

Don't be a victim of BEC !

~To prevent Business E-mail Compromise~

(About 3 minutes to view without audio)

<Contents>

1. BEC fraud growing sharply on world-wide basis
2. Methods of BEC fraud
3. Case Study
 - Case#1 Vendor Fraud
 - Case#2 CEO Fraud
4. Three effective measures to prevent BEC from victimizing you
5. Self-diagnosis: Can you save yourself from BEC?



1. BEC fraud growing sharply on world-wide basis

BEC fraud caused USD43.3bil loss in the past five years, announced by the Federal Bureau of Investigation (FBI)* on May 04 2022. *The FBI's Internet Crime Complaint Center (IC3)

**Approx USD43.3 Billion lost for
5years !**

(*Total amount of damage occurred by US related transactions: \$43,312,749,946)

**Number of BEC cases in US :
241,206**

(between June 2016 and December 2021)

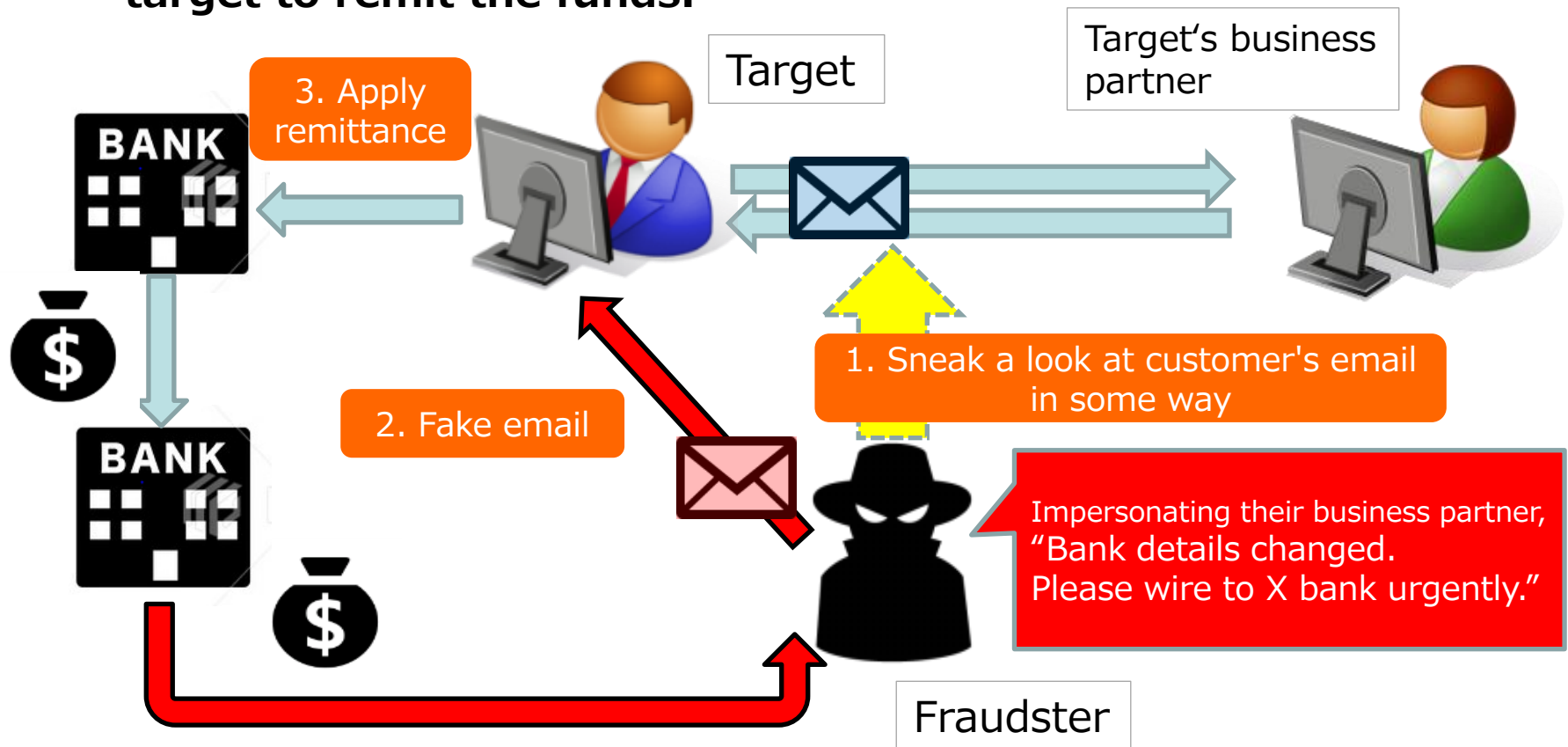
Average amount of damage per a case :

Approx USD180 thousand

**What kinds of methods of Business E-mail
Compromise (BEC) fraud are frequently seen?**

2. Methods of BEC fraud

- Criminals sneak a look at E-mails sent and received mainly by corporate customers in some way.
- Fraudster impersonates the target's business partner or CEO etc. and sends clever and sophisticated fake email to instruct the target to remit the funds.



Please see case studies in the following pages.

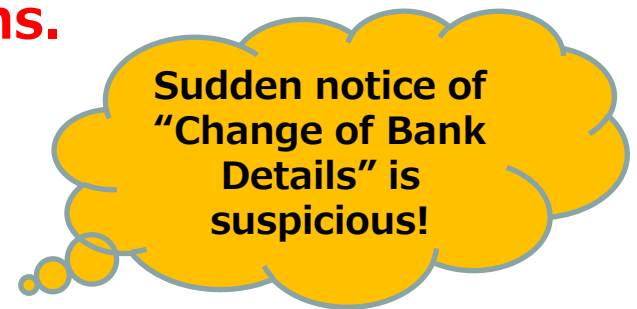
3. Case Study <Case#1>

Vendor Fraud (Identity thief impersonating the target's business Partner)

- a. Company A in Japan has a business with Company B in overseas.
- b. Company A has been sending the fund to Company B's account at Bank X in Hong Kong for many years. Suddenly, Company A received an email from Company B stating that, " Due to the audit, we can't use the existing account we always use. Please send the fund to Bank Y in China this time."
- c. Since Company B has a close relationship with Company A, Company A sent the fund without any doubt (any suspicious concern this is a fraud) .
- d. At a later date, Company A realized that it was a fraud, but could not recover the funds.

Fraudster makes its target believe "Change of Bank Details" with plausible reasons.

- Wire money this time to the account of one of our **Group Companies**.
- The account name changed because of a **Merger**.
- The usual account cannot be used because of **Audit**.
- The usual account is frozen under the authority's **Tax Inspection**.



3. Case Study <Case#2>

CEO Fraud (Identity thief pretending CEO incl. parent company's CEO)

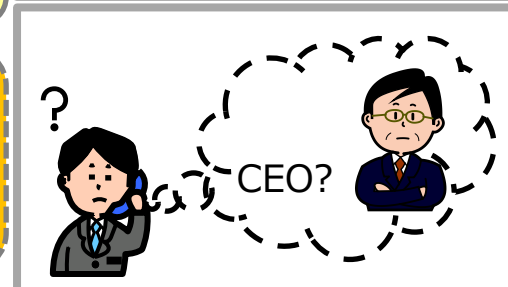
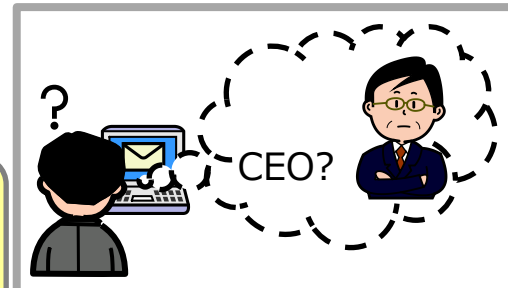
- Company C is a subsidiary in Japan with its parent company outside Japan.
- CEO of Company C received emails from someone who pretends to be the parent company's CEO. "As we have a top secret M&A deal, we need funds. Send money confidentially to the designated account".
- Parent's CEO said "If you don't pay, we can't make a contract. Please do it right away", and the CEO of Company C made a payment immediately to the designated account.
- At a later date, CEO of Company C had a chance to contact the genuine parent company's CEO, and talked about the M&A transfer above. He replied, "I had never instructed such funds transfer," and as such, the CEO of Company C recognized that it was a fraud but could not recover funds.

Fraudsters force the targeted person to conduct information control to keep the matter of the fraudulent remittance secret.

- Handle this **Confidentially**. Keep it **Secret**. This is **between us**.
- This **important M&A** deal must be completed **urgently**.

Latest topic : Deep Fake Audio (Voice) Fraud

- By means of a voice-generating AI software, fraudsters could make telephone calls with deep fake CEO's voice.
- An actual CEO's voice at a press conference seemed to be used as a sample material for the AI method.



4. Three effective measures to prevent BEC from victimizing you

a. Reviewing your security measures

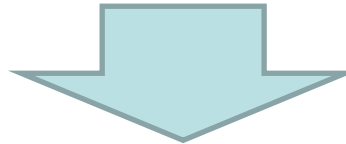
- i. To check your internal information security environment including PCs, network, various communication tools, etc.
- ii. To establish a system / framework that detects unauthorized logins.
- iii. To implement multi- factor authentication process.

b. Ensuring confirmation with your concerned party(s)

- i. To make direct communication e.g. telephone, if noticed by email of “Change of Bank Details”
- ii. It is better to reply by “Forward” than by “Reply”, when you cannot help confirming by email.
- iii. To avoid staff’s independent judgement, if the instructions of remittance are “Confidential” / “Urgent”.

c. Reviewing your fund management framework

- i. To review fund management authorities for situations when the representative is absent.
- ii. To establish an internal check framework such as requiring two persons’ signature.



To prevent BEC Fraud, information sharing is very important within all of your company and related individuals, not only Accounting/Treasury but also Sales/Purchasing /International Affairs and Domestic/Overseas Subsidiary, etc.

5. Self-diagnosis: Can you save yourself from BEC?

<Scenario>

1. You belong to Accounting Dept. in your company and are in charge of various payments overseas. On a certain day, you received an internal memo of payment to Supplier A, submitted by your Purchasing Dept.
2. You recognized that, in the memo, a bank name and an account holder's name were different from Supplier A's usual ones.
3. Then, you contacted your Purchasing Dept for confirmation. Purchasing dept replied, "The supplier surely requested this of us by email due to the change of their bank details."

**In such situation, how will you respond?
You have 3 choices as follows.**

- a. To agree with the Purchasing Dept (PD) staff and apply remittance.
- b. To recommend the PD staff to reconfirm the fact by "Reply" mail.
- c. To advise the PD staff to contact the supplier by telephone or fax etc, other than email, and to confirm that the request is genuine.

The right answer is "c".

**When trying to contact the genuine payee by telephone or fax, its number must be a registered one.
Do not access the number stated in the email, or you will be deceived and victimized.**

In case of being victimized by BEC Fraud,
please contact our bank staff at once.



Disclaimer

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.