WARDYŃSKI & PARTNERS

Business Email Compromise (BEC)

NOVEMBER 2022

A BRIEF GUIDE FOR ALL CONCERNED

I What is BEC

Business email compromise (BEC) is a cyber-facilitated fraud where culprits send spoofed emails fraudulently impersonating an individual or company to deceive the recipient into disposing of assets or revealing confidential information to unauthorised persons.

The most common type of BEC involves hacking email correspondence between established business partners who use wire transfers to settle their accounts. Hackers impersonate the payee and use various social manipulation techniques to instruct the payer to redirect payments to a "new" (fake) bank account.

EXAMPLE 1: TYPICAL FRAUDULENT EMAIL

> Dear Mark,
>
> I hope you are well and had a great holiday in Spain.
>
> I am writing to kindly let you know that our bank account will be suspended in August due to a financial audit of our company. Your next payments should be wired to our substitute bank account:
>
> 1 1 0 1 01 1 01 0 10 1 0 0000 0000 010 1
>
> Cyber Bank A.S.
>
> Thank you for your cooperation. In case of any questions please do let me know. Regards,
>
> Justin

BECs commonly refer to real people (using real names) and situations (e.g. monthly payments). To increase their credibility, the culprits may monitor and then mimie the patterns of communication, e.g. send spoofed emails at times of habitual contact, use characteristic expressions, and refer to previous correspondence or personal matters discussed in earlier correspondence.

Most often (but not always) these emails are not sent from real addresses. lnstead, the culprits register addresses similar to the bona-fide ones, but with

a small change that passes unnoticed by the recipient. Often the domain name is obscured by the user name.

EXAMPLE 2: SPOOFED DOMAIN NAMES

Original email address:	johnsmith@loremipsum.com	
Spoofed email addresses:	johnsmith@loremispum.com	switched letters “p” and “s”
	johnsmith@lorremipsum.com	doubled letter “r”
	john.smith@lorremipsum.com	added dot

This type of BEC has adverse effects on both sides of the business relationship: the payer loses its money to unknown culprits and the payee is deprived of its revenue.

The issue of which party ultimately bears the cost of the loss depends on the applicable substantive law and factual circumstances, specifically whether the party contributed to the fraud by not putting in place effective IT security measures.

CASE STUDY 1

Best-Food makes food products. lt has established a distribution network for its products on the European market. Super-Seller is one of its Polish distributors. The companies have a good, longstanding relationship.

Super-Seller received an email in which Best-Food instructed it to make all wire transfers to a new bank account. Super-Seller made a regular monthly payment to the new bank account. lt was only when Best-Food reminded it to make a payment that Best-Food discovered that the payment instruction had been sent from a spoofed email account (BestFoood).

The parties were in dispute over which of them should absorb the loss. Best-Food insisted on receiving the entire monthly payment. Super-Seller argued that Best-Food contributed to the loss. Super-Seller learned from other distributors that Best-Food had been informed by another customer of the registration of the BestFoood domain name and the risk of related BEC fraud. However, Best Food failed to take measures to alert its vendors to the potentiaI fraud.

No matter which party ultimately has to absorb the loss, when a business partner falIs victim to BEC fraud and incurs a financial loss, the situation gives rise to suspicion and distrust between the parties, and can spoil their good business relations.

II How to protect your business against BEC

To commit BEC, the culprits need to access prior email communications to learn the names and context necessary to make a credible impersonation. Therefore, the likelihood of BEC occurring in your business depends, first of all, on how easy it is to hack your email correspondence. The second element contributing to the BEC threat is the recipient's insufficient regard for cybersecurity. Bath can be easily remedied with the introduction of a handful of anti-BEC measures: raising the cyber-threat awareness among your staff, tightening your procedures, and providing new IT solutions.

Raise the cyber-threat awareness among your staff

Your employees need to become cyber-threat aware. They need to know how to use IT devices and services securely. To enhance the protection of your email correspondence and your IT system in general:

- lnstall antivirus software and remember to update it regularly.
- Do not check your email inbox from publicly accessible computers.
- lntroduce a dual authentication system where any email login requires entering an extra code received in the form of a text message.
- Use tools to filler and flag emails that come from unusual locations or have suspicious content.

To make your co-workers more cautious when it comes to cybersecurity, organise awareness training sessions showing the most common BEC patterns. lf your business is particularly prane to BEC fraud, consider simulating cyber-incidents (mock BEC attacks) as part of regular training.

Design and enforce effective procedures

Businesses are subject to a lot of regulations these days, so you may think that adopting more procedures will simply add more red tape to your operations. But aur experience shows that a business that has procedures for changing bank accounts and a plan for responding to cyber-incidents is less likely to become a victim of cyber fraud and, if it does, it will lose less money.

In aur opinion, every business should introduce at least these two security procedures:

- Mandatory double checks when changing banking instructions. lf your business receives a request to alter a banking instruction, your employees should confirm it with the requesting entity using a different channel of communications (e.g. calling them back).
- An action plan in case of a cyber-incident. Obviously, each attack is different and may require different response measures. Nonetheless, the procedure should make it clear who within the business is responsible for applying these measures and which resources they can use. Often it is important to have a panel of advisers available to assist (IT consultancy, forensic IT, lawyers).

Adopt IT solutions

There are new IT solutions that can flag all emails originating outside the organisation. This is a clear sign that the email needs to be carefully checked. These IT solutions can also show the exact domoin name from which the email originates and check whether your organisation considers it trustworthy.

Cyber insurance

You can never eliminate entirely the risk of a cyber-attack even when using the best security measures and procedures. So you may also consider taking out insurance against cyber-incidents.

III What to do in case of BEC?

Companies most often realise that they have fallen victim to BEC when one of their suppliers calls them with an urgent payment reminder even though they thought they had made the payment, or when they themselves do not receive an expected money transfer from their customer. That is when they find out that payments they made by wire transfer have not reached their intended addressee but, instead, an unknown third party.

In such case, it is important to act quickly to ensure the best chances of retrieval of as much of the funds as possible, and to minimise potential further losses. We suggest making the following steps applicable in all BEC cases related to diverted wire transfers.

Let your bank know ASAP

Notify your bank about the scam. Briefly explain what happened. To substantiate your claim, emphasise that the number of the fake recipient's bank account does not match the name of the intended recipient. This should be sufficiently alarming for the bank to take measures in response to your notification.

Your bank can pass this information immediately to the recipient bank via the SWIFT system of worldwide interbank communications. In turn, the recipient's bank will be able to pass the SWIFT warning on to banks where the transfers were made from the spoofed account.

Although banks are not under any general obligation to proceed, they usually consider the client's scam notification and account number/name mismatch sufficient to freeze the suspected account. And whenever a bank in Poland freezes a bank account because of a suspected crime, such as BEC, it must notify the prosecutor's office within 72 hours.

Thus notifying your bank may greatly improve your chance of retrieving the money. Even more, it may lead to freezing of the fake account, but also notifying law enforcement authorities of the scam.

PRACTICAL TIP:

> When you ask your bank to send a "stop payment" SWIFT message, instruct it to ask the correspondent bank to forward the message to any other bank(s) where it knows the funds were wired.

Contact the correspondent bank

Contact the correspondent bank personally. The bank will not disclose any information concerning the account to which you have wired your funds (bank secrecy bans disclosing information about the account holder or its funds in the account). However, the bank has certain obligations under anti money laundering laws and is required to evaluate the risk of fraud and money laundering on an ongoing basis.

Hence you should put the bank on notice that you were misled inio making a wire transfer to the account held at that bank. Request that the bank verify the account under suspicion of fraud, freeze the funds in the account and secure all evidence, in particular evidence prane to loss (CCTV and voice recordings, online banking IP logs, etc). Request the correspondent bank to put on notice other banks to which funds were transferred out of that account.

PRACTICAL TIP:

> Having an account number should be sufficient to establish which bank holds the account and the jurisdiction. Plenty of online services offer a free check. One of them is IBAN Checker, which is offered by IBAN: https://www.iban.com/

Talk to your business partners

lf you learn that one of your business partners has been deceived inio redirecting wire transfers from your bona-fide account to a fake one, your other business partners may have been too. To curb a potential spill-over of BEC, be quick to contact other firms that owe you money. Check if they got any false instructions for wire transfers and explain that they were fraudulent and should not be followed. Each of your partners that has fallen victim to BEC means another lost payment, another notification to the bank, and another criminal case for the prosecutor to pursue. That means less revenue and more costs. Do not let this happen.

Check your IT security

Have your IT system checked to establish if any of your data has been exposed to attacks. lf it has, the culprits may want to attack again. To minimise the risk of another BEC in the future, address the root causes that enabled the data theft.

Report the scam to law enforcement authorities

Even if the bank has been in contact with the prosecutor's office, we advise you to approach law enforcement authorities personally as well. The bank only notifies the prosecutor's office of the account freeze; it does not request it. Once notified, prosecutors may not necessarily uphold the freeze and take further action. They may be more prone to do so when the scam has been also reported by the defrauded party.

lf the prosecutor agrees to initiate an investigation, he will most likely assign a police officer to manage the case. The prosecutor will make decisions and the assigned officer will execute them. You should be active in the criminal investigation and request the law enforcement authorities to secure and collect the necessary evidence. Your actions will have three objectives: to find the culprits, to establish what happened to your money, and to check whether the banks complied with the AML rules when opening the fraudulent account. The most common actions in BEC cases include:

- Examining the bank employees who opened the fraudulent bank account
- Requesting the banks to reveal documents (e.g. the bank account agreement) and video surveillance footage (e.g. from the date when the account was opened)
- lnquiries to other institutions to verify the person specified as the holder of the fraudulent bank account (e.g. at the embassy of the alleged culprit's home country, if the alleged culprit is a foreigner)
- Requesting an expert to authenticate the documents (e.g. the passport presented by the person opening the fraudulent bank account).

As the police and prosecutor's offices are often understaffed, the investigation may proceed slowly. This problem may be greatly mitigated by the pro-active assistance of a lawyer, who may for instance:

- Provide the prosecutor with a summary of the facts in the case
- Analyse documents in the case file
- Request specific actions expected at different levels of the investigation
- Check on the progress by the police officer assigned to the case

- Map out the findings of different actions, emphasise facts, and suggest new links.

Take down the spoofed domain name

If the culprits created a spoofed domain name, take action to take it down. This will prevent the culprits from reusing the domain name in the future. Also, taking this action may yield information about the culprits (who registered the domain name, from which IP address, how payment was made, etc).

IV. Where to seek damages for BEC?

There are several potential means for you to recoup the lost money, although same may not always be available.

Request the prosecutor to disburse the frozen funds to you

lf the fake recipient account was frozen by the prosecutor, the prosecutor has the right to disburse the frozen funds to you. Moreover, the prosecutor may do so even before the investigation is concluded.

However, bear in mind that you may not be the only creditor entitled to funds frozen in the fake account. lf the fake account was also credited with funds transferred from accounts other than yours, the frozen funds ought to be divided proportionally between all creditors. This holds true even if the other creditors did not report any scam and do not take part in the investigation.

EXAMPLE 3: PRO RATA RETRIEVAL OF STOLEN MONEY

> The fake account was credited with USD 800 from your firm and USD 200 from another firm.
>
> Hence the total stolen funds amounted to USD 1,000, of which 80% was wired by your company.
>
> N ext, USD 300 was withdrawn from various ATMs, leaving a balance of USD 700.
>
> The account is frozen. Your firm gets 80% of the funds frozen in the account, i.e. USD 560.

Pro rata division of frozen funds gets more complicated in a situation where there have been a large number of incoming and outgoing transfers involving the fake account. In particularly complex cases, the prosecutor is likely to seek assistance from an expert, which may delay the disbursement.

EXAMPLE 4: COMPLEX TRANSFERS INTO AND OUT OF THE FRAUDULENT ACCOUNT

Incoming Transfers	*Outgoing Transfers*
Your company wired USD 5,000	
	USD 4,000 was wired to a second account of culprits (Account #2)
Company A wired USD 5,000	
	USD 3,000 was wired to a third account of culprits (Account #3)
	USD 500 was wired to Account #2
Company A wired USD 1,000	
Culprits wired USD 1,000 from Account #3	
Culprits wired USD 1,000 from Account #2	
Your company wired USD 3,000	

Suing the culprits

lf the disbursement of frozen funds did not cover all your losses or no funds were frozen, you can bring a civil action for damages against the culprits, including "mules." That scenario is feasible only when the investigation identifies the persons behind the BEC. However, even if this is the case, civil proceedings against them may be burdensome if these people reside abroad (which is often the case). Proceedings may prove futile if the culprits do not have sufficient assets (which is often the case when the only identified culprits are money mules).

Suing the bank

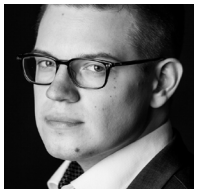
Another option for enforcement of damages is with a lawsuit against the bank that opened and ran the fake account used for the BEC. But the bank can be held liable for the money lost to BEC only to the extent that it failed to comply with its statutory AML obligations and where such failure clearly enabled the commission of fraud. To prove these prerequisites, extensive litigation is necessary. Pre-trial disclosure is not available in Poland, and hence the criminal investigation must be used to collect the necessary data and documents. With the permission of law enforcement authorities, these documents may be used in civil litigation.

As for the bank's failure to comply with statutes, the defrauded payer will need to establish the legaI standards arising under laws and regulations, such as regarding AML screening of potential clients ("know your customer") and continuous monitoring of accounts. As for the causal link between the failure and the fraud, it must be shown that if the bank had followed all applicable laws, the fraud would not have occurred.

However, recourse to such a civil action is only gaining popularity in Poland, and so far the legal precedents in this area are scarce. Only a couple of cases are currently proceeding in the Polish courts against ban ks that maintained fraudulent accounts, and neither has been decided yet. Thus extensive Iegal argumentation will most likely be required to persuade the court to award damages.

V Team

Łukasz Lasek
adwokat, partner
lukasz.lasek@wardynski.com.pl



Jakub Barański
adwokat, partner
jakub.baranski@wardynski.com.pl

Bartosz Troczyński
adwokat
bartosz.troczynski@wardynski.com.pl

Filip Rak
adwokat
filip.rak@wardynski.com.pl