins to in-house email accounts and systems.</li> <li>■ Require strong passwords.</li> </ul>
<b>2 Thoroughly confirm legitimacy with the counterparty</b> <b>Sales/ Purchasing</b> <b>Treasury / Accounting</b>	<ul style="list-style-type: none"> <li>■ Confirm requests for changes to account details by <b>methods other than email</b> such as phone or fax.</li> <li>■ When using email, set and confirm the correct address as written on the person's business card, etc.</li> <li>■ If instructed that a matter is “confidential” or “urgent,” do not make an independent decision; share and confirm information internally.</li> </ul>
<b>3 Review fund management / remittance approval processes, etc.</b> <b>Treasury / Accounting</b>	<ul style="list-style-type: none"> <li>■ Review fund management authority when the person with approval authority for bank transactions is absent.</li> <li>■ Establish a system of internal checks, such as requiring multiple-person approval for remittances.</li> <li>■ Strengthen confirmation processes when creating remittance templates.</li> </ul>
 <b>Key points</b>	<ul style="list-style-type: none"> <li>■ When confirming by phone or fax, please make sure to use the number on the business card or the number registered or reported beforehand, <b>not the number in the email</b>.</li> <li>■ If the only means of contact is by email, please <b>do not hit reply</b>, but instead manually enter the correct email address (as written on a business card, etc.) and forward the email.</li> </ul>

### Be careful in the following scenarios:

- ( ) Emails marked “urgent” requesting that money be sent immediately.
- ( ) When a fund transfer is requested to a bank account never used before for reasons such as “the account is incorrect” or “the account cannot be used due to an audit” (unfamiliar country / region).
- ( ) There is a mismatch in the currency and the country for the remittance (e.g. a request to send funds in USD to a UK bank for the first time).
- ( ) The destination bank account has never been verified (and no other methods of contact have been attempted other than email).
- ( ) A request is made when the person in charge / authorized person (at either your company or a business partner) is absent due to a business trip or vacation.
- ( ) No one has been asked to double-check whether the invoice / remittance application, including the imprint of the company/name seal and the signature, are correct. (Imprints and signatures are often unclear in cases of BEC.)
- ( ) It has never been confirmed if the email address matches the one printed on the corresponding business card (e.g. when replying to an email, you do not check whether the destination is the correct address.)
- ( ) No one in the company was consulted about instructions received for a “confidential” money transfer. (Accounting staff has not confirmed the transaction with the sales/purchasing staff, anyone in charge at the parent company, etc.)
- ( ) The computer being used does not have the latest antivirus software installed or updated.



It is important to establish a framework in advance that allows for immediate internal consultation if anything seems suspicious. Some companies are also sharing alerts about BEC measures in their internal newsletters. We urge your company to share information and implement anti-BEC measures comprehensively (involving not only accounting and treasury divisions, but also sales, purchasing, international divisions, domestic and overseas subsidiaries, etc.).

# Response to Damage from BEC · Reference Materials

## Response to damage from BEC · Reference materials

### Initial response to damage from BEC

<b>1</b>	<p><b>Immediately request a reversal of the transfer (to the bank)</b></p> <ul style="list-style-type: none"> <li>It is essential to request that the receiving bank return the funds immediately.</li> </ul>
<b>2</b>	<p><b>Consultation with the police/Report damages to the police</b></p> <ul style="list-style-type: none"> <li>It is important to consult with the police and submit a damage report not only to the Japanese police but also to the local police (in the country where the receiving bank is located). In some cases, the receiving bank will require you to submit a damage report when they issue the refund.</li> </ul>
<b>3</b>	<p><b>Conduct a security inspection and implement countermeasures</b></p> <ul style="list-style-type: none"> <li>Prompt response is required to prevent secondary damages.</li> <li>Confidential information and customer information may also have been hacked. A systems-related inspection is recommended.</li> <li>Investigate and prevent the cause of unauthorized access. Have all parties who send and receive relevant transaction emails change their passwords at once.</li> </ul>
<b>4</b>	<p><b>Other</b></p> <ul style="list-style-type: none"> <li>Avoiding the use of e-mail addresses etc leaked to criminals</li> </ul>

### Examples of response to BEC damage at an overseas subsidiary

<b>Parent company</b>	<ul style="list-style-type: none"> <li>Treasury officers at the head office report and explain incidents at the meeting of the board of directors.</li> <li>An internal team is launched to investigate the causes and build a recurrence prevention system.</li> <li>[For listed companies] Depending on the amount of damage, may need to disclose a downward revision to the company's business performance due to posting extraordinary losses.</li> <li>Support the subsidiary's cash flow (through a capital increase, intra-group loan, etc.)</li> <li>There may be increased burden on the head office side due to reviewing the authority of subsidiaries.</li> </ul>
<b>Overseas subsidiary</b>	<ul style="list-style-type: none"> <li>Request a reversal of the transfer (to the bank).</li> <li>Submit damage reports to police at both the head office and overseas, and consult with a corporate lawyer.</li> <li>Scrutinize cash flow, obtain capital increase or intra-group loan (where necessary), consider borrowing from external sources.</li> <li>Revise HR-related rules and training of local employees.</li> <li>Review the governance structure (limit sign-off authority to the president of the overseas subsidiary, restructure the payment workflow, etc.).</li> <li>Review security across the board.</li> </ul>

### Reference (1)

- You can find relevant materials on the MUFG website: "Understanding BEC - How to protect yourself from BEC" (Available in both English and Japanese)
- We would like to invite everyone involved in foreign remittance transactions, not only those in charge of accounting and treasury, but also those in sales, purchasing, international divisions, domestic and overseas affiliates, as well as everyone from those in charge on the working level to managers and executives to view this clip.  
URL: [https://www.bk.mufg.jp/global/noticeaboutfraud/caution\\_bec.html](https://www.bk.mufg.jp/global/noticeaboutfraud/caution_bec.html)



### Reference (2)

- The Information-technology Promotion Agency (IPA) (an external organization) has created a video on BEC prevention called "What's BEC? – "Business email compromise" tricks and countermeasures."  
(Available in both English and Japanese)
- This is an easy-to-understand, dramatized overview of what BEC is and the countermeasures to take. Please take a look. (Duration: approx. 12 min.)  
URL: <https://www.ipa.go.jp/security/videos/list.html>



MUFG Bank, Ltd.  
2-7-1, Marunouchi, Chiyoda-ku, Tokyo, Japan 100-8388  
<https://www.bk.mufg.jp/global/>

#### Disclaimer

This presentation shall create no contractual relations such as commitments between your company and MUFG Bank, Ltd. (hereinafter referred to as the Bank), and therefore the Bank shall assume no legal obligations or liabilities.

While the Bank believes that factual statements herein and any assumptions on which information herein are based, are in each case accurate, the Bank makes no representation or warranty regarding such accuracy and shall not be responsible for any inaccuracy in such statements or assumptions. All statements herein represent only the Bank's current judgment. The Bank shall assume no responsibility for any damages arising from this material. With respect to matters pertaining to specialized knowledge, we would like to ask your company to make judgments on its own account upon prior consultation with your company's specialists such as corporate tax accountants, certified public accountants, and lawyers.

The copyright of this material is held by the Bank and protected by copyright laws. Unauthorized use is prohibited. This information is intended for the recipient only and may not be quoted, reprinted or transferred in whole or in part without the prior approval of the Bank.

Copyright 2023 MUFG Bank, Ltd. All rights reserved.